

Communicate via **Micro network**



Micronet®
Making Communication Easier

User Manual

28-PORT GIGABIT MANAGED SWITCH

Model No.: SP6528



User Manual

SP6528

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

How to Use This Guide

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

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

How this Guide is Organized This guide provides detailed information about the switch's key features. It also describes the switch's web browser interface and command line interface.

The guide includes these sections:

- ◆ Section I [“Getting Started”](#) — Includes an introduction to switch management, and the basic settings required to access the management interface.
- ◆ Section II [“Web Configuration”](#) — Includes all management options available through the web browser interface.
- ◆ Section III [“Command Line Interface”](#) — Includes all management options available through the CLI.
- ◆ Section IV [“Appendices”](#) — Includes information on troubleshooting switch management access.

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

Installation Guide

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

Quick Start Guide

Safety and Regulatory Information

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



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



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

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

March 2017 Revision

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

Contents

How to Use This Guide	3
Contents	5
Figures	35
Tables	45

Section I	Getting Started	50
1	Introduction	51
	Key Features	51
	Description of Software Features	52
	Address Resolution Protocol	56
	System Defaults	57
2	Initial Switch Configuration	60
	Connecting to the Switch	60
	Configuration Options	60
	Connecting to the Console Port	61
	Logging Onto the Command Line Interface	62
	Setting Passwords	62
	Remote Connections	63
	Configuring the Switch for Remote Management	63
	Using the Network Interface	63
	Setting an IP Address	64
	Enabling SNMP Management Access	69
	Managing System Files	71
	Upgrading the Operation Code	72
	Saving or Restoring Configuration Settings	73

Automatic Installation of Operation Code and Configuration Settings	74
Downloading Operation Code from a File Server	74
Specifying a DHCP Client Identifier	77
Downloading a Configuration File and Other Parameters From a DHCP Server	78
Setting the System Clock	80
Setting the Time Manually	80
Configuring SNTP	81
Configuring NTP	81

Section II	Web Configuration	83
3	Using the Web Interface	84
	Connecting to the Web Interface	84
	Navigating the Web Browser Interface	85
	Dashboard	85
	Home Page	87
	Configuration Options	87
	Panel Display	88
	Main Menu	89
4	Basic Management Tasks	103
	Displaying System Information	104
	Displaying Hardware/Software Versions	105
	Configuring Support for Jumbo Frames	106
	Displaying Bridge Extension Capabilities	107
	Managing System Files	108
	Copying Files via FTP/ TFTP or HTTP	108
	Saving the Running Configuration to a Local File	110
	Setting the Start-up File	111
	Showing System Files	112
	Automatic Operation Code Upgrade	113
	Setting the System Clock	117
	Setting the Time Manually	117
	Setting the SNTP Polling Interval	118
	Configuring NTP	119

Configuring Time Servers	120
Setting the Time Zone	123
Configuring Summer Time	124
Configuring the Console Port	126
Configuring Telnet Settings	128
Displaying CPU Utilization	130
Configuring CPU Guard	131
Displaying Memory Utilization	132
Resetting the System	133
5 Interface Configuration	137
Port Configuration	138
Configuring by Port List	138
Configuring by Port Range	140
Displaying Connection Status	141
Showing Port or Trunk Statistics	142
Displaying Statistical History	146
Displaying Transceiver Data	150
Configuring Transceiver Thresholds	151
Trunk Configuration	153
Configuring a Static Trunk	155
Configuring a Dynamic Trunk	157
Displaying LACP Port Counters	163
Displaying LACP Settings and Status for the Local Side	164
Displaying LACP Settings and Status for the Remote Side	166
Configuring Load Balancing	167
Saving Power	169
Configuring Local Port Mirroring	171
Configuring Remote Port Mirroring	172
Traffic Segmentation	177
Enabling Traffic Segmentation	177
Configuring Uplink and Downlink Ports	178
6 VLAN Configuration	181
IEEE 802.1Q VLANs	181
Configuring VLAN Groups	184

Adding Static Members to VLANs	186
Protocol VLANs	190
Configuring Protocol VLAN Groups	191
Mapping Protocol Groups to Interfaces	192
Configuring MAC-based VLANs	194
7 Address Table Settings	197
Configuring MAC Address Learning	197
Setting Static Addresses	199
Changing the Aging Time	201
Displaying the Dynamic Address Table	201
Clearing the Dynamic Address Table	203
Issuing MAC Address Traps	204
8 Spanning Tree Algorithm	206
Overview	206
Configuring Loopback Detection	208
Configuring Global Settings for STA	210
Displaying Global Settings for STA	215
Configuring Interface Settings for STA	216
Displaying Interface Settings for STA	221
Configuring Multiple Spanning Trees	224
Configuring Interface Settings for MSTP	228
9 Congestion Control	230
Rate Limiting	230
Storm Control	231
10 Class of Service	233
Layer 2 Queue Settings	233
Setting the Default Priority for Interfaces	233
Selecting the Queue Mode	234
Layer 3/4 Priority Settings	237
Setting Priority Processing to DSCP or CoS	238
Mapping Ingress DSCP Values to Internal DSCP Values	239
Mapping CoS Priorities to Internal DSCP Values	241

11 Quality of Service	244
Overview	244
Configuring a Class Map	245
Creating QoS Policies	249
Attaching a Policy Map to a Port	253
12 VoIP Traffic Configuration	255
Overview	255
Configuring VoIP Traffic	256
Configuring Telephony OUI	257
Configuring VoIP Traffic Ports	258
13 Security Measures	261
AAA (Authentication, Authorization and Accounting)	262
Configuring Local/Remote Logon Authentication	263
Configuring Remote Logon Authentication Servers	264
Configuring AAA Accounting	269
Configuring AAA Authorization	275
Configuring User Accounts	279
Network Access (MAC Address Authentication)	281
Configuring Global Settings for Network Access	283
Configuring Network Access for Ports	284
Configuring a MAC Address Filter	286
Displaying Secure MAC Address Information	287
Configuring HTTPS	289
Configuring Global Settings for HTTPS	289
Replacing the Default Secure-site Certificate	290
Configuring the Secure Shell	292
Configuring the SSH Server	294
Generating the Host Key Pair	296
Importing User Public Keys	297
Access Control Lists	299
Showing TCAM Utilization	300
Setting the ACL Name and Type	302
Configuring a Standard IPv4 ACL	304
Configuring an Extended IPv4 ACL	305

Configuring a Standard IPv6 ACL	307
Configuring an Extended IPv6 ACL	309
Configuring a MAC ACL	311
Configuring an ARP ACL	313
Binding a Port to an Access Control List	315
Showing ACL Hardware Counters	316
ARP Inspection	317
Configuring Global Settings for ARP Inspection	318
Configuring VLAN Settings for ARP Inspection	320
Configuring Interface Settings for ARP Inspection	322
Displaying ARP Inspection Statistics	323
Displaying the ARP Inspection Log	324
Filtering IP Addresses for Management Access	325
Configuring Port Security	327
Configuring 802.1X Port Authentication	329
Configuring 802.1X Global Settings	331
Configuring Port Authenticator Settings for 802.1X	332
Displaying 802.1X Statistics	336
DHCP Snooping	337
DHCP Snooping Global Configuration	340
DHCP Snooping VLAN Configuration	341
Configuring Ports for DHCP Snooping	342
Displaying DHCP Snooping Binding Information	344
DoS Protection	345
IPv4 Source Guard	346
Configuring Ports for IPv4 Source Guard	346
Configuring Static Bindings for IPv4 Source Guard	349
Displaying Information for Dynamic IPv4 Source Guard Bindings	351
14 Basic Administration Protocols	353
Configuring Event Logging	354
System Log Configuration	354
Remote Log Configuration	356
Sending Simple Mail Transfer Protocol Alerts	357

Link Layer Discovery Protocol	359
Setting LLDP Timing Attributes	359
Configuring LLDP Interface Attributes	361
Configuring LLDP Interface Civic-Address	365
Displaying LLDP Local Device Information	367
Displaying LLDP Remote Device Information	371
Displaying Device Statistics	379
Simple Network Management Protocol	381
Configuring Global Settings for SNMP	383
Setting the Local Engine ID	384
Specifying a Remote Engine ID	385
Setting SNMPv3 Views	387
Configuring SNMPv3 Groups	389
Setting Community Access Strings	396
Configuring Local SNMPv3 Users	397
Configuring Remote SNMPv3 Users	399
Specifying Trap Managers	402
Creating SNMP Notification Logs	406
Showing SNMP Statistics	408
Remote Monitoring	410
Configuring RMON Alarms	411
Configuring RMON Events	413
Configuring RMON History Samples	415
Configuring RMON Statistical Samples	418
Setting a Time Range	421
LBD Configuration	423
Configuring Global Settings for LBD	424
Configuring Interface Settings for LBD	426
15 Multicast Filtering	427
Overview	427
Layer 2 IGMP (Snooping and Query for IPv4)	428
Configuring IGMP Snooping and Query Parameters	430
Specifying Static Interfaces for a Multicast Router	434
Assigning Interfaces to Multicast Services	436

Setting IGMP Snooping Status per Interface	438
Filtering IGMP Query Packets and Multicast Data	444
Displaying Multicast Groups Discovered by IGMP Snooping	445
Displaying IGMP Snooping Statistics	446
Filtering and Throttling IGMP Groups	450
Enabling IGMP Filtering and Throttling	450
Configuring IGMP Filter Profiles	451
Configuring IGMP Filtering and Throttling for Interfaces	453
MLD Snooping (Snooping and Query for IPv4)	455
Configuring MLD Snooping and Query Parameters	455
Setting Immediate Leave Status for MLD Snooping per Interface	457
Specifying Static Interfaces for an IPv6 Multicast Router	458
Assigning Interfaces to IPv6 Multicast Services	460
Showing MLD Snooping Groups and Source List	462
16 IP Tools	464
Using the Ping Function	464
Using the Trace Route Function	465
Address Resolution Protocol	467
Displaying Dynamic or Local ARP Entries	468
17 IP Services	469
Domain Name Service	469
Configuring General DNS Service Parameters	469
Configuring a List of Domain Names	470
Configuring a List of Name Servers	472
Configuring Static DNS Host to Address Entries	473
Displaying the DNS Cache	474
Dynamic Host Configuration Protocol	475
Specifying a DHCP Client Identifier	476
Configuring DHCP Relay Service	477
Enabling DHCP Dynamic Provision	481
18 IP Configuration	483
Setting the Switch's IP Address (IP Version 4)	483
Configuring the IPv4 Default Gateway	483

Configuring IPv4 Interface Settings	484
Setting the Switch's IP Address (IP Version 6)	487
Configuring the IPv6 Default Gateway	488
Configuring IPv6 Interface Settings	489
Configuring an IPv6 Address	493
Showing IPv6 Addresses	496
Showing the IPv6 Neighbor Cache	497
Showing IPv6 Statistics	498
Showing the MTU for Responding Destinations	504

Section III	Command Line Interface	505
19	Using the Command Line Interface	507
Accessing the CLI		507
Console Connection		507
Telnet Connection		508
Entering Commands		509
Keywords and Arguments		509
Minimum Abbreviation		509
Command Completion		509
Getting Help on Commands		510
Partial Keyword Lookup		511
Negating the Effect of Commands		512
Using Command History		512
Understanding Command Modes		512
Exec Commands		512
Configuration Commands		513
Command Line Processing		515
Showing Status Information		515
CLI Command Groups		516
20	General Commands	518
prompt		518
reload (Global Configuration)		519
enable		520

quit	521
show history	521
configure	522
disable	523
reload (Privileged Exec)	523
show reload	524
end	524
exit	524
21 System Management Commands	526
Device Designation	526
hostname	527
System Status	527
show access-list tcam-utilization	528
show memory	529
show process cpu	530
show process cpu guard	530
show process cpu task	531
show running-config	533
show startup-config	534
show system	535
show tech-support	536
show users	537
show version	537
show watchdog	538
watchdog software	538
Frame Size	539
jumbo frame	539
File Management	540
General Commands	541
boot system	541
copy	542
delete	545
dir	546
whichboot	547

Automatic Code Upgrade Commands	547
upgrade opcode auto	547
upgrade opcode path	549
upgrade opcode reload	550
show upgrade	550
TFTP Configuration Commands	550
ip tftp retry	550
ip tftp timeout	551
show ip tftp	551
Line	552
line	553
databits	554
exec-timeout	554
login	555
parity	556
password	557
password-thresh	557
silent-time	558
speed	559
stopbits	559
timeout login response	560
disconnect	561
terminal	561
show line	562
Event Logging	563
logging command	563
logging facility	564
logging history	564
logging host	565
logging on	566
logging trap	567
clear log	567
show log	568
show logging	569

SMTP Alerts	570
logging sendmail	571
logging sendmail destination-email	571
logging sendmail host	572
logging sendmail level	572
logging sendmail source-email	573
show logging sendmail	574
Time	574
SNTP Commands	575
sntp client	575
sntp poll	576
sntp server	576
show sntp	577
NTP Commands	578
ntp authenticate	578
ntp authentication-key	578
ntp client	579
ntp server	580
show ntp	581
Manual Configuration Commands	581
clock summer-time (date)	581
clock summer-time (predefined)	583
clock summer-time (recurring)	584
clock timezone	585
calendar set	586
show calendar	587
Time Range	587
time-range	587
absolute	588
periodic	589
show time-range	590
22 SNMP Commands	591
General SNMP Commands	593
snmp-server	593

snmp-server community	593
snmp-server contact	594
snmp-server location	595
show snmp	595
SNMP Target Host Commands	596
snmp-server enable traps	596
snmp-server host	597
snmp-server enable port-traps link-up-down	599
snmp-server enable port-traps mac-notification	600
show snmp-server enable port-traps	600
SNMPv3 Commands	601
snmp-server engine-id	601
snmp-server group	602
snmp-server user	603
snmp-server view	605
show snmp engine-id	606
show snmp group	607
show snmp user	608
show snmp view	609
Notification Log Commands	609
nlm	609
snmp-server notify-filter	610
show nlm oper-status	612
show snmp notify-filter	612
Additional Trap Commands	612
memory	612
process cpu	613
process cpu guard	614
23 Remote Monitoring Commands	616
rmon alarm	617
rmon event	618
rmon collection history	619
rmon collection rmon1	620
show rmon alarms	621

show rmon events	621
show rmon history	622
show rmon statistics	622
24 Authentication Commands	623
User Accounts and Privilege Levels	624
enable password	624
username	625
privilege	627
show privilege	627
Authentication Sequence	628
authentication enable	628
authentication login	629
RADIUS Client	630
radius-server acct-port	630
radius-server auth-port	631
radius-server host	631
radius-server key	632
radius-server retransmit	633
radius-server timeout	633
show radius-server	634
TACACS+ Client	634
tacacs-server host	635
tacacs-server key	635
tacacs-server port	636
tacacs-server retransmit	636
tacacs-server timeout	637
show tacacs-server	637
AAA	638
aaa accounting commands	639
aaa accounting dot1x	640
aaa accounting exec	641
aaa accounting update	642
aaa authorization commands	642
aaa authorization exec	643

aaa group server	644
server	645
accounting dot1x	645
accounting commands	646
accounting exec	646
authorization commands	647
authorization exec	648
show accounting	648
show authorization	649
Web Server	650
ip http authentication	651
ip http port	651
ip http server	652
ip http secure-port	652
ip http secure-server	653
Telnet Server	654
ip telnet max-sessions	655
ip telnet port	655
ip telnet server	656
telnet (client)	656
show ip telnet	657
Secure Shell	657
ip ssh authentication-retries	660
ip ssh server	660
ip ssh server-key size	661
ip ssh timeout	662
delete public-key	662
ip ssh crypto host-key generate	663
ip ssh crypto zeroize	664
ip ssh save host-key	664
show ip ssh	665
show public-key	665
show ssh	666

802.1X Port Authentication	666
General Commands	667
dot1x default	667
dot1x system-auth-control	668
Authenticator Commands	668
dot1x intrusion-action	668
dot1x max-reauth-req	669
dot1x max-req	670
dot1x operation-mode	670
dot1x port-control	671
dot1x re-authentication	672
dot1x timeout quiet-period	672
dot1x timeout re-authperiod	673
dot1x timeout supp-timeout	673
dot1x timeout tx-period	674
dot1x re-authenticate	674
Supplicant Commands	675
dot1x identity profile	675
dot1x max-start	676
dot1x pae supplicant	676
dot1x timeout auth-period	677
dot1x timeout held-period	677
dot1x timeout start-period	678
Information Display Commands	678
show dot1x	678
Management IP Filter	681
management	681
show management	682
25 General Security Measures	684
Port Security	685
mac-learning	685
port security	686
show port security	688

Network Access (MAC Address Authentication)	690
network-access aging	690
network-access mac-filter	691
network-access dynamic-vlan	692
network-access guest-vlan	693
clear network-access	693
show network-access	694
show network-access mac-address-table	695
show network-access mac-filter	696
DHCPv4 Snooping	696
ip dhcp snooping	697
ip dhcp snooping information option	699
ip dhcp snooping information option encode no-subtype	700
ip dhcp snooping information policy	702
ip dhcp snooping verify mac-address	702
ip dhcp snooping vlan	703
ip dhcp snooping information option circuit-id	704
ip dhcp snooping max-number	705
ip dhcp snooping trust	706
clear ip dhcp snooping binding	707
clear ip dhcp snooping database flash	707
ip dhcp snooping database flash	707
show ip dhcp snooping	708
show ip dhcp snooping binding	708
IPv4 Source Guard	709
ip source-guard binding	709
ip source-guard	711
ip source-guard max-binding	713
ip source-guard mode	714
clear ip source-guard binding blocked	714
show ip source-guard	715
show ip source-guard binding	715
ARP Inspection	716
ip arp inspection	717
ip arp inspection filter	718

ip arp inspection log-buffer logs	719
ip arp inspection validate	720
ip arp inspection vlan	721
ip arp inspection limit	722
ip arp inspection trust	722
show ip arp inspection configuration	723
show ip arp inspection interface	723
show ip arp inspection log	724
show ip arp inspection statistics	724
show ip arp inspection vlan	724
Denial of Service Protection	725
dos-protection smurf	725
dos-protection tcp-null-scan	726
dos-protection tcp-syn-fin-scan	726
dos-protection tcp-xmas-scan	727
show dos-protection	727
Port-based Traffic Segmentation	727
traffic-segmentation	728
traffic-segmentation session	729
traffic-segmentation uplink/downlink	730
traffic-segmentation uplink-to-uplink	731
show traffic-segmentation	732
26 Access Control Lists	733
IPv4 ACLs	733
access-list ip	734
permit, deny (Standard IP ACL)	735
permit, deny (Extended IPv4 ACL)	736
ip access-group	738
show ip access-group	739
show ip access-list	739
IPv6 ACLs	740
access-list ipv6	740
permit, deny (Standard IPv6 ACL)	741
permit, deny (Extended IPv6 ACL)	742

ipv6 access-group	745
show ipv6 access-group	745
show ipv6 access-list	746
MAC ACLs	746
access-list mac	747
permit, deny (MAC ACL)	747
mac access-group	750
show mac access-group	751
show mac access-list	751
ARP ACLs	752
access-list arp	752
permit, deny (ARP ACL)	753
show access-list arp	754
ACL Information	754
clear access-list hardware counters	755
show access-group	755
show access-list	756
27 Interface Commands	757
Interface Configuration	758
interface	758
capabilities	759
description	760
flowcontrol	761
history	762
media-type	762
negotiation	763
shutdown	764
speed-duplex	764
clear counters	765
show interfaces brief	766
show interfaces counters	767
show interfaces history	770
show interfaces status	772
show interfaces switchport	773

Transceiver Threshold Configuration	774
transceiver-monitor	774
transceiver-threshold-auto	775
transceiver-threshold current	775
transceiver-threshold rx-power	776
transceiver-threshold temperature	777
transceiver-threshold tx-power	778
transceiver-threshold voltage	779
show interfaces transceiver	780
show interfaces transceiver-threshold	781
Cable Diagnostics	782
test cable-diagnostics	782
show cable-diagnostics	783
Power Savings	784
power-save	784
show power-save	785
28 Link Aggregation Commands	786
Manual Configuration Commands	787
port channel load-balance	787
channel-group	789
Dynamic Configuration Commands	790
lacp	790
lacp admin-key (Ethernet Interface)	791
lacp port-priority	792
lacp system-priority	793
lacp admin-key (Port Channel)	794
lacp timeout	795
Trunk Status Display Commands	796
show lacp	796
show port-channel load-balance	799
29 Port Mirroring Commands	800
Local Port Mirroring Commands	800
port monitor	800
show port monitor	802

RSPAN Mirroring Commands	803
rspan source	805
rspan destination	806
rspan remote vlan	807
no rspan session	808
show rspan	809
30 Congestion Control Commands	810
Rate Limit Commands	810
rate-limit	811
Storm Control Commands	812
switchport packet-rate	812
31 Loopback Detection Commands	814
loopback-detection	815
loopback-detection action	815
loopback-detection recover-time	816
loopback-detection transmit-interval	817
loopback detection trap	817
loopback-detection release	818
show loopback-detection	818
32 Address Table Commands	820
mac-address-table aging-time	820
mac-address-table static	821
clear collision-mac-address-table	822
clear mac-address-table dynamic	822
show collision-mac-address-table	822
show mac-address-table	823
show mac-address-table aging-time	824
show mac-address-table count	824
33 Spanning Tree Commands	826
spanning-tree	827
spanning-tree cisco-prestandard	828
spanning-tree forward-time	828
spanning-tree hello-time	829

spanning-tree max-age	830
spanning-tree mode	830
spanning-tree mst configuration	832
spanning-tree pathcost method	832
spanning-tree priority	833
spanning-tree system-bpdu-flooding	834
spanning-tree tc-prop	834
spanning-tree transmission-limit	835
max-hops	836
mst priority	836
mst vlan	837
name	838
revision	838
spanning-tree bpdu-filter	839
spanning-tree bpdu-guard	840
spanning-tree cost	841
spanning-tree edge-port	842
spanning-tree link-type	843
spanning-tree loopback-detection	843
spanning-tree loopback-detection action	844
spanning-tree loopback-detection release-mode	845
spanning-tree loopback-detection trap	846
spanning-tree mst cost	846
spanning-tree mst port-priority	847
spanning-tree port-bpdu-flooding	848
spanning-tree port-priority	848
spanning-tree root-guard	849
spanning-tree spanning-disabled	850
spanning-tree tc-prop-stop	850
spanning-tree loopback-detection release	851
spanning-tree protocol-migration	852
show spanning-tree	852
show spanning-tree mst configuration	854
show spanning-tree tc-prop	854

34 VLAN Commands	856
Bridge Extension Commands	856
garp timer	857
switchport forbidden vlan	858
show bridge-ext	858
show garp timer	859
Editing VLAN Groups	860
vlan database	860
vlan	861
Configuring VLAN Interfaces	862
interface vlan	862
switchport acceptable-frame-types	863
switchport allowed vlan	864
switchport ingress-filtering	865
switchport mode	866
switchport native vlan	867
vlan-trunking	867
Displaying VLAN Information	869
show vlan	869
Configuring Protocol-based VLANs	870
protocol-vlan protocol-group (Configuring Groups)	871
protocol-vlan protocol-group (Configuring Interfaces)	871
show protocol-vlan protocol-group	872
show interfaces protocol-vlan protocol-group	873
Configuring Voice VLANs	874
voice vlan	874
voice vlan aging	875
voice vlan mac-address	876
switchport voice vlan	877
switchport voice vlan priority	878
switchport voice vlan rule	878
switchport voice vlan security	879
show voice vlan	880

35 Class of Service Commands	881
Priority Commands (Layer 2)	881
queue mode	882
queue weight	883
switchport priority default	884
show queue mode	885
show queue weight	885
Priority Commands (Layer 3 and 4)	886
qos map cos-dscp	886
qos map dscp-mutation	888
qos map trust-mode	889
show qos map cos-dscp	890
show qos map dscp-mutation	891
show qos map trust-mode	891
36 Quality of Service Commands	893
class-map	894
description	895
match	896
rename	897
policy-map	897
class	898
police rate	899
set cos	900
set ip dscp	901
set phb	902
service-policy	903
show class-map	903
show policy-map	904
show policy-map interface	905
37 Multicast Filtering Commands	906
IGMP Snooping	906
ip igmp snooping	908
ip igmp snooping priority	909
ip igmp snooping proxy-reporting	909

ip igmp snooping querier	910
ip igmp snooping router-alert-option-check	911
ip igmp snooping router-port-expire-time	911
ip igmp snooping tcn-flood	912
ip igmp snooping tcn-query-solicit	913
ip igmp snooping unregistered-data-flood	914
ip igmp snooping unsolicited-report-interval	914
ip igmp snooping version	915
ip igmp snooping version-exclusive	916
ip igmp snooping vlan general-query-suppression	916
ip igmp snooping vlan immediate-leave	917
ip igmp snooping vlan last-memb-query-count	918
ip igmp snooping vlan last-memb-query-intvl	919
ip igmp snooping vlan mrd	919
ip igmp snooping vlan proxy-address	920
ip igmp snooping vlan query-interval	922
ip igmp snooping vlan query-resp-intvl	922
ip igmp snooping vlan static	923
clear ip igmp snooping groups dynamic	924
clear ip igmp snooping statistics	924
show ip igmp snooping	925
show ip igmp snooping group	926
show ip igmp snooping mrouter	927
show ip igmp snooping statistics	927
Static Multicast Routing	930
ip igmp snooping vlan mrouter	930
IGMP Filtering and Throttling	931
ip igmp filter (Global Configuration)	932
ip igmp profile	932
permit, deny	933
range	933
ip igmp filter (Interface Configuration)	934
ip igmp max-groups	935
ip igmp max-groups action	935
ip igmp query-drop	936

ip multicast-data-drop	936
show ip igmp filter	937
show ip igmp profile	938
show ip igmp query-drop	938
show ip igmp throttle interface	939
show ip multicast-data-drop	940
MLD Snooping	940
ipv6 mld snooping	942
ipv6 mld snooping proxy-reporting	942
ipv6 mld snooping querier	943
ipv6 mld snooping query-interval	943
ipv6 mld snooping query-max-response-time	944
ipv6 mld snooping robustness	944
ipv6 mld snooping router-port-expire-time	945
ipv6 mld snooping unknown-multicast mode	946
ipv6 mld snooping unsolicited-report-interval	946
ipv6 mld snooping version	947
ipv6 mld snooping vlan immediate-leave	947
ipv6 mld snooping vlan mrouter	948
ipv6 mld snooping vlan static	949
clear ipv6 mld snooping groups dynamic	949
clear ipv6 mld snooping statistics	950
show ipv6 mld snooping	950
show ipv6 mld snooping group	951
show ipv6 mld snooping group source-list	952
show ipv6 mld snooping mrouter	952
show ipv6 mld snooping statistics	953
MLD Filtering and Throttling	954
ipv6 mld filter (Global Configuration)	954
ipv6 mld profile	955
permit, deny	956
range	956
ipv6 mld filter (Interface Configuration)	957
ipv6 mld max-groups	957
ipv6 mld max-groups action	958

ipv6 mld query-drop	959
show ipv6 mld filter	959
show ipv6 mld profile	960
show ipv6 mld query-drop	960
show ipv6 mld throttle interface	961
38 LLDP Commands	962
lldp	964
lldp holdtime-multiplier	964
lldp med-fast-start-count	965
lldp notification-interval	965
lldp refresh-interval	966
lldp reinit-delay	966
lldp tx-delay	967
lldp admin-status	968
lldp basic-tlv management-ip-address	968
lldp basic-tlv port-description	969
lldp basic-tlv system-capabilities	969
lldp basic-tlv system-description	970
lldp basic-tlv system-name	970
lldp dot1-tlv proto-ident	971
lldp dot1-tlv proto-vid	971
lldp dot1-tlv pvid	972
lldp dot1-tlv vlan-name	972
lldp dot3-tlv link-aggr	973
lldp dot3-tlv mac-phy	973
lldp dot3-tlv max-frame	974
lldp med-location civic-addr	975
lldp med-notification	976
lldp med-tlv inventory	977
lldp med-tlv location	978
lldp med-tlv med-cap	978
lldp med-tlv network-policy	979
lldp notification	979
show lldp config	980

show lldp info local-device	981
show lldp info remote-device	982
show lldp info statistics	984
39 Domain Name Service Commands	985
ip domain-list	985
ip domain-lookup	986
ip domain-name	987
ip host	988
ip name-server	989
ipv6 host	990
clear dns cache	990
clear host	991
show dns	991
show dns cache	992
show hosts	992
40 DHCP Commands	994
DHCP Client	994
DHCP for IPv4	995
ip dhcp dynamic-provision	995
ip dhcp client class-id	996
ip dhcp restart client	998
show ip dhcp dynamic-provision	998
DHCP for IPv6	999
ipv6 dhcp client rapid-commit vlan	999
ipv6 dhcp restart client vlan	999
show ipv6 dhcp duid	1001
show ipv6 dhcp vlan	1001
41 IP Interface Commands	1003
IPv4 Interface	1003
Basic IPv4 Configuration	1004
ip address	1004
ip default-gateway	1006
show ip default-gateway	1007

show ip interface	1007
show ip traffic	1008
tracert	1009
ping	1010
ARP Configuration	1011
arp timeout	1011
clear arp-cache	1012
show arp	1012
IPv6 Interface	1013
Interface Address Configuration and Utilities	1014
ipv6 default-gateway	1014
ipv6 address	1015
ipv6 address autoconfig	1016
ipv6 address eui-64	1018
ipv6 address link-local	1020
ipv6 enable	1021
ipv6 mtu	1022
show ipv6 default-gateway	1023
show ipv6 interface	1023
show ipv6 mtu	1026
show ipv6 traffic	1026
clear ipv6 traffic	1030
ping6	1031
tracert6	1032
Neighbor Discovery	1033
ipv6 nd dad attempts	1033
ipv6 nd ns-interval	1035
ipv6 nd reachable-time	1036
clear ipv6 neighbors	1037
show ipv6 neighbors	1037

Section IV	Appendices	1039
	A Software Specifications	1040
	Software Features	1040
	Management Features	1041
	Standards	1042
	Management Information Bases	1042
	B Troubleshooting	1044
	Problems Accessing the Management Interface	1044
	Using System Logs	1045
	C License Information	1046
	The GNU General Public License	1046
	Glossary	1050
	CLI Command List	1057
	Index	1063

Figures

Figure 1: Dashboard	85
Figure 2: Home Page	87
Figure 3: Front Panel Indicators	88
Figure 4: System Information	104
Figure 5: General Switch Information	105
Figure 6: Configuring Support for Jumbo Frames	106
Figure 7: Displaying Bridge Extension Configuration	108
Figure 8: Copy Firmware	110
Figure 9: Saving the Running Configuration	111
Figure 10: Setting Start-Up Files	112
Figure 11: Displaying System Files	112
Figure 12: Configuring Automatic Code Upgrade	116
Figure 13: Manually Setting the System Clock	118
Figure 14: Setting the Polling Interval for SNTP	118
Figure 15: Configuring NTP	119
Figure 16: Specifying SNTP Time Servers	120
Figure 17: Adding an NTP Time Server	121
Figure 18: Showing the NTP Time Server List	122
Figure 19: Adding an NTP Authentication Key	123
Figure 20: Showing the NTP Authentication Key List	123
Figure 21: Setting the Time Zone	124
Figure 22: Configuring Summer Time	126
Figure 23: Console Port Settings	128
Figure 24: Telnet Connection Settings	129
Figure 25: Displaying CPU Utilization	130
Figure 26: Configuring CPU Guard	132
Figure 27: Displaying Memory Utilization	133
Figure 28: Restarting the Switch (Immediately)	135
Figure 29: Restarting the Switch (In)	135

Figure 30: Restarting the Switch (At)	136
Figure 31: Restarting the Switch (Regularly)	136
Figure 32: Configuring Connections by Port List	140
Figure 33: Configuring Connections by Port Range	141
Figure 34: Displaying Port Information	142
Figure 35: Showing Port Statistics (Table)	145
Figure 36: Showing Port Statistics (Chart)	146
Figure 37: Configuring a History Sample	148
Figure 38: Showing Entries for History Sampling	148
Figure 39: Showing Status of Statistical History Sample	149
Figure 40: Showing Current Statistics for a History Sample	149
Figure 41: Showing Ingress Statistics for a History Sample	150
Figure 42: Displaying Transceiver Data	151
Figure 43: Configuring Transceiver Thresholds	153
Figure 44: Configuring Static Trunks	155
Figure 45: Creating Static Trunks	156
Figure 46: Adding Static Trunks Members	156
Figure 47: Configuring Connection Parameters for a Static Trunk	157
Figure 48: Showing Information for Static Trunks	157
Figure 49: Configuring Dynamic Trunks	157
Figure 50: Configuring the LACP Aggregator Admin Key	160
Figure 51: Enabling LACP on a Port	161
Figure 52: Configuring LACP Parameters on a Port	162
Figure 53: Showing Members of a Dynamic Trunk	162
Figure 54: Configuring Connection Settings for a Dynamic Trunk	163
Figure 55: Showing Connection Parameters for Dynamic Trunks	163
Figure 56: Displaying LACP Port Counters	164
Figure 57: Displaying LACP Port Internal Information	166
Figure 58: Displaying LACP Port Remote Information	167
Figure 59: Configuring Load Balancing	169
Figure 60: Enabling Power Savings	170
Figure 61: Configuring Local Port Mirroring	171
Figure 62: Configuring Local Port Mirroring	172
Figure 63: Displaying Local Port Mirror Sessions	172
Figure 64: Configuring Remote Port Mirroring	173

Figure 65: Configuring Remote Port Mirroring (Source)	176
Figure 66: Configuring Remote Port Mirroring (Intermediate)	176
Figure 67: Configuring Remote Port Mirroring (Destination)	176
Figure 68: Enabling Traffic Segmentation	178
Figure 69: Configuring Members for Traffic Segmentation	179
Figure 70: Showing Traffic Segmentation Members	180
Figure 71: VLAN Compliant and VLAN Non-compliant Devices	182
Figure 72: Creating Static VLANs	185
Figure 73: Modifying Settings for Static VLANs	185
Figure 74: Showing Static VLANs	186
Figure 75: Configuring Static Members by VLAN Index	188
Figure 76: Configuring Static VLAN Members by Interface	189
Figure 77: Configuring Static VLAN Members by Interface Range	190
Figure 78: Configuring Protocol VLANs	192
Figure 79: Displaying Protocol VLANs	192
Figure 80: Assigning Interfaces to Protocol VLANs	194
Figure 81: Showing the Interface to Protocol Group Mapping	194
Figure 82: Configuring MAC-Based VLANs	196
Figure 83: Showing MAC-Based VLANs	196
Figure 84: Configuring MAC Address Learning	198
Figure 85: Configuring Static MAC Addresses	200
Figure 86: Displaying Static MAC Addresses	200
Figure 87: Setting the Address Aging Time	201
Figure 88: Displaying the Dynamic MAC Address Table	202
Figure 89: Clearing Entries in the Dynamic MAC Address Table	203
Figure 90: Issuing MAC Address Traps (Global Configuration)	204
Figure 91: Issuing MAC Address Traps (Interface Configuration)	205
Figure 92: STP Root Ports and Designated Ports	207
Figure 93: MSTP Region, Internal Spanning Tree, Multiple Spanning Tree	207
Figure 94: Spanning Tree – Common Internal, Common, Internal	208
Figure 95: Configuring Port Loopback Detection	210
Figure 96: Configuring Global Settings for STA (STP)	214
Figure 97: Configuring Global Settings for STA (RSTP)	214
Figure 98: Configuring Global Settings for STA (MSTP)	215
Figure 99: Displaying Global Settings for STA	216

Figure 100: Determining the Root Port	218
Figure 101: Configuring Interface Settings for STA	221
Figure 102: STA Port Roles	222
Figure 103: Displaying Interface Settings for STA	223
Figure 104: Creating an MST Instance	225
Figure 105: Displaying MST Instances	225
Figure 106: Modifying the Priority for an MST Instance	226
Figure 107: Displaying Global Settings for an MST Instance	226
Figure 108: Adding a VLAN to an MST Instance	227
Figure 109: Displaying Members of an MST Instance	227
Figure 110: Configuring MSTP Interface Settings	229
Figure 111: Displaying MSTP Interface Settings	229
Figure 112: Configuring Rate Limits	231
Figure 113: Configuring Storm Control	232
Figure 114: Setting the Default Port Priority	234
Figure 115: Setting the Queue Mode (Strict)	236
Figure 116: Setting the Queue Mode (WRR)	236
Figure 117: Setting the Queue Mode (Strict and WRR)	237
Figure 118: Setting the Trust Mode	239
Figure 119: Configuring DSCP to DSCP Internal Mapping	240
Figure 120: Showing DSCP to DSCP Internal Mapping	241
Figure 121: Configuring CoS to DSCP Internal Mapping	242
Figure 122: Showing CoS to DSCP Internal Mapping	243
Figure 123: Configuring a Class Map	246
Figure 124: Showing Class Maps	247
Figure 125: Adding Rules to a Class Map	248
Figure 126: Showing the Rules for a Class Map	248
Figure 127: Configuring a Policy Map	251
Figure 128: Showing Policy Maps	251
Figure 129: Adding Rules to a Policy Map	252
Figure 130: Showing the Rules for a Policy Map	253
Figure 131: Attaching a Policy Map to a Port	254
Figure 132: Configuring a Voice VLAN	257
Figure 133: Configuring an OUI Telephony List	258
Figure 134: Showing an OUI Telephony List	258

Figure 135: Configuring Port Settings for a Voice VLAN	260
Figure 136: Configuring the Authentication Sequence	264
Figure 137: Authentication Server Operation	264
Figure 138: Configuring Remote Authentication Server (RADIUS)	267
Figure 139: Configuring Remote Authentication Server (TACACS+)	268
Figure 140: Configuring AAA Server Groups	268
Figure 141: Showing AAA Server Groups	269
Figure 142: Configuring Global Settings for AAA Accounting	271
Figure 143: Configuring AAA Accounting Methods	272
Figure 144: Showing AAA Accounting Methods	273
Figure 145: Configuring AAA Accounting Service for 802.1X Service	273
Figure 146: Configuring AAA Accounting Service for Command Service	274
Figure 147: Configuring AAA Accounting Service for Exec Service	274
Figure 148: Displaying a Summary of Applied AAA Accounting Methods	275
Figure 149: Displaying Statistics for AAA Accounting Sessions	275
Figure 150: Configuring AAA Authorization Methods	277
Figure 151: Showing AAA Authorization Methods	277
Figure 152: Configuring AAA Authorization Methods for Exec Service	278
Figure 153: Displaying the Applied AAA Authorization Method	278
Figure 154: Configuring User Accounts	280
Figure 155: Showing User Accounts	281
Figure 156: Configuring Global Settings for Network Access	284
Figure 157: Configuring Interface Settings for Network Access	285
Figure 158: Configuring a MAC Address Filter for Network Access	286
Figure 159: Showing the MAC Address Filter Table for Network Access	287
Figure 160: Showing Addresses Authenticated for Network Access	288
Figure 161: Configuring HTTPS	290
Figure 162: Downloading the Secure-Site Certificate	292
Figure 163: Configuring the SSH Server	295
Figure 164: Generating the SSH Host Key Pair	296
Figure 165: Showing the SSH Host Key Pair	297
Figure 166: Copying the SSH User's Public Key	298
Figure 167: Showing the SSH User's Public Key	299
Figure 168: Showing TCAM Utilization	302
Figure 169: Creating an ACL	303

Figure 170: Showing a List of ACLs	303
Figure 171: Configuring a Standard IPv4 ACL	305
Figure 172: Configuring an Extended IPv4 ACL	307
Figure 173: Configuring a Standard IPv6 ACL	308
Figure 174: Configuring an Extended IPv6 ACL	311
Figure 175: Configuring a MAC ACL	313
Figure 176: Configuring a ARP ACL	315
Figure 177: Binding a Port to an ACL	316
Figure 178: Showing ACL Statistics	317
Figure 179: Configuring Global Settings for ARP Inspection	320
Figure 180: Configuring VLAN Settings for ARP Inspection	321
Figure 181: Configuring Interface Settings for ARP Inspection	322
Figure 182: Displaying Statistics for ARP Inspection	324
Figure 183: Displaying the ARP Inspection Log	325
Figure 184: Creating an IP Address Filter for Management Access	326
Figure 185: Showing IP Addresses Authorized for Management Access	327
Figure 186: Configuring Port Security	329
Figure 187: Configuring Port Authentication	330
Figure 188: Configuring Global Settings for 802.1X Port Authentication	331
Figure 189: Configuring Interface Settings for 802.1X Port Authenticator	335
Figure 190: Showing Statistics for 802.1X Port Authenticator	337
Figure 191: Configuring Global Settings for DHCP Snooping	341
Figure 192: Configuring DHCP Snooping on a VLAN	342
Figure 193: Configuring the Port Mode for DHCP Snooping	343
Figure 194: Displaying the Binding Table for DHCP Snooping	345
Figure 195: Protecting Against DoS Attacks	346
Figure 196: Setting the Filter Type for IPv4 Source Guard	348
Figure 197: Configuring Static Bindings for IPv4 Source Guard	351
Figure 198: Showing Static Bindings for IPv4 Source Guard	351
Figure 199: Showing the IPv4 Source Guard Binding Table	352
Figure 200: Configuring Settings for System Memory Logs	355
Figure 201: Showing Error Messages Logged to System Memory	356
Figure 202: Configuring Settings for Remote Logging of Error Messages	357
Figure 203: Configuring SMTP Alert Messages	358
Figure 204: Configuring LLDP Timing Attributes	361

Figure 205: Configuring LLDP Interface Attributes	365
Figure 206: Configuring the Civic Address for an LLDP Interface	366
Figure 207: Showing the Civic Address for an LLDP Interface	367
Figure 208: Displaying Local Device Information for LLDP (General)	370
Figure 209: Displaying Local Device Information for LLDP (Port)	370
Figure 210: Displaying Local Device Information for LLDP (Port Details)	370
Figure 211: Displaying Remote Device Information for LLDP (Port)	377
Figure 212: Displaying Remote Device Information for LLDP (Port Details)	378
Figure 213: Displaying Remote Device Information for LLDP (End Node)	379
Figure 214: Displaying LLDP Device Statistics (General)	381
Figure 215: Displaying LLDP Device Statistics (Port)	381
Figure 216: Configuring Global Settings for SNMP	384
Figure 217: Configuring the Local Engine ID for SNMP	385
Figure 218: Configuring a Remote Engine ID for SNMP	386
Figure 219: Showing Remote Engine IDs for SNMP	386
Figure 220: Creating an SNMP View	388
Figure 221: Showing SNMP Views	388
Figure 222: Adding an OID Subtree to an SNMP View	389
Figure 223: Showing the OID Subtree Configured for SNMP Views	389
Figure 224: Creating an SNMP Group	395
Figure 225: Showing SNMP Groups	395
Figure 226: Setting Community Access Strings	396
Figure 227: Showing Community Access Strings	397
Figure 228: Configuring Local SNMPv3 Users	398
Figure 229: Showing Local SNMPv3 Users	399
Figure 230: Changing a Local SNMPv3 User Group	399
Figure 231: Configuring Remote SNMPv3 Users	401
Figure 232: Showing Remote SNMPv3 Users	402
Figure 233: Configuring Trap Managers (SNMPv1)	405
Figure 234: Configuring Trap Managers (SNMPv2c)	405
Figure 235: Configuring Trap Managers (SNMPv3)	406
Figure 236: Showing Trap Managers	406
Figure 237: Creating SNMP Notification Logs	408
Figure 238: Showing SNMP Notification Logs	408
Figure 239: Showing SNMP Statistics	410

Figure 240: Configuring an RMON Alarm	412
Figure 241: Showing Configured RMON Alarms	413
Figure 242: Configuring an RMON Event	415
Figure 243: Showing Configured RMON Events	415
Figure 244: Configuring an RMON History Sample	417
Figure 245: Showing Configured RMON History Samples	417
Figure 246: Showing Collected RMON History Samples	418
Figure 247: Configuring an RMON Statistical Sample	419
Figure 248: Showing Configured RMON Statistical Samples	420
Figure 249: Showing Collected RMON Statistical Samples	420
Figure 250: Setting the Name of a Time Range	422
Figure 251: Showing a List of Time Ranges	422
Figure 252: Add a Rule to a Time Range	423
Figure 253: Showing the Rules Configured for a Time Range	423
Figure 254: Configuring Global Settings for LBD	425
Figure 255: Configuring Interface Settings for LBD	426
Figure 256: Multicast Filtering Concept	427
Figure 257: Configuring General Settings for IGMP Snooping	433
Figure 258: Configuring a Static Interface for a Multicast Router	435
Figure 259: Showing Static Interfaces Attached a Multicast Router	435
Figure 260: Showing Current Interfaces Attached a Multicast Router	436
Figure 261: Assigning an Interface to a Multicast Service	437
Figure 262: Showing Static Interfaces Assigned to a Multicast Service	438
Figure 263: Configuring IGMP Snooping on a VLAN	443
Figure 264: Showing Interface Settings for IGMP Snooping	443
Figure 265: Dropping IGMP Query or Multicast Data Packets	444
Figure 266: Showing Multicast Groups Learned by IGMP Snooping	445
Figure 267: Displaying IGMP Snooping Statistics – Query	448
Figure 268: Displaying IGMP Snooping Statistics – VLAN	449
Figure 269: Displaying IGMP Snooping Statistics – Port	449
Figure 270: Enabling IGMP Filtering and Throttling	451
Figure 271: Creating an IGMP Filtering Profile	452
Figure 272: Showing the IGMP Filtering Profiles Created	452
Figure 273: Adding Multicast Groups to an IGMP Filtering Profile	453
Figure 274: Showing the Groups Assigned to an IGMP Filtering Profile	453

Figure 275: Configuring IGMP Filtering and Throttling Interface Settings	455
Figure 276: Configuring General Settings for MLD Snooping	457
Figure 277: Configuring Immediate Leave for MLD Snooping	458
Figure 278: Configuring a Static Interface for an IPv6 Multicast Router	459
Figure 279: Showing Static Interfaces Attached an IPv6 Multicast Router	459
Figure 280: Showing Current Interfaces Attached an IPv6 Multicast Router	459
Figure 281: Assigning an Interface to an IPv6 Multicast Service	461
Figure 282: Showing Static Interfaces Assigned to an IPv6 Multicast Service	461
Figure 283: Showing Current Interfaces Assigned to an IPv6 Multicast Service	462
Figure 284: Showing IPv6 Multicast Services and Corresponding Sources	463
Figure 285: Pinging a Network Device	465
Figure 286: Tracing the Route to a Network Device	467
Figure 287: Displaying ARP Entries	468
Figure 288: Configuring General Settings for DNS	470
Figure 289: Configuring a List of Domain Names for DNS	471
Figure 290: Showing the List of Domain Names for DNS	472
Figure 291: Configuring a List of Name Servers for DNS	473
Figure 292: Showing the List of Name Servers for DNS	473
Figure 293: Configuring Static Entries in the DNS Table	474
Figure 294: Showing Static Entries in the DNS Table	474
Figure 295: Showing Entries in the DNS Cache	475
Figure 296: Specifying a DHCP Client Identifier	477
Figure 297: Layer 3 DHCP Relay Service	478
Figure 298: Configuring DHCP Relay Service	481
Figure 299: Enabling Dynamic Provisioning via DHCP	482
Figure 300: Configuring the IPv4 Default Gateway	484
Figure 301: Configuring a Static IPv4 Address	486
Figure 302: Configuring a Dynamic IPv4 Address	486
Figure 303: Showing the Configured IPv4 Address for an Interface	487
Figure 304: Configuring the IPv6 Default Gateway	488
Figure 305: Configuring General Settings for an IPv6 Interface	493
Figure 306: Configuring an IPv6 Address	495
Figure 307: Showing Configured IPv6 Addresses	497
Figure 308: Showing IPv6 Neighbors	498
Figure 309: Showing IPv6 Statistics (IPv6)	502

Figure 310: Showing IPv6 Statistics (ICMPv6)	503
Figure 311: Showing IPv6 Statistics (UDP)	503
Figure 312: Showing Reported MTU Values	504
Figure 313: Configuring VLAN Trunking	868

Tables

Table 1: Key Features	51
Table 2: System Defaults	57
Table 3: Options 60, 66 and 67 Statements	79
Table 4: Options 55 and 124 Statements	79
Table 5: Web Page Configuration Buttons	87
Table 6: Switch Main Menu	89
Table 7: Predefined Summer-Time Parameters	125
Table 8: Port Statistics	142
Table 9: LACP Port Counters	163
Table 10: LACP Internal Configuration Information	164
Table 11: LACP Remote Device Configuration Information	166
Table 12: Traffic Segmentation Forwarding	178
Table 13: Recommended STA Path Cost Range	217
Table 14: Default STA Path Costs	218
Table 15: Default Mapping of DSCP Values to Internal PHB/Drop Values	240
Table 16: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence	242
Table 17: Dynamic QoS Profiles	282
Table 18: HTTPS System Support	289
Table 19: ARP Inspection Statistics	323
Table 20: ARP Inspection Log	324
Table 21: 802.1X Statistics	336
Table 22: Logging Levels	354
Table 23: LLDP MED Location CA Types	365
Table 24: Chassis ID Subtype	367
Table 25: System Capabilities	368
Table 26: Port ID Subtype	369
Table 27: Remote Port Auto-Negotiation Advertised Capability	372
Table 28: SNMPv3 Security Models and Levels	382
Table 29: Supported Notification Messages	391

Table 30: Address Resolution Protocol	467
Table 31: Options 60, 66 and 67 Statements	476
Table 32: Options 55 and 124 Statements	476
Table 33: Show IPv6 Neighbors - display description	497
Table 34: Show IPv6 Statistics - display description	499
Table 35: Show MTU - display description	504
Table 36: General Command Modes	512
Table 37: Configuration Command Modes	514
Table 38: Keystroke Commands	515
Table 39: Command Group Index	516
Table 40: General Commands	518
Table 41: System Management Commands	526
Table 42: Device Designation Commands	526
Table 43: System Status Commands	527
Table 44: show access-list tcam-utilization - display description	529
Table 45: show process cpu guard - display description	531
Table 46: show system – display description	535
Table 47: show version – display description	538
Table 48: Frame Size Commands	539
Table 49: Flash/File Commands	540
Table 50: File Directory Information	546
Table 51: Line Commands	552
Table 52: Event Logging Commands	563
Table 53: Logging Levels	565
Table 54: show logging flash/ram - display description	569
Table 55: show logging trap - display description	570
Table 56: Event Logging Commands	570
Table 57: Time Commands	574
Table 58: Predefined Summer-Time Parameters	583
Table 59: Time Range Commands	587
Table 60: SNMP Commands	591
Table 61: show snmp engine-id - display description	606
Table 62: show snmp group - display description	607
Table 63: show snmp user - display description	608
Table 64: show snmp view - display description	609

Table 65: RMON Commands	616
Table 66: Authentication Commands	623
Table 67: User Access Commands	624
Table 68: Default Login Settings	626
Table 69: Authentication Sequence Commands	628
Table 70: RADIUS Client Commands	630
Table 71: TACACS+ Client Commands	634
Table 72: AAA Commands	638
Table 73: Web Server Commands	650
Table 74: HTTPS System Support	654
Table 75: Telnet Server Commands	654
Table 76: Secure Shell Commands	657
Table 77: show ssh - display description	666
Table 78: 802.1X Port Authentication Commands	666
Table 79: Management IP Filter Commands	681
Table 80: General Security Commands	684
Table 81: Management IP Filter Commands	685
Table 82: show port security - display description	688
Table 83: Network Access Commands	690
Table 84: DHCP Snooping Commands	696
Table 85: Option 82 information	701
Table 86: Option 82 information	704
Table 87: IPv4 Source Guard Commands	709
Table 88: ARP Inspection Commands	716
Table 89: DoS Protection Commands	725
Table 90: Commands for Configuring Traffic Segmentation	728
Table 91: Traffic Segmentation Forwarding	729
Table 92: Access Control List Commands	733
Table 93: IPv4 ACL Commands	733
Table 94: IPv6 ACL Commands	740
Table 95: MAC ACL Commands	746
Table 96: ARP ACL Commands	752
Table 97: ACL Information Commands	754
Table 98: Interface Commands	757
Table 99: show interfaces counters - display description	768

Table 100: show interfaces switchport - display description	774
Table 101: Link Aggregation Commands	786
Table 102: show lacp counters - display description	796
Table 103: show lacp internal - display description	797
Table 104: show lacp neighbors - display description	798
Table 105: show lacp sysid - display description	799
Table 106: Port Mirroring Commands	800
Table 107: Mirror Port Commands	800
Table 108: RSPAN Commands	803
Table 109: Congestion Control Commands	810
Table 110: Rate Limit Commands	810
Table 111: Rate Limit Commands	812
Table 112: Loopback Detection Commands	814
Table 113: Address Table Commands	820
Table 114: Spanning Tree Commands	826
Table 115: Recommended STA Path Cost Range	841
Table 116: Default STA Path Costs	841
Table 117: VLAN Commands	856
Table 118: Bridge Extension Commands	856
Table 119: show bridge-ext - display description	859
Table 120: Commands for Editing VLAN Groups	860
Table 121: Commands for Configuring VLAN Interfaces	862
Table 122: Commands for Displaying VLAN Information	869
Table 123: Protocol-based VLAN Commands	870
Table 124: Voice VLAN Commands	874
Table 125: Priority Commands	881
Table 126: Priority Commands (Layer 2)	881
Table 127: Priority Commands (Layer 3 and 4)	886
Table 128: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence	887
Table 129: Default Mapping of DSCP Values to Internal PHB/Drop Values	888
Table 130: Quality of Service Commands	893
Table 131: Multicast Filtering Commands	906
Table 132: IGMP Snooping Commands	906
Table 133: show ip igmp snooping statistics input - display description	928
Table 134: show ip igmp snooping statistics output - display description	928

Table 135: show ip igmp snooping statistics vlan query - display description	929
Table 136: Static Multicast Interface Commands	930
Table 137: IGMP Filtering and Throttling Commands	931
Table 138: MLD Snooping Commands	941
Table 139: MLD Filtering and Throttling Commands	954
Table 140: LLDP Commands	962
Table 141: LLDP MED Location CA Types	975
Table 142: Address Table Commands	985
Table 143: show dns cache - display description	992
Table 144: show hosts - display description	993
Table 145: DHCP Commands	994
Table 146: DHCP Client Commands	994
Table 147: Options 60, 66 and 67 Statements	997
Table 148: Options 55 and 124 Statements	997
Table 149: IP Interface Commands	1003
Table 150: IPv4 Interface Commands	1003
Table 151: Basic IP Configuration Commands	1004
Table 152: Address Resolution Protocol Commands	1011
Table 153: IPv6 Configuration Commands	1013
Table 154: show ipv6 interface - display description	1024
Table 155: show ipv6 mtu - display description	1026
Table 156: show ipv6 traffic - display description	1027
Table 157: show ipv6 neighbors - display description	1038
Table 158: Troubleshooting Chart	1044

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 51](#)

Introduction

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 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 Port Authentication – IEEE 802.1X Port Security – MAC address filtering
Access Control Lists	Supports up to 256 ACLs, 128 rules per ACL, and 512 rules per system
DHCP/DHCPv6	Client, Relay, Relay Option 82
Port Configuration	Speed, duplex mode, and flow control
Port Trunking	Supports up to 8 trunks – static or dynamic trunking (LACP)
Port Mirroring	3 sessions, one or more source ports to an analysis port
Congestion Control	Rate Limiting Throttling for broadcast, multicast, unknown unicast storms
Address Table	8K MAC addresses in the forwarding table (shared with L2 unicast, L2 multicast, IPv4 multicast, IPv6 multicast); 1K static MAC addresses; 512 L2 IPv4 multicast groups (shared with MAC address table)
IP Version 4 and 6	Supports IPv4 and IPv6 addressing and management

Table 1: Key Features (Continued)

Feature	Description
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 4094 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)
Quality of Service	Supports Differentiated Services (DiffServ)
Link Layer Discovery Protocol	Used to discover basic information about neighboring devices
Multicast Filtering	Supports IGMP snooping and query for Layer 2

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. Storm suppression prevents broadcast, multicast, and unknown unicast 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 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.

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.

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 8 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).

Virtual LANs The switch supports up to 4094 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.

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) scheduling, 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.

- Address Resolution Protocol** The switch uses 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.
- 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 for IPv4, and MLD Snooping and Query for IPv6 to manage multicast group registration.
- 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 and Security Measures	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
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
	DHCP Snooping	Disabled
	IP Source Guard	Disabled (all ports)
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Server Port	443

Table 2: System Defaults (Continued)

Function	Parameter	Default
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)
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
Address Table	Aging Time	300 seconds
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: RSTP standard)
	Edge Ports	Auto
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
	QinQ Tunneling	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	WRR
	Queue Weight	Queue: 0 1 2 3 4 5 6 7 Weight: 1 2 4 6 8 10 12 14
	Class of Service	Enabled
	IP DSCP Priority	Disabled

Table 2: System Defaults (Continued)

Function	Parameter	Default
IP Settings	Management. VLAN	VLAN 1
	IP Address	192.168.2.10
	Subnet Mask	255.255.255.0
	Default Gateway	Not configured
	DHCP	Client: Enabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes
Multicast Filtering	IGMP Snooping (Layer 2)	Snooping: Enabled Querier: Disabled
	MLD Snooping (Layer 2 IPv6)	Snooping: Enabled Querier: 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

2

Initial Switch Configuration

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

Connecting to the Switch

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



Note: An IPv4 address for this switch is obtained via DHCP by default. To change this address, see [“Setting an IP Address” on page 64](#).

Configuration Options

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

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

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

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

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

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

Connecting to the Console Port

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

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

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

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

4. Power on the switch.

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

**Logging Onto the
Command Line
Interface**

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

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

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

Setting Passwords

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

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

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

4. Type “username admin password 0 *password*,” for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:

CLI session with the SP6528 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)#
```

Remote Connections Prior to accessing the switch’s onboard agent via a network connection, you must first configure it with a valid IPv4 or IPv6 address, subnet mask, and default gateway using a console connection, or DHCP protocol.

An IPv4 address for the switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP, see [“Setting an IP Address” on page 64](#).

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



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

Note: Any VLAN group can be assigned an IP interface address ([page 64](#)) for managing the switch.

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

Configuring the Switch for Remote Management

Using the Network Interface The switch can be managed through the operational network, known as in-band management. Because in-band management traffic is mixed in with operational network traffic, it is subject to all of the filtering rules usually applied to a standard

network ports such as ACLs and VLAN tagging. In-band network management can be accessed via a connection to any network port (1-10).

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

- ◆ **Manual** — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.
- ◆ **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 68](#).

Manual Configuration

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



Note: The default IPv4 address and subnet mask for VLAN 1 is 192.168.2.10 255.255.255.255.

Assigning an IPv4 Address

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

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

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

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

4. To set the IP address of the default gateway for the network to which the switch belongs, type “ip default-gateway *gateway*,” where “gateway” is the IP address of the default gateway. Press <Enter>.

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

Assigning an IPv6 Address

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

An IPv6 prefix or address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields. For detailed information on the other ways to assign IPv6 addresses, see “[IPv6 Interface](#)” on page 1013.

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#conf
Console(config)#interface vlan 1
Console(config-if)#ipv6 address fe80::a58:5800 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::a58:5800%1/64
Global unicast address(es):
    (None)
Joined group address(es):
    ff02::1:ff58:5800
```

```
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#conf
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2000:1::/64
Console(config-if)#exit
Console(config)#ipv6 default-gateway 2000:1::254
Console(config)#end
```

```
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
    fe80::a58:5800%1/64
Global unicast address(es):
    2000:1::/64, subnet is 2000:1::/64
Joined group address(es):
    ff02::1:ff00:0
    ff02::1:ff58:5800
    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 2000:1::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#conf
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-E0-0C-00-00-FD
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.4 Mask: 255.255.255.0
  DHCP Client Vendor Class ID (text): SFP6528
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#conf
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::a58:5800%1/64
Global unicast address(es):
  2000:1::/64, subnet is 2000:1::/6
Joined group address(es):
  ff02::1:ff00:0
  ff02::1:ff58:5800
  ff02::1
```



```
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

Console#

Enabling SNMP Management Access

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

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

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

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

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

The default strings are:

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

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

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)
2. To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

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



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

Trap Receivers

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

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

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

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

Configuring Access for SNMP Version 3 Clients

To configure management access for SNMPv3 clients, you need to first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group. The following example creates one view called “mib-2” that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.1d bridge MIB. It assigns these respective read and read/write views to a group call “r&d” and specifies group authentication

via MD5 or SHA. In the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password “greenpeace” for authentication, and the password “einstien” for encryption.

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

For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to [“SNMP Commands” on page 591](#) or to [“Simple Network Management Protocol” on page 381](#).

Managing System Files

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

The types of files are:

- ◆ **Configuration** — This file type stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via 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 73](#) for more information.
- ◆ **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces.
- ◆ **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).



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

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows. The switch has a total of 128 Mbytes of flash memory for system files.

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

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

Upgrading the Operation Code

The following example shows how to download new firmware to the switch and activate it. The TFTP server could be any standards-compliant server running on Windows or Linux. Note that "anonymous" is set as the default user name.

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

```

Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
1. config: 2. opcode: 2
Source file name: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode: m360.bix
Console(config)#exit
Console#dir

```

File Name	Type	Startup	Modified Time	Size (bytes)
Unit 1:				
SP6528_V1.1.2.0.bix	OpCode	Y	2016-11-24 04:26:03	8057096
Factory_Default_Config.cfg	Config	N	2015-07-01 07:24:11	455
startup1.cfg	Config	Y	2015-07-01 07:24:22	1343

```

-----
Free space for compressed user config files: 24043520
Console#

```

Saving or Restoring Configuration Settings

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

New startup configuration files must have a name specified. File names on the switch are case-sensitive, can be from 1 to 31 characters, must not contain slashes (\ or /), and the leading letter of the file name must not be a period (.). (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

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

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

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

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

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

\Write to FLASH finish.
Success.

Console#
```

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

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

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

Success.
Console#
```

Automatic Installation of Operation Code and Configuration Settings

Downloading Operation Code from a File Server

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

Usage Guidelines

- ◆ If this feature is enabled, the switch searches the defined URL once during the bootup sequence.
- ◆ FTP (port 21) and TFTP (port 69) are both supported. Note that the TCP/UDP port bindings cannot be modified to support servers listening on non-standard ports.
- ◆ The host portion of the upgrade file location URL must be a valid IPv4 IP address. DNS host names are not recognized. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- ◆ The path to the directory must also be defined. If the file is stored in the root directory for the FTP/TFTP service, then use the "/" to indicate this (e.g., ftp://192.168.0.1/).
- ◆ The file name must not be included in the upgrade file location URL. The file name of the code stored on the remote server must be SP6528.bix (using lower case letters as indicated).
- ◆ The FTP connection is made with PASV mode enabled. PASV mode is needed to traverse some fire walls, even if FTP traffic is not blocked. PASV mode cannot be disabled.
- ◆ The switch-based search function is case-insensitive in that it will accept a file name in upper or lower case (i.e., the switch will accept *SP6528.BIX* from the server even though *SP6528.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, *sp6528.bix* and *SP6528.BIX* are considered to be unique files. Thus, if the upgrade file is stored

as *SP6528.BIX* (or even *Sp6528.bix*) on a case-sensitive server, then the switch (requesting *SP6528.bix*) will not be upgraded because the server does not recognize the requested file name and the stored file name as being equal. A notable exception in the list of case-sensitive Unix-like operating systems is Mac OS X, which by default is case-insensitive. Please check the documentation for your server's operating system if you are unsure of its file system's behavior.

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

To enable automatic upgrade, enter the following commands:

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Set the switch to automatically upgrade the current operational code when a new version is detected on the server. When the switch starts up and automatic image upgrade is enabled by this command, the switch will follow these steps when it boots up:

- a. It will search for a new version of the image at the location specified by **upgrade opcode path** command. The name for the new image stored on the FTP/TFTP server must be SP6528.bix. If the switch detects a code version newer than the one currently in use, it will download the new image. If two code images are already stored in the switch, the image not set to start up the system will be overwritten by the new version.
- b. After the image has been downloaded, the switch will send a trap message to log whether or not the upgrade operation was successful.
- c. It sets the new version as the startup image.
- d. It then restarts the system to start using the new image.

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

4. Display the automatic upgrade settings.

```
Console#show upgrade  
Auto Image Upgrade Global Settings:  
Status      : Enabled  
Reload Status : Enabled  
Path        :  
File Name   : SP6528.bix  
Console#
```


The following shows an example of the upgrade process.

```
Console#dir
      File Name                               Type  Startup Modify Time          Size(bytes)
-----
Unit 1:
SP6528_V1.1.1.27.bix                        OpCode Y      2016-11-24 04:26:03          8057096
Factory_Default_Config.cfg                  Config  N      2015-04-13 13:55:58           455
startup1.cfg                               Config  Y      2015-07-13 04:03:49          1707
-----
Free space for compressed user config files: 1355776

...
Press ENTER to start session
Automatic Upgrade is looking for a new image
New image detected: current version V1.1.1.27; new version V1.1.1.31
Image upgrade in progress
Downloading new image
Flash programming started
Flash programming completed
Success
The switch will now restart
...
Press ENTER to start session
Automatic Upgrade is looking for a new image
No new image detected
User Access Verification

Username: admin
Password:

      CLI session with the SP6528 is opened.
      To end the CLI session, enter [Exit].

Console#dir
      File Name                               Type  Startup Modify Time          Size(bytes)
-----
Unit 1:
SP6528_V1.1.1.27.bix                        OpCode  N      2015-06-10 11:21:26          8058496
SP6528_V1.1.1.31.bix                      OpCode  Y      2015-11-30 08:40:36          8098056
Factory_Default_Config.cfg                  Config  N      2015-04-13 13:55:58           455
startup1.cfg                               Config  Y      2015-07-13 04:03:49          1707
-----
Free space for compressed user config files: 1310720

Console#
```

Specifying a DHCP Client Identifier

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

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

The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification

information about a client, but the specific string to use should be supplied by your service provider or network administrator. Options 60 (vendor-class-identifier), 66 (tftp-server-name) and 67 (bootfile-name) statements can be added to the server daemon's configuration file as described in the following section.

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

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 000011112222
Console(config-if)#
```

Downloading a Configuration File and Other Parameters From a DHCP Server

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

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

Note the following DHCP client behavior:

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

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

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

Table 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 these items, the client request also includes a "vendor class identifier" that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.

Table 4: Options 55 and 124 Statements

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

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

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

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

log-facility local7;

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

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

class "Option66,67_1" {                                #DHCP Option 60 Vendor class
two
    match if option vendor-class-identifier = "sp6528.cfg";
    option tftp-server-name "192.168.255.101";
    option bootfile-name "test";
}
```



Note: Use "sp6528.cfg" for the vendor-class-identifier in the dhcpd.conf file.

Setting the System Clock

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

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

The switch also supports the following time settings:

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

Setting the Time Manually

To manually set the clock to 14:11:36, April 1st, 2013, enter this command.

```
Console#calendar set 14 11 36 1 April 2013
Console#
```

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

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

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

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

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

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

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

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

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

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

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

```
Console(config)#ntp client
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#ntp authenticate
Console(config)#ntp server 192.168.3.20
```

```
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.5.23 key 19
Console(config)#exit
Console#show ntp
Current Time           : Jan 19 10:20:32 2017
Polling                : 1024 seconds
Current Mode           : unicast
NTP Status              : Disabled
NTP Authenticate Status : Disabled
Last Update NTP Server  : 0.0.0.0      Port: 0
Last Update Time        : Jan  1 00:00:00 1970 UTC
Console#show ntp
Current Time           : Jan 19 10:25:39 2017
Polling                : 1024 seconds
Current Mode           : unicast
NTP Status              : Enabled
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 118.163.81.61 version 3
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 84
- ◆ "Basic Management Tasks" on page 103
- ◆ "Interface Configuration" on page 137
- ◆ "VLAN Configuration" on page 181
- ◆ "Address Table Settings" on page 197
- ◆ "Spanning Tree Algorithm" on page 206
- ◆ "Congestion Control" on page 230
- ◆ "Class of Service" on page 233
- ◆ "Quality of Service" on page 244
- ◆ "VoIP Traffic Configuration" on page 255
- ◆ "Security Measures" on page 261
- ◆ "Basic Administration Protocols" on page 353
- ◆ "Multicast Filtering" on page 427
- ◆ "IP Tools" on page 464
- ◆ "IP Services" on page 469
- ◆ "IP Configuration" on page 483

3

Using the Web Interface

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 9, Mozilla Firefox 39, or Google Chrome 44, or more recent versions).



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 [“Command Line Interface” on page 505](#).

Connecting to the Web Interface

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

1. The default IP address and subnet mask for the switch is 192.168.2.10 and 255.255.255.0, with no default gateway. If this is not compatible with the subnet connected to the switch, you can configure it with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See [“Initial Switch Configuration” on page 60](#).)
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 [“Configuring User Accounts” on page 279](#).)
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 216](#).

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

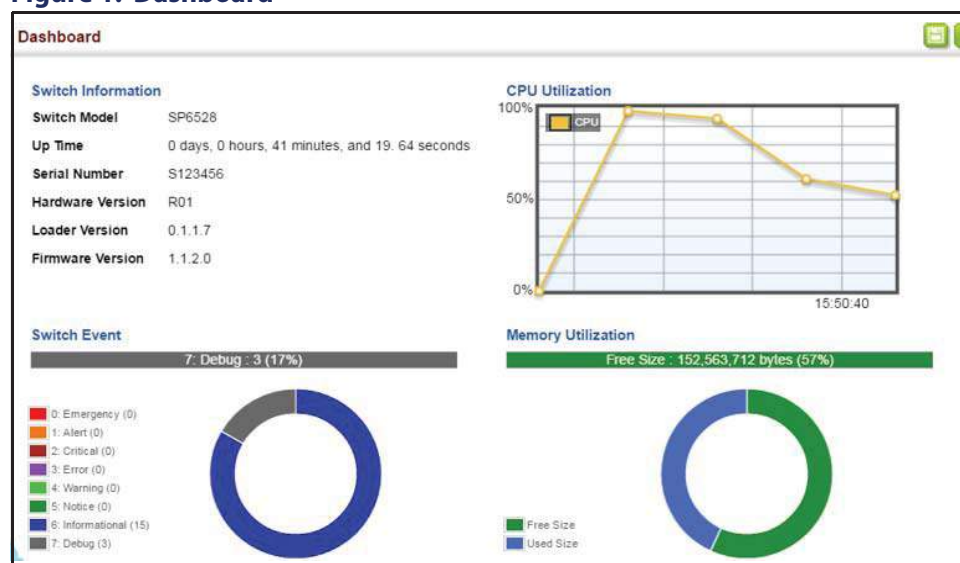
Note: Connection to the web interface is not supported for HTTPS using an IPv6 link local address.

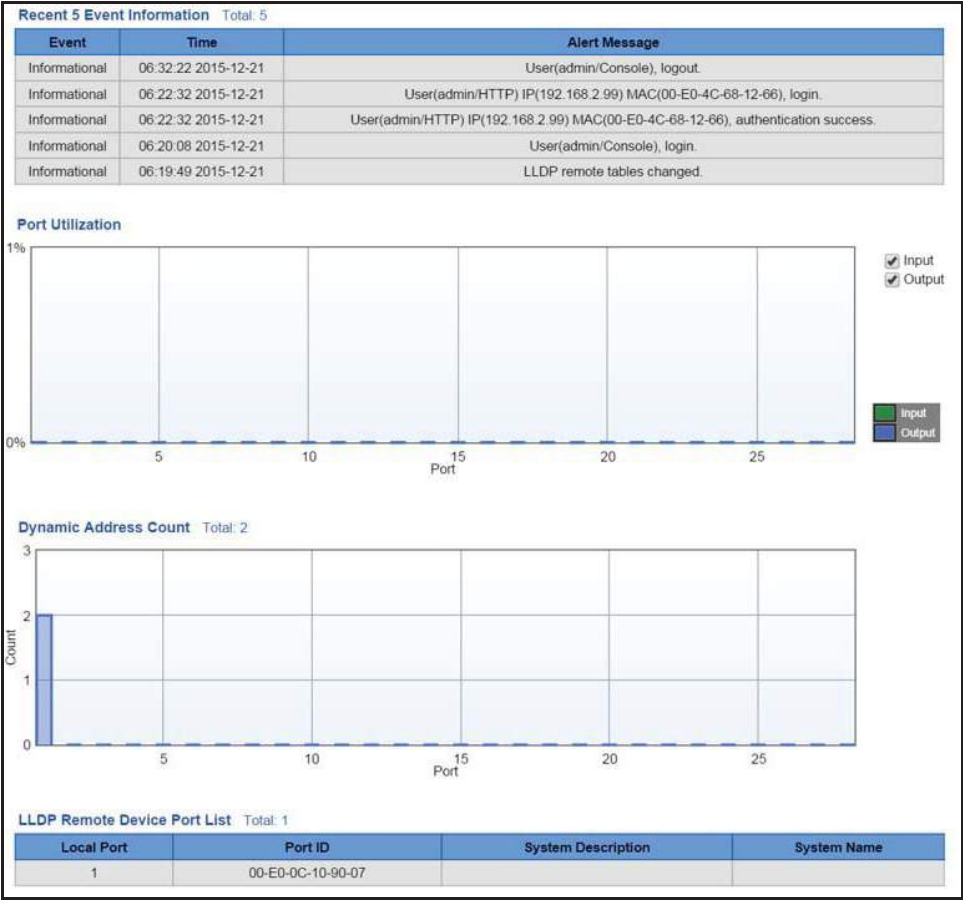
Navigating the Web Browser Interface

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.” The administrator has full access privileges to configure any parameters in the web interface. The default user name and password for guest access is “guest.” The guest only has read access for most configuration parameters. Refer to [“Configuring User Accounts” on page 279](#) for more details.

Dashboard When your web browser connects with the switch's web agent, the Dashboard is displayed as shown below. The Dashboard displays the main menu on the left side of the screen. Switch Information, CPU Utilization, Switch Events, Memory Utilization, Recent 5 Event Information, Port Utilization, Dynamic Address Count, and LLDP Remote Device Port List are displayed on the right side. The main menu links are used to navigate to other menus, and display configuration parameters and statistics.

Figure 1: Dashboard





Note: You can open a connection to the vendor’s web site by clicking on the Micronet logo.

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 2: Home Page





NOTE: You can open a connection to the vendor’s web site by clicking on the Micronet 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

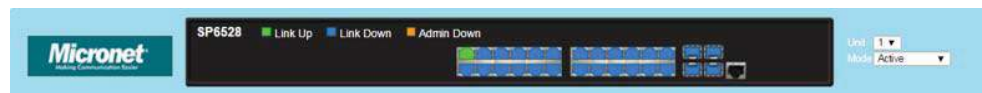
Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing “Apply.”
	Saves current configuration settings
	Displays help for the selected page.
	Refreshes the current page.
	Displays the site map.

Table 5: Web Page Configuration Buttons (Continued)

Button	Action
	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 3: Front Panel Indicators



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
Dashboard	Display switch Information, CPU utilization, switch events, memory utilization, recent 5 event information, port utilization, dynamic address count, and LLDP remote device port list	85
System		
General	Provides basic system description, including contact information	104
Switch	Shows the number of ports, hardware version, power status, and firmware version numbers	105
IP	Sets IPv4 address for management interface and gateway	483
Configure Global	Sets IP address of the gateway router between this device and management stations that exist on other network segments	483
Configure Interface	Configures IP address for management access	484
Add Address	Sets the IPv4 address for management access	484
Show Address	Shows the IPv4 address for management access	484
IPv6 Configuration		487
Configure Global	Sets an IPv6 default gateway for traffic with no known next hop	488
Configure Interface	Configures IPv6 interface address using auto-configuration or link-local address, and sets related protocol settings	489
Add IPv6 Address	Adds an global unicast, EUI-64, or link-local IPv6 address to an interface	493
Show IPv6 Address	Show the IPv6 addresses assigned to an interface	496
Show IPv6 Neighbor Cache	Displays information in the IPv6 neighbor discovery cache	497
Show Statistics		498
IPv6	Shows statistics about IPv6 traffic	498
ICMPv6	Shows statistics about ICMPv6 messages	498
UDP	Shows statistics about UDP messages	498
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	504
Capability	Enables support for jumbo frames; shows the bridge extension parameters	106, 107
File		108
Copy	Allows the transfer and copying files	108
Set Startup	Sets the startup file	111
Show	Shows the files stored in flash memory; allows deletion of files	112

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Time		117
Configure General		
Manual	Manually sets the current time	117
SNTP	Configures SNTP polling interval	118
NTP	Configures NTP authentication parameters	119
Configure Time Server	Configures a list of SNTP servers	120
Configure SNTP Server	Sets the IP address for SNTP time servers	120
Add NTP Server	Adds NTP time server and index of authentication key	120
Show NTP Server	Shows list of configured NTP time servers	120
Add NTP Authentication Key	Adds key index and corresponding MD5 key	122
Show NTP Authentication Key	Shows list of configured authentication keys	122
Configure Time Zone	Sets the local time zone for the system clock	123
Configure Summer Time	Configures summer time settings	124
Console	Sets console port connection parameters	126
Telnet	Sets Telnet connection parameters	128
CPU Utilization	Displays information on CPU utilization	130
CPU Guard	Sets the CPU utilization watermark and threshold	131
Memory Status	Shows memory utilization parameters	132
Reset	Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval	133
Interface		137
Port		138
General		138
Configure by Port List	Configures connection settings per port	138
Configure by Port Range	Configures connection settings for a range of ports	140
Show Information	Displays port connection status	141
Statistics	Shows Interface, Etherlike, and RMON port statistics	142
Chart	Shows Interface, Etherlike, and RMON port statistics	142
History	Shows statistical history for specified interfaces	146
Transceiver	Shows identifying information and operational parameters for optical transceivers which support Digital Diagnostic Monitoring (DDM), and configures thresholds for alarm and warning messages for optical transceivers which support DDM	150 151

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Trunk		153
Static		155
Configure Trunk		155
Add	Creates a trunk, along with the first port member	155
Show	Shows the configured trunk identifiers	155
Add Member	Specifies ports to group into static trunks	155
Show Member	Shows the port members for the selected trunk	155
Configure General		155
Configure	Configures trunk connection settings	155
Show Information	Displays trunk connection settings	155
Dynamic		157
Configure Aggregator	Configures administration key and timeout for specific LACP groups	157
Configure Aggregation Port		157
Configure		157
General	Allows ports to dynamically join trunks	157
Actor	Configures parameters for link aggregation group members on the local side	157
Partner	Configures parameters for link aggregation group members on the remote side	157
Show Information		163
Counters	Displays statistics for LACP protocol messages	163
Internal	Displays configuration settings and operational state for the local side of a link aggregation	164
Neighbors	Displays configuration settings and operational state for the remote side of a link aggregation	166
Configure Trunk		157
Configure	Configures connection settings	157
Show	Displays port connection status	157
Show Member	Shows the active members in a trunk	157
Statistics	Shows Interface, Etherlike, and RMON port statistics	142
Chart	Shows Interface, Etherlike, and RMON port statistics	142
Load Balance	Sets the load-distribution method among ports in aggregated links	167
History	Shows statistical history for specified interfaces	146
Green Ethernet	Adjusts the power provided to ports based on the length of the cable used to connect to other devices	169

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Mirror		171
Add	Sets the source and target ports for mirroring	171
Show	Shows the configured mirror sessions	171
RSPAN	Mirrors traffic from remote switches for analysis at a destination port on the local switch	172
Traffic Segmentation		177
Configure Global	Enables traffic segmentation globally	177
Configure Session	Configures the uplink and down-link ports for a segmented group of ports	178
VLAN	Virtual LAN	181
Static		184
Add	Creates VLAN groups	184
Show	Displays configured VLAN groups	184
Modify	Configures group name and administrative status	184
Edit Member by VLAN	Specifies VLAN attributes per VLAN	186
Edit Member by Interface	Specifies VLAN attributes per interface	186
Edit Member by Interface Range	Specifies VLAN attributes per interface range	186
Protocol		190
Configure Protocol		191
Add	Creates a protocol group, specifying supported protocols	191
Show	Shows configured protocol groups	191
Configure Interface		192
Add	Maps a protocol group to a VLAN	192
Show	Shows the protocol groups mapped to each VLAN	192
MAC-Based		194
Add	Maps traffic with specified source MAC address to a VLAN	194
Show	Shows source MAC address to VLAN mapping	194
MAC Address		197
Dynamic		
Configure Aging	Sets timeout for dynamically learned entries	201
Show Dynamic MAC	Displays dynamic entries in the address table	201
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	203
Learning Status	Enables MAC address learning on selected interfaces	197

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Static		199
Add	Configures static entries in the address table	199
Show	Displays static entries in the address table	199
MAC Notification		204
Configure Global	Issues a trap when a dynamic MAC address is added or removed	204
Configure Interface	Enables MAC authentication traps on the current interface	204
Spanning Tree		206
Loopback Detection	Configures Loopback Detection parameters	208
STA	Spanning Tree Algorithm	
Configure Global		
Configure	Configures global bridge settings for STP, RSTP and MSTP	210
Show Information	Displays STA values used for the bridge	215
Configure Interface		
Configure	Configures interface settings for STA	216
Show Information	Displays interface settings for STA	221
MSTP	Multiple Spanning Tree Algorithm	224
Configure Global		224
Add	Configures initial VLAN and priority for an MST instance	224
Modify	Configures the priority of an MST instance	224
Show	Configures global settings for an MST instance	224
Add Member	Adds VLAN members for an MST instance	224
Show Member	Adds or deletes VLAN members for an MST instance	224
Show Information	Displays MSTP values used for the bridge	
Configure Interface		228
Configure	Configures interface settings for an MST instance	228
Show Information	Displays interface settings for an MST instance	228
Traffic		
Rate Limit	Sets the input and output rate limits for a port	230
Storm Control	Sets the broadcast storm threshold for each interface	231
Priority		
Default Priority	Sets the default priority for each port or trunk	233
Queue	Sets queue mode for the switch; sets the service weight for each queue that will use a weighted or hybrid mode	234
Trust Mode	Selects DSCP or CoS priority processing	238

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
DSCP to DSCP		239
Add	Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	239
Show	Shows the DSCP to DSCP mapping list	239
CoS to DSCP		241
Add	Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing	241
Show	Shows the CoS to DSCP mapping list	241
DiffServ		244
Configure Class		245
Add	Creates a class map for a type of traffic	245
Show	Shows configured class maps	245
Modify	Modifies the name of a class map	245
Add Rule	Configures the criteria used to classify ingress traffic	245
Show Rule	Shows the traffic classification rules for a class map	245
Configure Policy		249
Add	Creates a policy map to apply to multiple interfaces	249
Show	Shows configured policy maps	249
Modify	Modifies the name of a policy map	249
Add Rule	Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic	249
Show Rule	Shows the rules used to enforce bandwidth policing for a policy map	249
Configure Interface	Applies a policy map to an ingress port	253
VoIP	Voice over IP	255
Configure Global	Configures auto-detection of VoIP traffic, sets the Voice VLAN, and VLAN aging time	256
Configure OUI		257
Add	Maps the OUI in the source MAC address of ingress packets to the VoIP device manufacturer	257
Show	Shows the OUI telephony list	257
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	258
Security		261
AAA	Authentication, Authorization and Accounting	262
System Authentication	Configures authentication sequence – local, RADIUS, and TACACS	263

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Server		264
Configure Server	Configures RADIUS and TACACS server message exchange settings	264
Configure Group		264
Add	Specifies a group of authentication servers and sets the priority sequence	264
Show	Shows the authentication server groups and priority sequence	264
Accounting	Enables accounting of requested services for billing or security purposes	269
Configure Global	Specifies the interval at which the local accounting service updates information to the accounting server	269
Configure Method		269
Add	Configures accounting for various service types	269
Show	Shows the accounting settings used for various service types	269
Configure Service	Sets the accounting method applied to specific interfaces for 802.1X, CLI command privilege levels for the console port, and for Telnet	269
Show Information		269
Summary	Shows the configured accounting methods, and the methods applied to specific interfaces	269
Statistics	Shows basic accounting information recorded for user sessions	269
Authorization	Enables authorization of requested services	275
Configure Method		275
Add	Configures authorization for various service types	275
Show	Shows the authorization settings used for various service types	275
Configure Service	Sets the authorization method applied used for the console port, and for Telnet	275
Show Information	Shows the configured authorization methods, and the methods applied to specific interfaces	275
User Accounts		279
Add	Configures user names, passwords, and access levels	279
Show	Shows authorized users	279
Modify	Modifies user attributes	279
Network Access	MAC address-based network access authentication	281
Configure Global	Enables aging for authenticated MAC addresses, and sets the time period after which a connected MAC address must be reauthenticated	283
Configure Interface		284
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	284

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Configure MAC Filter		286
Add	Specifies MAC addresses exempt from authentication	286
Show	Shows the list of exempt MAC addresses	286
Show Information	Shows the authenticated MAC address list	287
HTTPS	Secure HTTP	289
Configure Global	Enables HTTPSs, and specifies the UDP port to use	289
Copy Certificate	Replaces the default secure-site certificate	290
SSH	Secure Shell	292
Configure Global	Configures SSH server settings	294
Configure Host Key		296
Generate	Generates the host key pair (public and private)	296
Show	Displays RSA and DSA host keys; deletes host keys	296
Configure User Key		297
Copy	Imports user public keys from a TFTP server	297
Show	Displays RSA and DSA user keys; deletes user keys	297
ACL	Access Control Lists	299
Configure ACL		302
Show TCAM	Shows utilization parameters for TCAM	300
Add	Adds an ACL based on IP or MAC address filtering	302
Show	Shows the name and type of configured ACLs	302
Add Rule	Configures packet filtering based on IP or MAC addresses and other packet attributes	302
Show Rule	Shows the rules specified for an ACL	302
Configure Interface	Binds a port to the specified ACL and time range	
Configure	Binds a port to the specified ACL and time range	315
Show Hardware Counters	Shows statistics for ACL hardware counters	316
ARP Inspection		317
Configure General	Enables inspection globally, configures validation of additional address components, and sets the log rate for packet inspection	318
Configure VLAN	Enables ARP inspection on specified VLANs	320
Configure Interface	Sets the trust mode for ports, and sets the rate limit for packet inspection	322
Show Information		323
Show Statistics	Displays statistics on the inspection process	323
Show Log	Shows the inspection log list	324

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
IP Filter		325
Add	Sets IP addresses of clients allowed management access via the web, SNMP, and Telnet	325
Show	Shows the addresses to be allowed management access	325
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	327
Port Authentication	IEEE 802.1X	329
Configure Global	Enables authentication and EAPOL pass-through	331
Configure Interface	Sets authentication parameters for individual ports	332
Show Statistics	Displays protocol statistics for the selected port	336
DoS Protection	Protects against Denial-of-Service attacks	345
DHCP Snooping		337
Configure Global	Enables DHCP snooping globally, MAC-address verification, information option; and sets the information policy	340
Configure VLAN	Enables DHCP snooping on a VLAN	341
Configure Interface	Sets the trust mode for an interface	342
Show Information	Displays the DHCP Snooping binding information	344
IP Source Guard	Filters IP traffic based on static entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table	346
General	Enables IP source guard and selects filter type per port	346
Static Binding		349
Configure ACL Table		349
Add	Adds static addresses to the source guard ACL binding table	349
Show	Shows static addresses in the source guard ACL binding table	349
Configure MAC Table		349
Add	Adds static addresses to the source guard MAC address binding table	349
Show	Shows static addresses in the source guard MAC address binding table	349
Dynamic Binding	Displays the source-guard binding table for a selected interface	351
Administration		353
Log		354
System		354
Configure Global	Stores error messages in local memory	354
Show System Logs	Shows logged error messages	354
Remote	Configures the logging of messages to a remote logging process	356
SMTP	Sends an SMTP client message to a participating server	357

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
LLDP		359
Configure Global	Configures global LLDP timing parameters	359
Configure Interface		361
Configure General	Sets the message transmission mode; enables SNMP notification; and sets the LLDP attributes to advertise	361
Add CA-Type	Specifies the physical location of the device attached to an interface	365
Show Local Device Information		367
General	Displays general information about the local device	367
Port/Trunk	Displays information about each interface	367
Show Remote Device Information		371
Port/Trunk	Displays information about a remote device connected to a port on this switch	371
Port/Trunk Details	Displays detailed information about a remote device connected to this switch	371
Show Device Statistics		379
General	Displays statistics for all connected remote devices	379
Port/Trunk	Displays statistics for remote devices on a selected port or trunk	379
SNMP	Simple Network Management Protocol	381
Configure Global	Enables SNMP agent status, and sets related trap functions	383
Configure Community		396
Add	Configures community strings and access mode	396
Show	Shows community strings and access mode	396
Configure Engine		384
Set Engine ID	Sets the SNMP v3 engine ID on this switch	384
Add Remote Engine	Sets the SNMP v3 engine ID for a remote device	385
Show Remote Engine	Shows configured engine ID for remote devices	385
Configure View		387
Add View	Adds an SNMP v3 view of the OID MIB	387
Show View	Shows configured SNMP v3 views	387
Add OID Subtree	Specifies a part of the subtree for the selected view	387
Show OID Subtree	Shows the subtrees assigned to each view	387
Configure Group		389
Add	Adds a group with access policies for assigned users	389
Show	Shows configured groups and access policies	389
Configure User		
Add SNMPv3 Local User	Configures SNMPv3 users on this switch	397

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show SNMPv3 Local User	Shows SNMPv3 users configured on this switch	397
Change SNMPv3 Local User Group	Assign a local user to a new group	397
Add SNMPv3 Remote User	Configures SNMPv3 users from a remote device	399
Show SNMPv3 Remote User	Shows SNMPv3 users set from a remote device	397
Configure Trap		402
Add	Configures trap managers to receive messages on key events that occur on this switch	402
Show	Shows configured trap managers	402
Configure Notify Filter		
Add	Creates an SNMP notification log	406
Show	Shows the configured notification logs	406
Show Statistics	Shows the status of SNMP communications	408
RMON	Remote Monitoring	410
Configure Global		
Add		
Alarm	Sets threshold bounds for a monitored variable	411
Event	Creates a response event for an alarm	413
Show		
Alarm	Shows all configured alarms	411
Event	Shows all configured events	413
Configure Interface		
Add		
History	Periodically samples statistics on a physical interface	415
Statistics	Enables collection of statistics on a physical interface	418
Show		
History	Shows sampling parameters for each entry in the history group	415
Statistics	Shows sampling parameters for each entry in the statistics group	418
Show Details		
History	Shows sampled data for each entry in the history group	415
Statistics	Shows sampled data for each entry in the history group	418
Time Range	Configures the time to apply an ACL or PoE port	421
Add	Specifies the name of a time range	421
Show	Shows the name of configured time ranges	421
Add Rule		421
Absolute	Sets exact time or time range	421

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Periodic	Sets a recurrent time	421
LDB	Loopback Detection	423
Configure Global	Enables loopback detection globally, specifies the interval at which to transmit control frames, specifies the interval to wait before releasing an interface from shutdown state, specifies response to detect loopback, and traps to send	424
Configure Interface	Enables loopback detection per interface	426
Tools		464
Ping	Sends ICMP echo request packets to another node on the network	464
Trace Route	Shows the route packets take to the specified destination	465
ARP	Shows entries in the Address Resolution Protocol cache	467
Show Information	Shows entries in the Address Resolution Protocol (ARP) cache	468
IP Service		469
DNS	Domain Name Service	469
General		469
Configure Global	Enables DNS lookup; defines the default domain name appended to incomplete host names	470
Add Domain Name	Defines a list of domain names that can be appended to incomplete host names	470
Show Domain Names	Shows the configured domain name list	470
Add Name Server	Specifies IP address of name servers for dynamic lookup	472
Show Name Servers	Shows the name server address list	472
Static Host Table		473
Add	Configures static entries for domain name to address mapping	473
Show	Shows the list of static mapping entries	473
Modify	Modifies the static address mapped to the selected host name	473
Cache	Displays cache entries discovered by designated name servers	474
DHCP	Dynamic Host Configuration Protocol	475
Client	Specifies the DHCP client identifier for an interface	476
Relay	Specifies DHCP relay servers	477
Dynamic Provision	Enables dynamic provisioning via DHCP	481
Multicast		427
IGMP Snooping		428
General	Enables multicast filtering; configures parameters for multicast snooping	430
Multicast Router		434
Add Static Multicast Router	Assigns ports that are attached to a neighboring multicast router	434

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show Static Multicast Router	Displays ports statically configured as attached to a neighboring multicast router	434
Show Current Multicast Router	Displays ports attached to a neighboring multicast router, either through static or dynamic configuration	434
IGMP Member		436
Add Static Member	Statically assigns multicast addresses to the selected VLAN	436
Show Static Member	Shows multicast addresses statically configured on the selected VLAN	436
Interface		438
Configure VLAN	Configures IGMP snooping per VLAN interface	438
Show VLAN Information	Shows IGMP snooping settings per VLAN interface	438
Configure Port	Configures the interface to drop IGMP query packets or all multicast data packets	444
Configure Trunk	Configures the interface to drop IGMP query packets or all multicast data packets	444
Forwarding Entry	Displays the current multicast groups learned through IGMP Snooping	445
Filter		450
Configure General	Enables IGMP filtering for the switch	450
Configure Profile		451
Add	Adds IGMP filter profile; and sets access mode	451
Show	Shows configured IGMP filter profiles	451
Add Multicast Group Range	Assigns multicast groups to selected profile	451
Show Multicast Group Range	Shows multicast groups assigned to a profile	451
Configure Interface	Assigns IGMP filter profiles to port interfaces and sets throttling action	453
Statistics		446
Show Query Statistics	Shows statistics for query-related messages	446
Show VLAN Statistics	Shows statistics for protocol messages, number of active groups	446
Show Port Statistics	Shows statistics for protocol messages, number of active groups	446
Show Trunk Statistics	Shows statistics for protocol messages, number of active groups	446
MLD Snooping		455
General	Enables multicast filtering; configures parameters for IPv6 multicast snooping	455
Interface	Configures Immediate Leave status for a VLAN	457
Multicast Router		458
Add Static Multicast Router	Assigns ports that are attached to a neighboring multicast router	458
Show Static Multicast Router	Displays ports statically configured as attached to a neighboring multicast router	458
Show Current Multicast Router	Displays ports attached to a neighboring multicast router, either through static or dynamic configuration	458

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
MLD Member		460
Add Static Member	Statically assigns multicast addresses to the selected VLAN	460
Show Static Member	Shows multicast addresses statically configured on the selected VLAN	460
Show Current Member	Shows multicast addresses associated with the selected VLAN, either through static or dynamic configuration	460
Group Information	Displays known multicast groups, member ports, the means by which each group was learned, and the corresponding source list	462

Basic Management Tasks

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.
- ◆ [Configuring CPU Guard](#) – Sets thresholds in terms of CPU usage time and number of packets processed per second.
- ◆ [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.

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 4: System Information

The screenshot shows a web interface for configuring system information. The title bar reads "System > General". Below this, there are six rows of configuration fields:

System Description	SP6528
System Object ID	1.3.6.1.4.1.16813.26.104
System Up Time	0 days, 0 hours, 17 minutes, and 49.31 seconds
System Name	
System Location	
System Contact	

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

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.

Management Software Information

- ◆ **Role** – Shows that this switch is operating as Master or Slave.
- ◆ **Loader Version** – Version number of loader code.
- ◆ **Operation Code Version** – Version number of runtime code.

Web Interface

To view hardware and software version information.

1. Click System, then Switch.

Figure 5: General Switch Information

System > Switch	
Main Board Information	
Serial Number	S123456
Number of Ports	28
Hardware Version	R01
Main Power Status	Up
Management Software Information	
Role	Master
Loader Version	0.1.1.7
Operation Code Version	1.1.2.0

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.

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 6: 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.

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 233.](#))
- ◆ **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to [“Setting Static Addresses” on page 199.](#))
- ◆ **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 181.](#))
- ◆ **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.

Web Interface

To view Bridge Extension information:

1. Click System, then Capability.

Figure 7: Displaying Bridge Extension Configuration

The screenshot shows the 'System > Capability' configuration page. It has two main sections: 'General Capability' and 'Bridge Extension'. In the 'General Capability' section, 'Jumbo Frame' is set to 'Enabled'. In the 'Bridge Extension' section, 'Extended Multicast Filtering Services' is 'No', 'Traffic Classes' is 'Enabled', 'Static Entry Individual Port' is 'Yes', 'VLAN Version Number' is '2', 'VLAN Learning' is 'IVL', 'Local VLAN Capable' is 'No', 'Configurable PVID Tagging' is 'Yes', 'Max Supported VLAN Numbers' is '4094', and 'Max Supported VLAN ID' is '4094'. At the bottom right, there are 'Apply' and 'Revert' buttons.

System > Capability	
General Capability	
Jumbo Frame	☒ Enabled
Bridge Extension	
Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Version Number	2
VLAN Learning	IVL
Local VLAN Capable	No
Configurable PVID Tagging	Yes
Max Supported VLAN Numbers	4094
Max Supported VLAN ID	4094

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.

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.
- ◆ The reset command will not be accepted during copy operations to flash memory.

Parameters

The following parameters are displayed:

- ◆ **Copy Type** – The firmware copy operation includes these options:
 - HTTP Upload – Copies a file from a management station to the switch.
 - HTTP Download – Copies a file from the switch to a management station
 - TFTP Upload – Copies a file from a TFTP server to the switch.
 - TFTP Download – Copies a file from the switch to a TFTP server.
 - FTP Upload – Copies a file from an FTP server to the switch.
 - FTP Download – Copies a file from the switch to an FTP 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 or Config File to copy configuration settings.
- ◆ **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 Upload, HTTP Upload or TFTP Upload as the file transfer method.
4. If FTP or TFTP Upload is used, enter the IP address of the file server.

5. If FTP Upload 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. Click Apply.

Figure 8: Copy Firmware

The screenshot shows the 'System > File' configuration page. At the top, the 'Action' is set to 'Copy'. Below this, the 'Copy Type' is set to 'TFTP Upload'. The 'TFTP Server IP Address' is '192.168.2.99'. The 'File Type' is 'Operation Code'. The 'Source File Name' is 'SP6528_V1.1.2.1.bix'. The 'Destination File Name' has two radio button options: 'SP6528_V1.1.2.0.bix' (unselected) and 'SP6528_V1.1.2.1.bix' (selected). At the bottom right, there are 'Apply' and 'Revert' buttons.

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.

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. (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 9: Saving the Running Configuration

The screenshot shows the 'System > File' web interface. 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

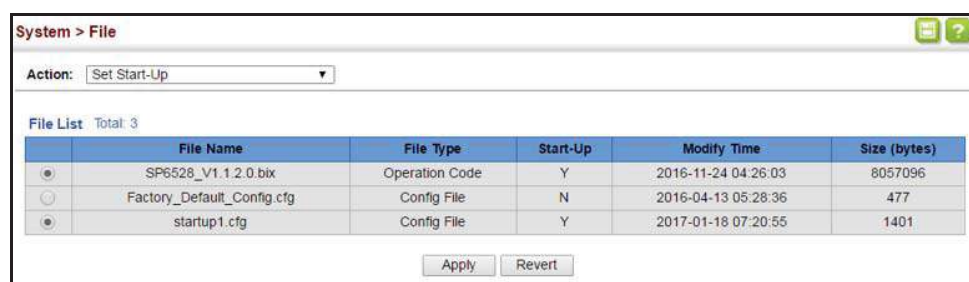
Use the System > File (Set Start-Up) page to specify the firmware or configuration file to use for system initialization.

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 10: Setting Start-Up Files



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.



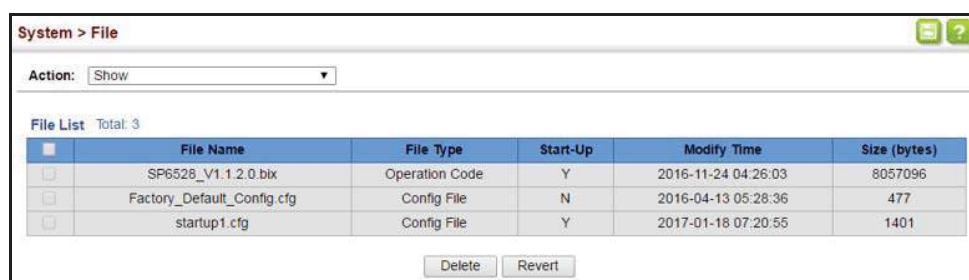
Note: Files designated for start-up, and the Factory_Default_Config.cfg file, cannot be deleted.

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 11: Displaying System Files



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.

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 *SP6528.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 *SP6528.BIX* from the server even though *SP6528.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, *sp6528.bix* and *SP6528.bix* are considered to be unique files. Thus, if the upgrade file is stored as *sp6528.bix* on a case-sensitive server, then the switch (requesting *SP6528.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 bootup 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 *SP6528.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.

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

- *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 12: Configuring Automatic Code Upgrade

The screenshot shows a web interface titled "System > File". Under the "Action:" dropdown, "Automatic Operation Code Upgrade" is selected. Below this, there is a section for "Automatic Opcode Upgrade" with a checkbox labeled "Enabled" that is checked. A text field for "Automatic Upgrade Location URL" contains the value "ftp://192.168.2.99/switches". A note below the text field states: "Note: For automatic upgrades, the operation code file name must be set as SP6528.bix." At the bottom right of the form are two buttons: "Apply" and "Revert".

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

```
Automatic Upgrade is looking for a new image
New image detected: current version 1.1.2.0; new version 1.1.2.1
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.

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 13: Manually Setting the System Clock

The screenshot shows the 'System > Time' configuration page. At the top, there is a breadcrumb 'System > Time' and a 'Step:' dropdown menu set to '1. Configure General'. Below this, the 'Current Time' is displayed as '2014-5-30 9:59:20'. The 'Maintain Type' is set to 'Manual' via a dropdown menu. Below the dropdown, there are input fields for time components: '9' for Hours, '59' for Minutes, '20' for Seconds, '5' for Month, '30' for Day, and '2014' for Year. At the bottom right, there 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.

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 14: Setting the Polling Interval for SNTP

The screenshot shows the 'System > Time' configuration page. At the top, there is a breadcrumb 'System > Time' and a 'Step:' dropdown menu set to '1. Configure General'. Below this, the 'Current Time' is displayed as '2014-5-30 9:59:20'. The 'Maintain Type' is set to 'SNTP' via a dropdown menu. Below the dropdown, there is a section titled 'SNTP Configuration' with a label 'SNTP Polling Interval (16-16384)' and an input field containing the value '16', followed by the unit 'sec'. At the bottom right, there 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.

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 15: Configuring NTP

The screenshot shows the 'System > Time' configuration page. At the top, there is a breadcrumb 'System > Time' and a 'Step:' dropdown menu set to '1. Configure General'. Below this, the 'Current Time' is displayed as '2014-5-30 9:59:20'. The 'Maintain Type' is set to 'NTP' via a dropdown menu. Under the 'NTP Configuration' section, the 'Authentication Status' is 'Enabled' with an unchecked checkbox. The 'Polling Interval' is set to '1024 sec'. At the bottom right, there are 'Apply' and 'Revert' buttons.

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.

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 16: Specifying SNTP Time Servers

The screenshot shows the 'System > Time' configuration page. At the top, there is a breadcrumb 'System > Time'. Below it, a 'Step:' dropdown is set to '2. Configure Time Server' and an 'Action:' dropdown is set to 'Configure SNTP Server'. The main area contains three input fields for SNTP Server IP addresses. The first field is labeled 'SNTP Server IP Address 1' and contains '10.1.0.19'. The second field is labeled 'SNTP Server IP Address 2' and contains '137.62.140.80'. The third field is labeled 'SNTP Server IP Address 3' and 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.

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.

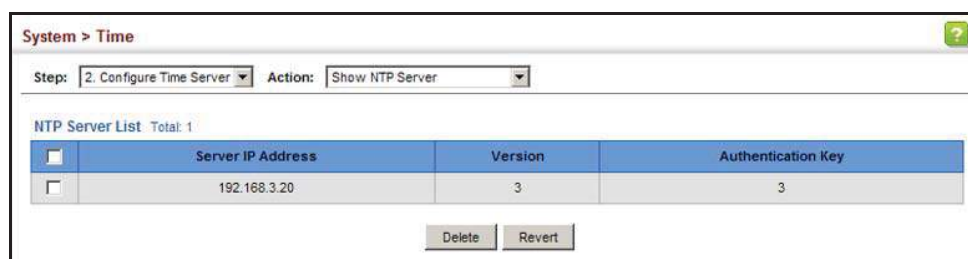
Figure 17: Adding an NTP Time Server

The screenshot shows the 'System > Time' configuration page. At the top, there is a breadcrumb 'System > Time'. Below it, there are two dropdown menus: 'Step: 2. Configure Time Server' and 'Action: Add NTP Server'. The main form contains three fields: 'NTP Server IP Address' with the value '192.168.3.20', 'Version' with the value '3', and 'Authentication Key (1-65535)' with the value '3' and a '(optional)' label. At the bottom right of the form are two buttons: 'Apply' and '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 18: Showing the NTP Time Server List



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.

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 19: Adding an NTP Authentication Key

System > Time

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

Authentication Key (1-65535) 3

Key Context (1-32) S1507N122103J068173M

Apply Revert

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 20: Showing the NTP Authentication Key List

System > Time

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

NTP Authentication Key List Total: 1

Authentication Key	Key Context
3	8J0774Q6699747D10867F12S505J62770084708278G1357878N8475052113Q69137L8

Delete Revert

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 east (before) or west (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.

Parameters

The following parameters are displayed:

- ◆ **Predefined Configuration** – A drop-down box provides access to the 80 predefined time zone configurations. Each choice indicates its offset from UTC and lists at least one major city or location covered by the time zone.
- ◆ **User-defined Configuration** – Allows the user to define all parameters of the local time zone.
 - **Direction** – Configures the time zone to be before (east of) or after (west of) UTC.

- **Name** – Assigns a name to the time zone. (Range: 1-30 characters)
- **Hours** (0-13) – 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 21: Setting the Time Zone

System > Time

Step: 3. Configure Time Zone ▼

☐ Predefined Configuration

☒ User Defined Configuration

Direction: After UTC ▼

Name: UTC

Hours (0-13): 0

Minutes (0-59): 0

Note: The maximum value before UTC is 12:00.
The maximum value after UTC is 13:00.

Apply Revert

Configuring Summer Time

Use the Summer Time page to set the system clock forward during the summer months (also known as daylight savings time).

In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

Parameters

The following parameters are displayed in the web interface:

General Configuration

- ◆ **Summer Time in Effect** – Shows if the system time has been adjusted.

- ◆ **Status** – Shows if summer time is set to take effect during the specified period.
- ◆ **Name** – Name of the time zone while summer time is in effect, usually an acronym. (Range: 1-30 characters)
- ◆ **Mode** – Selects one of the following configuration modes. (The Mode option can only be managed when the Summer Time Status option has been set to enabled for the switch.)

Predefined Mode – Configures the summer time status and settings for the switch using predefined configurations for several major regions of the world. To specify the time corresponding to your local time when summer time is in effect, select the predefined summer-time zone appropriate for your location.

Table 7: Predefined Summer-Time Parameters

Region	Start Time, Day, Week, & Month	End Time, Day, Week, & Month	Rel. Offset
Australia	00:00:00, Sunday, Week 5 of October	23:59:59, Sunday, Week 5 of March	60 min
Europe	00:00:00, Sunday, Week 5 of March	23:59:59, Sunday, Week 5 of October	60 min
New Zealand	00:00:00, Sunday, Week 1 of October	23:59:59, Sunday, Week 3 of March	60 min
USA	02:00:00, Sunday, Week 2 of March	02:00:00, Sunday, Week 1 of November	60 min

Date Mode – Sets the start, end, and offset times of summer time for the switch on a one-time basis. This mode sets the summer-time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time zone deviates from your regular time zone.

- ◆ **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 1-120 minutes)
- ◆ **From** – Start time for summer-time offset.
- ◆ **To** – End time for summer-time offset.

Recurring Mode – Sets the start, end, and offset times of summer time for the switch on a recurring basis. This mode sets the summer-time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time zone deviates from your regular time zone.

- ◆ **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 1-120 minutes)
- ◆ **From** – Start time for summer-time offset.
- ◆ **To** – End time for summer-time offset.

Web Interface

To specify summer time settings:

1. Click SNTP, Summer Time.
2. Select one of the configuration modes, configure the relevant attributes, enable summer time status.
3. Click Apply.

Figure 22: Configuring Summer Time

The screenshot shows a web interface for configuring system time. The breadcrumb is 'System > Time'. The current step is '4. Configure Summer Time'. The configuration options are as follows:

Field	Value
Summer Time in Effect	No
Status	☐ Enabled
Name	
Mode	Predefined
Daylight Savings	Australia

Buttons: Apply, 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.

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 557](#)).

Note: Password checking can be enabled or disabled for logging in to the console connection (see [“login” on page 555](#)). 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 23: Console Port Settings

The screenshot shows a web-based configuration interface for the console port. The title bar reads 'System > Console'. The settings are as follows:

Parameter	Value	Unit
Login Timeout (10-300)	300	sec
Exec Timeout (60-65535)	☒ 600	sec
Password Threshold (1-120)	☒ 3	
Silent Time (1-65535)	☐	sec
Data Bits	8	
Stop Bits	1	
Parity	None	
Speed	115200	baud

Buttons: Apply, Revert

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.

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 557).

Note: Password checking can be enabled or disabled for login to the console connection (see “login” on page 555). 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 24: Telnet Connection Settings

System > Telnet	
Telnet Status	☒ Enabled
TCP Port (1-65535)	23
Max Sessions (0-8)	8
Login Timeout (10-300)	300 sec
Exec Timeout (60-65535)	600 sec
Password Threshold (1-120)	☒ 3
Silent Time (1-65535)	☐ sec
Apply Revert	

Displaying CPU Utilization

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

Parameters

The following parameters are displayed:

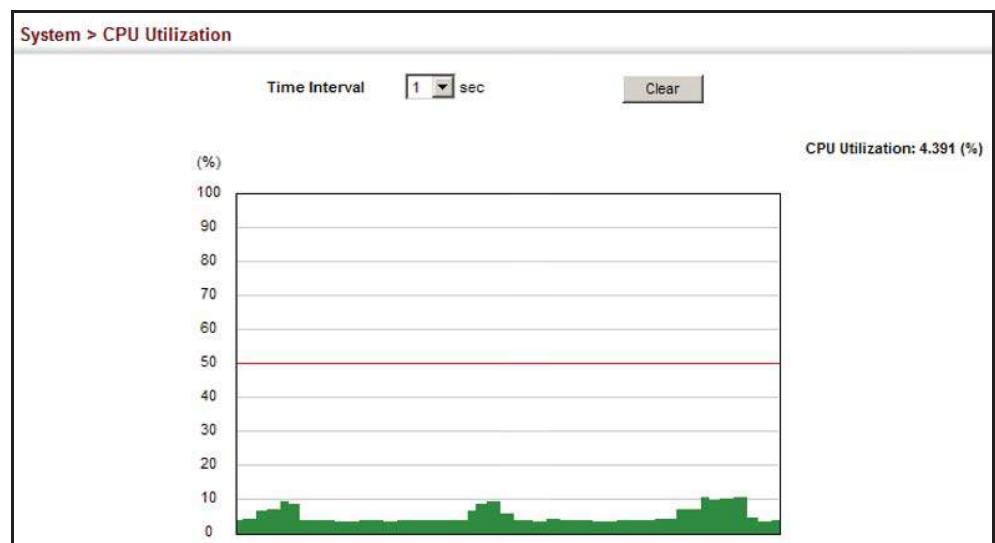
- ◆ **Time Interval** – The interval at which to update the displayed utilization rate. (Options: 1, 5, 10, 30, 60 seconds; Default: 1 second)
- ◆ **CPU Utilization** – CPU utilization over specified interval.

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 25: Displaying CPU Utilization



Configuring CPU Guard

Use the System > CPU Guard page to set the CPU utilization high and low watermarks in percentage of CPU time utilized and the CPU high and low thresholds in the number of packets being processed per second.

Parameters

The following parameters are displayed:

- ◆ **CPU Guard Status** – Enables CPU Guard. (Default: Disabled)
- ◆ **High Watermark** – If the percentage of CPU usage time is higher than the high-watermark, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until usage time falls below the low watermark. (Range: 40-100%; Default: 90%)
- ◆ **Low Watermark** – If packet flow has been stopped after exceeding the high watermark, normal flow will be restored after usage falls beneath the low watermark. (Range: 40-100%; Default: 70%)
- ◆ **Maximum Threshold** – If the number of packets being processed by the CPU is higher than the maximum threshold, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until the number of packets being processed falls below the minimum threshold. (Range: 50-500 pps; Default: 500 pps)
- ◆ **Minimum Threshold** – If packet flow has been stopped after exceeding the maximum threshold, normal flow will be restored after usage falls beneath the minimum threshold. (Range: 50-500 pps; Default: 50 pps)
- ◆ **Trap Status** – If enabled, an alarm message will be generated when utilization exceeds the high watermark or exceeds the maximum threshold. (Default: Disabled)

Once the high watermark is exceeded, utilization must drop beneath the low watermark before the alarm is terminated, and then exceed the high watermark again before another alarm is triggered.

Once the maximum threshold is exceeded, utilization must drop beneath the minimum threshold before the alarm is terminated, and then exceed the maximum threshold again before another alarm is triggered.

- ◆ **Current Threshold** – Shows the configured threshold in packets per second.

Web Interface

To configure CPU Guard:

1. Click System, CPU Guard.
2. Set CPU guard status, configure the watermarks or threshold parameter, enable traps if required.
3. Click Apply.

Figure 26: Configuring CPU Guard

System > CPU Guard

CPU Guard Status	☐ Enabled
High Watermark (40-100)	90 %
Low Watermark (40-100)	70 %
Maximum Threshold (50-500)	500 packets/sec
Minimum Threshold (50-500)	50 packets/sec
Trap Status	☐ Enabled
Current Threshold	500 packets/sec

Apply Revert

Displaying Memory Utilization

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

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 27: Displaying Memory Utilization

System > Memory Status		
Memory Status		
Free Size	45,416,448 bytes	16%
Used Size	223,019,008 bytes	84%
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.

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. (See [“Saving the Running Configuration to a Local File” on page 110](#)).

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: 01-31)
 - MM - The month at which to reload. (Range: 01-12)
 - YYYY - The year at which to reload. (Range: 1970-2037)
 - HH - The hour at which to reload. (Range: 00-23)
 - MM - The minute at which to reload. (Range: 00-59)
- **Regularly** – Specifies a periodic interval at which to reload the switch.

Time

- HH - The hour at which to reload. (Range: 00-23)
- MM - The minute at which to reload. (Range: 00-59)

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)

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 28: Restarting the Switch (Immediately)

System > Reset

System Reload Information:
No configured settings for reloading.

System Reload Configuration:
Reset Mode

Message from webpage

Do you want to reset the switch immediately?

Figure 29: Restarting the Switch (In)

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.

System Reload Configuration:
Reset Mode

Reload switch in hours minutes.

Note: The specified time must be equal to or less than 24 days.

Figure 30: 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.

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

Figure 31: Restarting the Switch (Regularly)

System > Reset

System Reload Information:
No configured settings for reloading.

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

Interface Configuration

This chapter describes the following topics:

- ◆ [Port Configuration](#) – Configures connection settings, including auto-negotiation, or manual setting of speed, duplex mode, and flow control.
- ◆ [Displaying Statistics](#) – Shows Interface, Etherlike, and RMON port statistics in table or chart form.
- ◆ [Displaying Statistical History](#) – Displays statistical history for the specified interfaces.
- ◆ [Displaying Transceiver Data](#) – Displays identifying information, and operational parameters for optical transceivers which support DDM.
- ◆ [Configuring Transceiver Thresholds](#) – Configures thresholds for alarm and warning messages for optical transceivers which support DDM.
- ◆ [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.
- ◆ [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.
- ◆ [Traffic Segmentation](#) – Configures the uplinks and down links to a segmented group of ports.

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.

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.



Note: Auto-negotiation is not supported for 1000BASE SFP transceivers.

Parameters

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Type** – Indicates the port type. (1000BASE-T or 1000BASE 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)
- ◆ **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.
- **1000f** - Supports 1000 Mbps full-duplex operation.
- **Sym** - Symmetric exchange of 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;

Advertised capabilities for

1000BASE-T – 10half, 10full, 100half, 100full, 1000full

1000BASE-SX/LX/LHX/ZX (SFP) – 1000full

- ◆ **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. (Default: Enabled)
- ◆ **Link Up Down Trap** – Issues a notification message whenever a port link is established or broken. (Default: Disabled)

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.
4. Click Apply.

Figure 32: Configuring Connections by Port List

The screenshot shows the 'Interface > Port > General' configuration page. At the top, there is a breadcrumb trail and an 'Action:' dropdown menu set to 'Configure by Port List'. Below this, a 'Port List' section shows 'Total: 28' ports. A table displays the configuration for three ports (1, 2, and 3). Each port is of type '1000BASE-T' and has its 'Admin' status set to 'Enabled'. The 'Autonegotiation' section for each port shows 'Enabled' with checkboxes for '10h', '100h', '1000f', and '10f' all checked, and 'Sym' unchecked. The 'Speed Duplex' is set to '100full'. The 'Flow Control' is set to 'Enabled'. The 'Link Up Down Trap' is also set to 'Enabled'.

Port	Type	Name	Admin	Autonegotiation	Speed Duplex	Flow Control	Link Up Down Trap
1	1000BASE-T		Enabled	☒ Enabled ☒ 10h ☒ 100h ☒ 1000f ☐ FC ☒ 10f ☒ 100f ☐ Sym	100full	Enabled	Enabled
2	1000BASE-T		Enabled	☒ Enabled ☒ 10h ☒ 100h ☒ 1000f ☐ FC ☒ 10f ☒ 100f ☐ Sym	100full	Enabled	Enabled
3	1000BASE-T		Enabled	☒ Enabled ☒ 10h ☒ 100h ☒ 1000f ☐ FC ☒ 10f ☒ 100f ☐ Sym	100full	Enabled	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.

Parameters

Except for the trap command, refer to [“Configuring by Port List” on page 138](#) for more information on command usage and a description of the parameters.

Web Interface

To configure port connection parameters:

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

Figure 33: Configuring Connections by Port Range

Interface > Port > General

Action: Configure by Port Range ▼

Port Range (1-28) 1-28

Admin ☒ Enabled

Autonegotiation ☒ Enabled

☐ 10h ☐ 100h ☐ 1000f ☐ FC

☐ 10f ☐ 100f ☐ Sym

Speed Duplex 10half ▼

Flow Control ☒ Enabled

Link Up Down Trap ☒ 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.

Parameters

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Type** – Indicates the port type. (1000BASE-T or 1000BASE SFP)
- ◆ **Name** – Interface label.
- ◆ **Admin** – Shows if the port is enabled or disabled.
- ◆ **Oper Status** – Indicates if the link is Up or Down.
- ◆ **Shutdown Reason** – Shows the reason this interface has been shut down if applicable. Some of the reasons for shutting down an interface include being administratively disabled, or exceeding traffic boundary limits set by auto traffic control.
- ◆ **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.
- ◆ **Link Up Down Trap** – Shows if a notification message will be sent whenever a port link is established or broken. (Default: Enabled)

Web Interface

To display port connection parameters:

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

Figure 34: Displaying Port Information

Interface > Port > General

Action: Show Information ▼

Port List Total: 28

Port	Type	Name	Admin	Oper Status	Shutdown Reason	Autonegotiation	Oper Speed Duplex	Oper Flow Control	Link Up Down Trap
1	1000BASE-T		Enabled	Up		Enabled	100full	None	Enabled
2	1000BASE-T		Enabled	Down		Enabled	1000full	None	Enabled
3	1000BASE-T		Enabled	Down		Enabled	1000full	None	Enabled
4	1000BASE-T		Enabled	Down		Enabled	1000full	None	Enabled
5	1000BASE-T		Enabled	Down		Enabled	1000full	None	Enabled

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.

Parameters

These parameters are displayed:

Table 8: 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.

Table 8: Port Statistics (Continued)

Parameter	Description
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.
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.

Table 8: Port Statistics (Continued)

Parameter	Description
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 Byte 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	
<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.

Table 8: Port Statistics (Continued)

Parameter	Description
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 to update the screen.

Figure 35: Showing Port Statistics (Table)

The screenshot shows the 'Interface > Port > Statistics' page. The 'Mode' is set to 'Interface', 'Port' is '1', and 'Auto-refresh' is unchecked. The 'Interface Statistics' table is displayed with the following data:

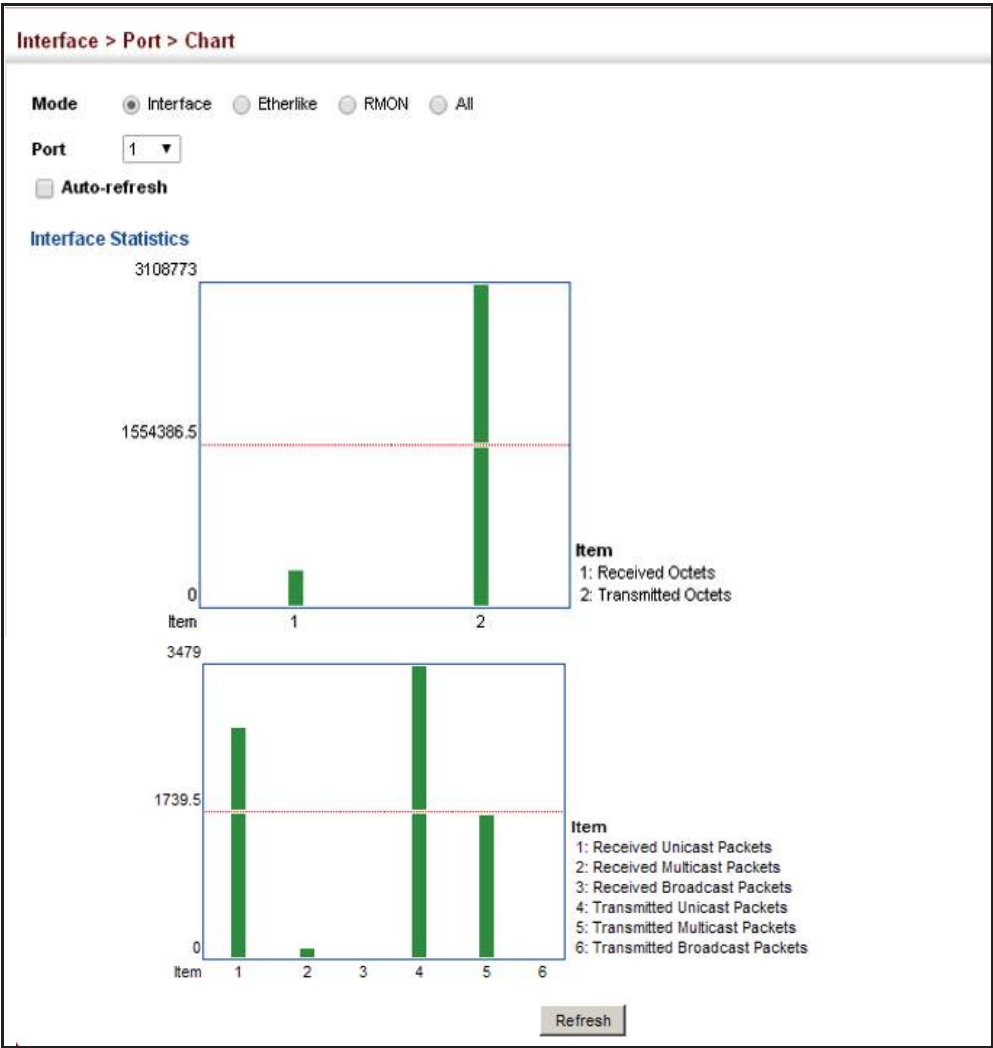
Interface Statistics	
Received Octets	1087697
Received Errors	0
Received Unicast Packets	5342
Received Discarded Packets	0
Received Multicast Packets	3692
Received Broadcast Packets	145
Received Unknown Packets	0
Transmitted Octets	5274231
Transmitted Errors	0
Transmitted Unicast Packets	6891
Transmitted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

A 'Refresh' button is located at the bottom right of the statistics table.

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 36: Showing Port Statistics (Chart)



Displaying Statistical History Use the Interface > Port > History or Interface > Trunk > History page to display statistical history for the specified interfaces.

Command Usage

- ◆ For a description of the statistics displayed on these pages, see “Showing Port or Trunk Statistics” on page 142.
- ◆ To configure statistical history sampling, use the “Displaying Statistical History” on page 146.

Parameters

These parameters are displayed:

Add

- ◆ **Port** – Port number. (Range: 1-28)

- ◆ **History Name** – Name of sample interval. (Range: 1-32 characters)
- ◆ **Interval** - The interval for sampling statistics. (Range: 1-86400 minutes)
- ◆ **Requested Buckets** - The number of samples to take. (Range: 1-96)

Show

- ◆ **Port** – Port number. (Range: 1-28)
- ◆ **History Name** – Name of sample interval. (Default settings: 15min, 1day)
- ◆ **Interval** - The interval for sampling statistics.
- ◆ **Requested Buckets** - The number of samples to take.

Show Details

- ◆ **Mode**
 - **Status** – Shows the sample parameters.
 - **Current Entry** – Shows current statistics for the specified port and named sample.
 - **Input Previous Entries** – Shows statistical history for ingress traffic.
 - **Output Previous Entries** – Shows statistical history for egress traffic.
- ◆ **Port** – Port number. (Range: 1-28)
- ◆ **Name** – Name of sample interval.

Web Configuration

To configure a periodic sample of statistics:

1. Click Interface, Port, Statistics, or Interface, Trunk, Statistics.
2. Select Add from the Action menu.
3. Select an interface from the Port or Trunk list.
4. Enter the sample name, the interval, and the number of buckets requested.
5. Click Apply.

Figure 37: Configuring a History Sample

Interface > Port > History

Action: Add

Port: 1

History Name: rd#1

Interval (1-86400): 60

Requested Buckets (1-96): 50

Apply Revert

To show the configured entries for a history sample:

1. Click Interface, Port, Statistics, or Interface, Trunk, Statistics.
2. Select Show from the Action menu.
3. Select an interface from the Port or Trunk list.

Figure 38: Showing Entries for History Sampling

Interface > Port > History

Action: Show

Port: 1

History Name List Total: 3

	History Name	Interval	Requested Buckets
☐	15min	900	96
☐	1day	86400	7
☐	rd#1	60	50

Delete Revert

To show the configured parameters for a sampling entry:

1. Click Interface, Port, Statistics, or Interface, Trunk, Statistics.
2. Select Show Details from the Action menu.
3. Select Status from the options for Mode.
4. Select an interface from the Port or Trunk list.
5. Select an sampling entry from the Name list.

Figure 39: Showing Status of Statistical History Sample

Interface > Port > History

Action: Show Details

Mode ☒ Status ☐ Current Entry ☐ Input Previous Entries ☐ Output Previous Entries

Port 1

Name 15min

History Status

Name	15min
Interval	15 minute(s)
Requested Buckets	96
Granted Buckets	35
Status	Active

Refresh

To show statistics for the current interval of a sample entry:

1. Click Interface, Port, Statistics, or Interface, Trunk, Statistics.
2. Select Show Details from the Action menu.
3. Select Current Entry from the options for Mode.
4. Select an interface from the Port or Trunk list.
5. Select an sampling entry from the Name list.

Figure 40: Showing Current Statistics for a History Sample

Interface > Port > History

Action: Show Details

Mode ☐ Status ☒ Current Entry ☐ Input Previous Entries ☐ Output Previous Entries

Port 1

Name 15min

Current Entry

Start Time	00d 08:45:09		
Received Octets	114377	Transmitted Octets	408498
Received Errors	0	Transmitted Errors	0
Received Unicast Packets	504	Transmitted Unicast Packets	589
Received Discarded Packets	0	Transmitted Discarded Packets	0
Received Multicast Packets	412	Transmitted Multicast Packets	25
Received Broadcast Packets	8	Transmitted Broadcast Packets	0
Received Unknown Packets	0		

Refresh

To show ingress or egress traffic statistics for a sample entry:

1. Click Interface, Port, Statistics, or Interface, Trunk, Statistics.
2. Select Show Details from the Action menu.
3. Select Input Previous Entry or Output Previous Entry from the options for Mode.
4. Select an interface from the Port or Trunk list.
5. Select an sampling entry from the Name list.

Figure 41: Showing Ingress Statistics for a History Sample

Interface > Port > History

Action: Show Details

Mode: ☐ Status ☐ Current Entry ☒ Input Previous Entries ☐ Output Previous Entries

Port: 1

Name: 15min

Input Previous Entry List Total: 16

Start Time	%	Octets	Unicast	Multicast	Broadcast	Discarded	Errors	Unknown Proto
00d 00:00:0	0.00	9401	0	40	36	24	0	0
00d 00:15:0	0.00	3246	0	30	9	9	0	0
00d 00:30:0	0.00	2999	0	30	8	8	0	0
00d 00:45:0	0.00	3863	0	30	17	17	0	0
00d 01:00:0	0.00	3511	0	29	14	14	0	0
00d 01:15:0	0.00	3246	0	30	9	9	0	0
00d 01:30:0	0.00	2999	0	30	8	8	0	0
00d 01:45:0	0.00	2999	0	30	8	8	0	0
00d 02:00:0	0.00	3575	0	30	14	14	0	0
00d 02:15:0	0.00	3246	0	30	9	9	0	0

Refresh

Displaying Transceiver Data

Use the Interface > Port > Transceiver page to display identifying information, and operational for optical transceivers which support Digital Diagnostic Monitoring (DDM).

Parameters

These parameters are displayed:

- ◆ **Port** – Port number. (Range: 25-28)
- ◆ **General** – Information on connector type and vendor-related parameters.
- ◆ **DDM Information** – Information on temperature, supply voltage, laser bias current, laser power, and received optical power.

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

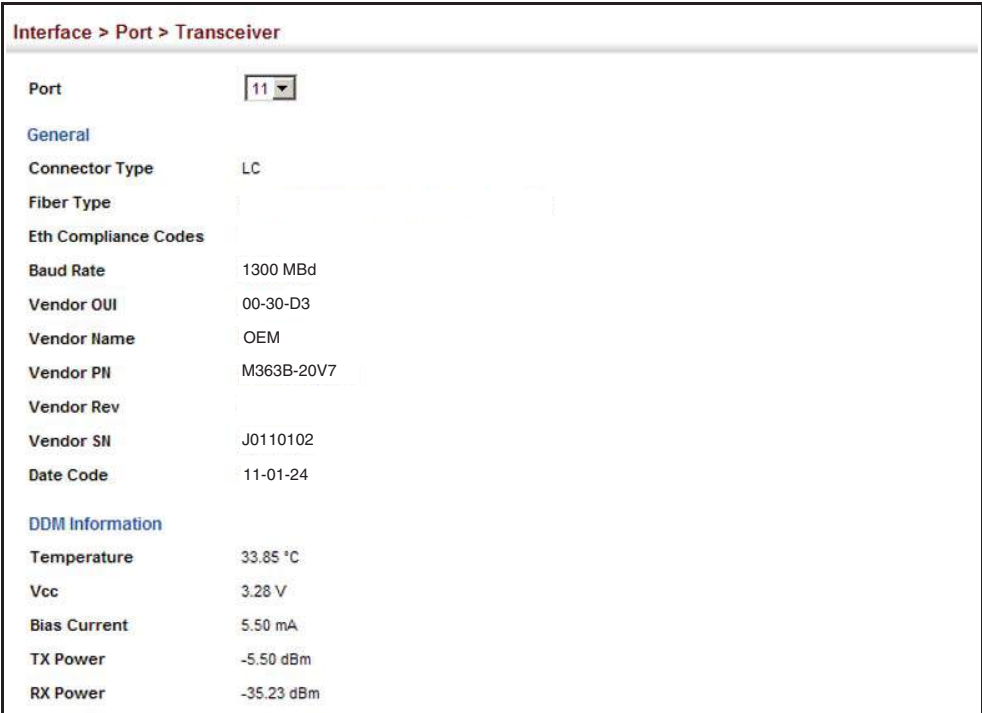
problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) provides information on transceiver parameters.

Web Interface

To display identifying information and functional parameters for optical transceivers:

1. Click Interface, Port, Transceiver.
2. Select a port from the scroll-down list.

Figure 42: Displaying Transceiver Data



Configuring Transceiver Thresholds

Use the Interface > Port > Transceiver page to configure thresholds for alarm and warning messages for optical transceivers which support Digital Diagnostic Monitoring (DDM). This page also displays identifying information for supported transceiver types, and operational parameters for transceivers which support DDM.

Parameters

These parameters are displayed:

- ◆ **Port** – Port number. (Range: 25-28)
- ◆ **General** – Information on connector type and vendor-related parameters.
- ◆ **DDM Information** – Information on temperature, supply voltage, laser bias current, laser power, and received optical power.

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) provides information on transceiver parameters.

- ◆ **Trap** – Sends a trap when any of the transceiver's operation values falls outside of specified thresholds. (Default: Disabled)
- ◆ **Auto Mode** – Uses default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent. (Default: Enabled)
- ◆ **DDM Thresholds** – Information on alarm and warning thresholds. The switch can be configured to send a trap when the measured parameter falls outside of the specified thresholds.

The following alarm and warning parameters are supported:

- **High Alarm** – Sends an alarm message when the high threshold is crossed.
- **High Warning** – Sends a warning message when the high threshold is crossed.
- **Low Warning** – Sends a warning message when the low threshold is crossed.
- **Low Alarm** – Sends an alarm message when the low threshold is crossed.

The configurable ranges are:

- **Temperature:** -128.00-128.00 °C
- **Voltage:** 0.00-6.55 Volts
- **Current:** 0.00-131.00 mA
- **Power:** -40.00-8.20 dBm

The threshold value for Rx and Tx power is calculated as the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).

Threshold values for alarm and warning messages can be configured as described below.

- A high-threshold alarm or warning message is sent if the current value is greater than or equal to the threshold, and the last sample value was less than the threshold. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the high threshold and reaches the low threshold.
- A low-threshold alarm or warning message is sent if the current value is less than or equal to the threshold, and the last sample value was greater than the threshold. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the low threshold and reaches the high threshold.

- Threshold events are triggered as described above to avoid a hysteresis effect which would continuously trigger event messages if the power level were to fluctuate just above and below either the high threshold or the low threshold.
- Trap messages configured by this command are sent to any management station configured as an SNMP trap manager using the Administration > SNMP (Configure Trap) page.

Web Interface

To configure threshold values for optical transceivers:

1. Click Interface, Port, Transceiver.
2. Select a port from the scroll-down list.
3. Set the switch to send a trap based on default or manual settings.
4. Set alarm and warning thresholds if manual configuration is used.
5. Click Apply.

Figure 43: Configuring Transceiver Thresholds

DDM Thresholds

☐ Trap

☐ Auto Mode

	High Alarm	High Warning	Low Warning	Low Alarm
Temperature(°C)	75.00	70.00	0.00	-123.00
Voltage(Volts)	3.50	3.45	3.15	3.10
Current(mA)	100.00	90.00	7.00	6.00
Tx Power(dBm)	-9.00	-9.50	-11.50	-12.00
Rx Power(dBm)	-3.00	-3.50	-21.00	-21.50

[Click this button to restore default DDM thresholds values.](#)

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 16 trunks at a time on the switch, or up to 32 across the stack.

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.

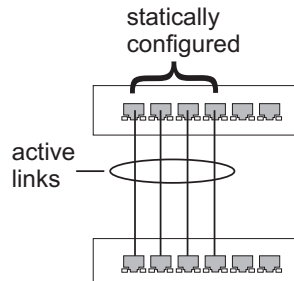
Command Usage

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 trunk, take note of the following points:

- ◆ Finish configuring 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 or 32 trunks in the stack, 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 44: Configuring Static Trunks



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: 1-8)
- ◆ **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)

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 45: Creating Static Trunks

Interface > Trunk > Static

Step: 1. Configure Trunk Action: Add

Trunk ID (1-8)

Member Unit 1 Port 1

Apply 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 46: Adding Static Trunks Members

Interface > Trunk > Static

Step: 1. Configure Trunk Action: Add

Trunk ID (1-8)

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 138](#) for a description of the parameters.)
5. Click Apply.

Figure 47: 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	Link Up Down Trap
1	1000BASE-T		☒ Enabled	☒ Enabled ☒ 10h ☒ 100h ☒ 1000f ☒ 10f ☒ 100f ☐ Sym	☐ FC 100full	☐ Enabled	☒ 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 48: Showing Information for Static Trunks

Interface > Trunk > Static

Step: 2. Configure General Action: Show Information

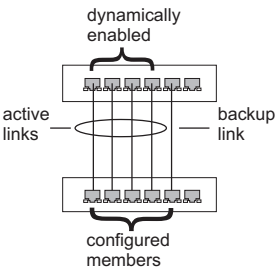
Static Trunk List Total: 1

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

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 49: Configuring Dynamic Trunks



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 on [page 796](#)).

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)

If the port channel admin key 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 (see *Configure Aggregation Port - Actor/Partner*) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

If the port channel admin key is set to a non-default value, the operational key is based upon LACP PDUs received from the partner, and the channel admin key is reset to the default value. The trunk identifier will also be changed by this process.

- ◆ **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 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.

- ◆ **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.
- ◆ **System MAC Address** – The device MAC address assigned to each trunk.

Configure Aggregation Port - General

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

Configure Aggregation Port - Actor/Partner

- ◆ **Port** – Port number. (Range: 1-28)
- ◆ **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)

Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state.



Note: Configuring the partner admin-key does not affect remote or local switch operation. The local switch just records the partner admin-key for user reference.

By default, the actor's operational key is determined by port's link speed (1000f - 4, 100f - 3, 10f - 2), and copied to the admin key.

- ◆ **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 50: Configuring the LACP Aggregator Admin Key

Interface > Trunk > Dynamic

Step: 1. Configure Aggregator

Trunk List Total: 8

Trunk	Admin Key (0-65535)	Timeout Mode	System Priority	System MAC Address
1	0	Long Timeout	32768	00-E0-0C-00-00-FD
2	0	Long Timeout	32768	00-E0-0C-00-00-FD
3	0	Long Timeout	32768	00-E0-0C-00-00-FD
4	0	Long Timeout	32768	00-E0-0C-00-00-FD
5	0	Long Timeout	32768	00-E0-0C-00-00-FD

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 51: 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	☐ Enabled
2	☒ Enabled
3	☐ Enabled
4	☐ Enabled
5	☐ 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 52: 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 53: 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 138](#) for a description of the interface settings.)
5. Click Apply.

Figure 54: Configuring Connection Settings for a Dynamic Trunk

Trunk	Type	Name	Admin	Autonegotiation	Speed Duplex	Flow Control	Link Up Down Trap
1	1000BASE-T		Enabled	Enabled	100full	Enabled	Enabled

To show 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 55: Showing Connection Parameters for Dynamic Trunks

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

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

Parameters

These parameters are displayed:

Table 9: 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 56: 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.

Parameters

These parameters are displayed:

Table 10: 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.

Table 10: LACP Internal Configuration Information (Continued)

Parameter	Description
Admin State, Oper State	Administrative or operational values of the actor's state parameters: ◆ 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)

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 57: 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.

Parameters

These parameters are displayed:

Table 11: 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 58: Displaying LACP Port Remote Information

Port Neighbors Information	
Partner Admin System ID	32768, 00-11-3B-11-22-33
Partner Oper System ID	32768, 00-11-3B-11-22-44
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

Configuring Load Balancing

Use the Interface > Trunk > Load Balance page to set the load-distribution method used among ports in aggregated links.

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:
 - **Destination IP Address:** 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.

- **Destination MAC Address:** 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.
- **Source and Destination IP Address:** 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.
- **Source and Destination MAC Address:** 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.
- **Source IP Address:** 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.
- **Source MAC Address:** 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.

Parameters

These parameters are displayed for the load balance mode:

- ◆ **Destination IP Address** - Load balancing based on destination IP address.
- ◆ **Destination MAC Address** - Load balancing based on destination MAC address.
- ◆ **Source and Destination IP Address** - Load balancing based on source and destination IP address.
- ◆ **Source and Destination MAC Address** - Load balancing based on source and destination MAC address.
- ◆ **Source IP Address** - Load balancing based on source IP address.
- ◆ **Source MAC Address** - Load balancing based on source MAC address.

Web Interface

To display the load-distribution method used by ports in aggregated links:

1. Click Interface, Trunk, Load Balance.
2. Select the required method from the Load Balance Mode list.
3. Click Apply.

Figure 59: Configuring Load Balancing



Saving Power

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

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 (entering Sleep Mode). In this mode, the low-power energy-detection circuit continuously checks for energy on the cable. If none is detected, the MAC interface is also powered down to save additional energy. If energy is detected, the switch immediately turns on both the transmitter and receiver functions, and powers up the MAC interface.
 - Power saving when there is a link partner:
Traditional Ethernet connections typically operate with enough power to support at least 100 meters of cable even though average network cable

length is shorter. When cable length is shorter, power consumption can be reduced since signal attenuation is proportional to cable length. When power-savings mode is enabled, the switch analyzes cable length to determine whether or not it can reduce the signal amplitude used on a particular link.



Note: Power savings can only be implemented on Gigabit Ethernet ports 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. (Range: 1-24)
- ◆ **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.

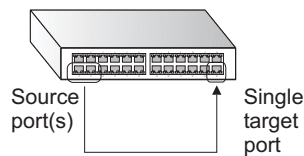
Figure 60: Enabling Power Savings

Port	Power Saving Status
21	☒ Enabled
22	☒ Enabled
23	☒ Enabled
24	☒ Enabled
25	☐ Enabled
26	☐ Enabled
27	☐ Enabled
28	☐ Enabled

Configuring Local Port Mirroring

Use the Interface > 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 61: Configuring Local Port Mirroring



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 172](#)).
- ◆ Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- ◆ 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, 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 62: Configuring Local Port Mirroring

Interface > Mirror

Action: Show ▼

Source Port Unit 1 ▼ Port 1 ▼

Target Port Unit 1 ▼ Port 1 ▼

Type Both ▼

Apply Revert

To display the configured mirror sessions:

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

Figure 63: Displaying Local Port Mirror Sessions

Interface > Mirror

Action: Show ▼

Mirror Session List Total: 2

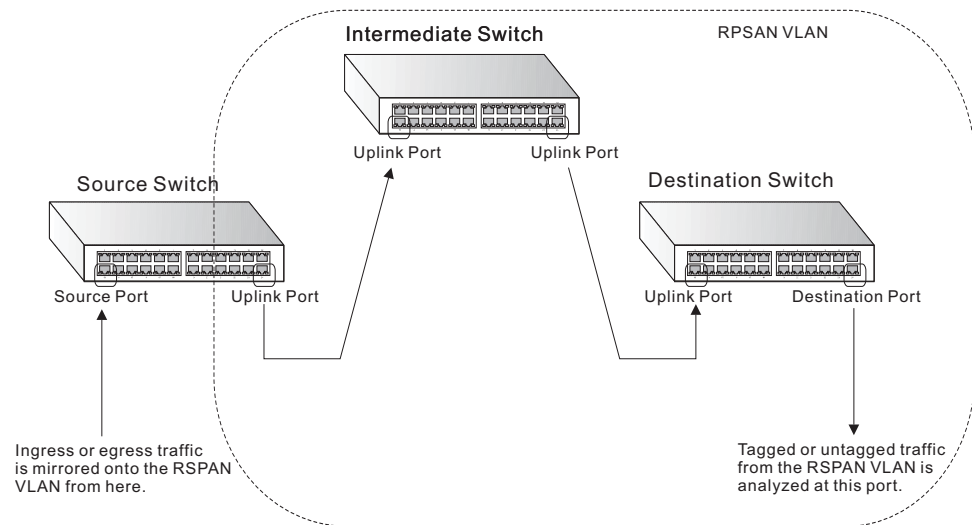
	Source (Unit/Port)	Target (Unit/Port)	Type
☐	1 / 7	1 / 8	Both
☐	1 / 9	1 / 10	Both

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 64: Configuring Remote Port Mirroring



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 171](#)), 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 184](#)) 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 port¹. 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 port¹, 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.

1. 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 186](#)).

◆ *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.
- *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: 1-3)
Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.
- ◆ **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 184](#)).
- ◆ **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 ports¹ 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 port¹ 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 65: Configuring Remote Port Mirroring (Source)

Interface > RSPAN

Session: 1

Operation Status: Up

Switch Role: Source

Remote VLAN: 2

Uplink Port: 4

Source Port Configuration List Total: 28

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

Figure 66: 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	☐
2	☐
3	☐
4	☒
5	☐

Figure 67: 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	☐
2	☐
3	☐
4	☒
5	☐

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.

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 68: Enabling Traffic Segmentation

Interface > Traffic Segmentation

Step: 1. Configure Global

Status ☐ Enabled

Uplink-to-Uplink Mode Blocking

Apply 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.

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 12: 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 177](#)).

- ◆ 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)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-8)

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.

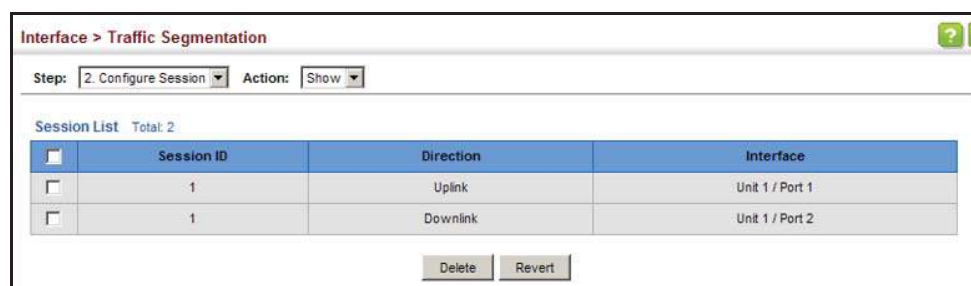
Figure 69: Configuring Members for Traffic Segmentation

The screenshot shows a web interface titled "Interface > Traffic Segmentation". At the top, there are two dropdown menus: "Step:" with "2. Configure Session" selected, and "Action:" with "Add" selected. Below these, there are three main configuration sections: "Session ID (1-4)" with a text input field; "Direction" with a dropdown menu showing "Uplink"; and "Interface" with two radio button options. The "Port (1-28)" option is selected, followed by a text input field and a hyphen. The "Trunk (1-8)" option is unselected, followed by a text input field and a hyphen. At the bottom right, there are two buttons: "Apply" and "Revert".

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 70: Showing Traffic Segmentation Members



Interface > Traffic Segmentation

Step: 2. Configure Session Action: Show

Session List Total: 2

	Session ID	Direction	Interface
☐	1	Uplink	Unit 1 / Port 1
☐	1	Downlink	Unit 1 / Port 2

Delete Revert

6

VLAN Configuration

This chapter includes the following topics:

- ◆ **IEEE 802.1Q VLANs** – Configures static and dynamic VLANs.
- ◆ **Protocol VLANs²** – Configures VLAN groups based on specified protocols.
- ◆ **MAC-based VLANs²** – Maps untagged ingress frames to a specified VLAN if the source MAC address is found in the IP MAC address-to-VLAN mapping table.

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.

2. If a packet matches the rules defined by more than one of these functions, only one of them is applied, with the precedence being MAC-based, protocol-based, and then native port-based.

This switch supports the following VLAN features:

- ◆ Up to 4094 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

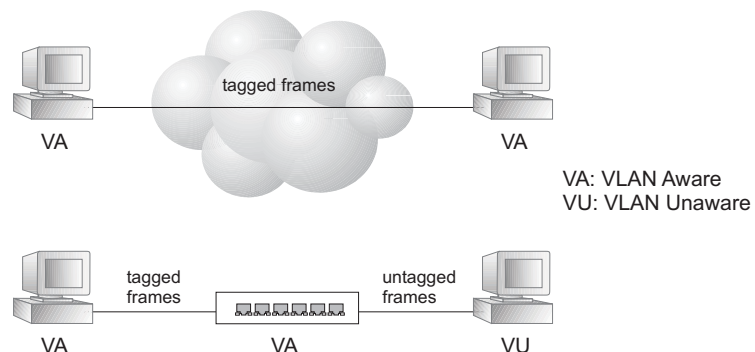
Assigning Ports to VLANs

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 71: 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 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.

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 172](#)). 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.

Parameters

These parameters are displayed:

Add

- ◆ **VLAN ID** – ID of VLAN or range of VLANs (1-4094).
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 172](#)).

Modify

- ◆ **VLAN ID** – ID of configured VLAN (1-4094).
- ◆ **VLAN Name** – Name of the VLAN (1 to 32 characters).
- ◆ **Status** – Enables or disables the specified 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 172](#)).

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. Check Status to configure the VLAN as operational.
5. Specify whether the VLANs are to be used for remote port mirroring.

6. Click Apply.

Figure 72: Creating Static VLANs

VLAN > Static

Action: Add

VLAN ID (1-4094): 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 or operational status as required.
5. Enable the L3 Interface field to specify that a VLAN will be used as a Layer 3 interface.
6. Click Apply.

Figure 73: Modifying Settings for Static VLANs

VLAN > Static

Action: Modify

VLAN ID (1-4094): 1

VLAN Name: DefaultVlan

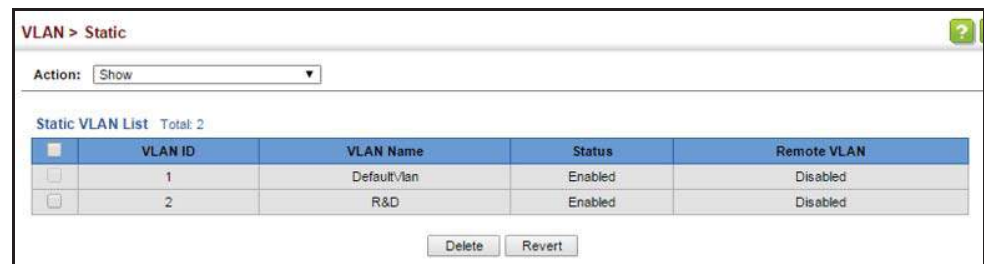
Status: ☒ Enabled

Apply Revert

To show the configuration settings for VLAN groups:

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

Figure 74: Showing Static VLANs



The screenshot shows the 'VLAN > Static' configuration page. At the top, there is a breadcrumb 'VLAN > Static' and a green help icon. Below this is an 'Action:' dropdown menu set to 'Show'. The main content area is titled 'Static VLAN List Total: 2'. It contains a table with the following data:

	VLAN ID	VLAN Name	Status	Remote VLAN
☐	1	DefaultVlan	Enabled	Disabled
☐	2	R&D	Enabled	Disabled

At the bottom of the table, there are 'Delete' and 'Revert' buttons.

Adding Static Members to VLANs

Use the VLAN > Static (Edit Member by VLAN, Edit Member by Interface, or Edit Member by Interface Range) 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 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.

Parameters

These parameters are displayed:

Edit Member by VLAN

- ◆ **VLAN** – ID of configured VLAN (1-4094).
- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Port** – Port Identifier. (Range: 1-28)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-8)
- ◆ **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.
 - **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: Enabled)
 - 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 cannot be included as a member of the VLAN.
 - **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 using Hybrid mode.

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)

◆ **Trunk Range** – Displays a list of ports. (Range: 1-8)



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 Edit Member by VLAN from the Action list.
3. Select a VLAN from the scroll-down list.
4. Set the Interface type to display as Port or Trunk.
5. Modify the settings for any interface as required.
6. Click Apply.

Figure 75: 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 (1-4094), 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', 'All' frame type, and 'Enabled' ingress filtering. The 'Membership Type' for all ports is 'Untagged'.

Port	Mode	PVID (1-4094)	Acceptable Frame Type	Ingress Filtering	Membership Type			
					Tagged	Untagged	Forbidden	None
1	Hybrid	1	All	Enabled				
2	Hybrid	1	All	Enabled				
3	Hybrid	1	All	Enabled				
4	Hybrid	1	All	Enabled				
5	Hybrid	1	All	Enabled				

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 76: Configuring Static VLAN Members by Interface

The screenshot shows the 'VLAN > Static' configuration page. The 'Action' dropdown is set to 'Edit Member by Interface'. The 'Interface' section has 'Port' selected with a value of '1'. The 'Mode' is set to 'Hybrid', 'PVID' is '1', 'Acceptable Frame Type' is 'All', and 'Ingress Filtering' is 'Enabled'. Below this is the 'Static VLAN Membership List' with a total of 4 members. The table has columns for 'VLAN' and 'Membership Type' (Tagged, Untagged, Forbidden, None). Each row represents a VLAN with radio buttons for each membership type.

VLAN	Membership Type			
	Tagged	Untagged	Forbidden	None
1	☒	☐	☐	☐
2	☐	☐	☐	☒
3	☐	☐	☐	☒
4	☐	☐	☐	☒

At the bottom of the table are 'Apply' and 'Revert' buttons.

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 77: Configuring Static VLAN Members by Interface Range

The screenshot shows a web-based configuration interface for VLANs. The title bar reads "VLAN > Static". Below the title bar, there is a section labeled "Action:" with a dropdown menu set to "Edit Member by Interface Range". The main configuration area contains several fields: "Interface" with radio buttons for "Port" (selected) and "Trunk"; "Port Range (1-28)" with two input boxes separated by a hyphen; "Mode" with a dropdown menu set to "Hybrid"; "VLAN ID (1-4093)" with two input boxes separated by a hyphen; and "Membership Type" with radio buttons for "Tagged" (selected), "Untagged", "Forbidden", and "None". At the bottom right of the form are "Apply" and "Revert" buttons.

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 (see ["Configuring VLAN Groups" on page 184](#)). 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, or 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.

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 78: 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 79: Displaying Protocol VLANs

VLAN > Protocol

Step: 1. Configure Protocol Action: Show

Protocol to Group Mapping Table Total: 5

	Frame Type	Protocol Type	Protocol Group ID
☐	Ethernet	08 06	1
☐	Ethernet	80 35	2
☐	RFC 1042	08 00	1
☐	RFC 1042	80 35	3
☐	LLC Other	FF FF	5

Delete Revert

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.

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 186), 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)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-8)
- ◆ **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: 1-4094)
- ◆ **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 80: Assigning Interfaces to Protocol VLANs

VLAN > Protocol

Step: 2. Configure Interface Action: Add

Interface ☒ Port 1 ☐ Trunk

Protocol Group ID 1

VLAN ID (1-4093)

Priority (0-7)

Apply Revert

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 81: Showing the Interface to Protocol Group Mapping

VLAN > Protocol

Step: 2. Configure Interface Action: Show

Interface ☒ Port 1 ☐ Trunk

Port To Protocol Group Mapping Table Total: 1

	Protocol Group ID	VLAN ID	Priority
☐	1	2	0

Delete Revert

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).

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, or 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.
- ◆ **Mask** – Identifies a range of MAC addresses. (Range: 00-00-00-00-00-00 to ff-ff-ff-ff-ff-ff)

The binary equivalent mask matching the characters in the front of the first non-zero character must all be 1s (e.g., 111, i.e., it cannot be 101 or 001...). A mask for the MAC address: 00-11-3B-11-22-33 translated into binary:
MAC: 00000000-01010000-01101110-00000000-01011111-10110001
could be: 11111111-11xxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx
So the mask in hexadecimal for this example could be:
ff-fx-xx-xx-xx-xx/ff-c0-00-00-00-00/ff-e0-00-00-00-00
- ◆ **VLAN** – VLAN to which ingress traffic matching the specified source MAC address is forwarded. (Range: 1-4094)
- ◆ **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, and a mask to indicate a range of addresses if required.
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 82: Configuring MAC-Based VLANs

VLAN > MAC-Based

Action: Add ▼

MAC Address:

Mask:

VLAN (1-4093):

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 83: Showing MAC-Based VLANs

VLAN > MAC-Based ?

Action: Show ▼

MAC-Based VLAN List Total: 1

	MAC Address	Mask	VLAN	Priority
☐	00-AB-CD-11-22-33	FF-FF-FF-FF-FF-FF	10	0

Delete Revert

Address Table Settings

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:

- ◆ [MAC Address Learning](#) – Enables or disables address learning on an interface.
- ◆ [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 Notification Traps](#) – Issue trap when a dynamic MAC address is added or removed.

Configuring MAC Address Learning

Use the [MAC Address > Learning Status](#) page to enable or disable MAC address learning on an interface.

Command Usage

- ◆ When MAC address learning is disabled, the switch immediately stops learning new MAC addresses on the specified interface. Only incoming traffic with source addresses stored in the static address table (see [“Setting Static Addresses” on page 199](#)) will be accepted as authorized to access the network through that interface.
- ◆ Dynamic addresses stored in the address table when MAC address learning is disabled are flushed from the system, and no dynamic addresses are subsequently learned until MAC address learning has been re-enabled. Any device not listed in the static address table that attempts to use the interface after MAC learning has been disabled will be prevented from accessing the switch.

- ◆ Also note that MAC address learning cannot be disabled if any of the following conditions exist:
 - 802.1X Port Authentication has been globally enabled on the switch (see “Configuring 802.1X Global Settings” on page 331).
 - Security Status (see “Configuring Port Security” on page 327) is enabled on the same interface.

Parameters

These parameters are displayed:

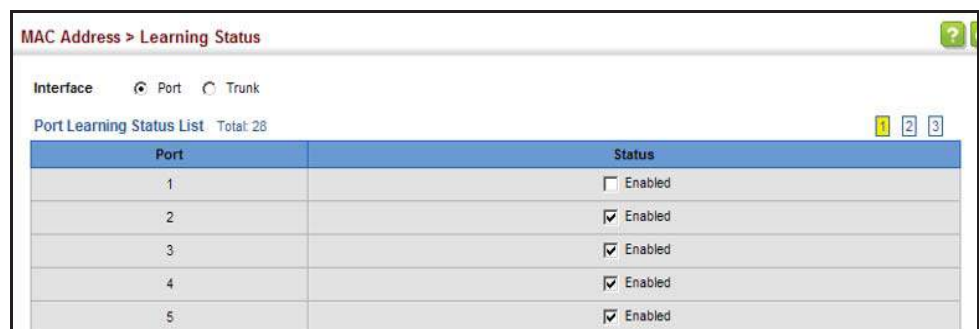
- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Port** – Port Identifier. (Range: 1-28)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-8)
- ◆ **Status** – The status of MAC address learning. (Default: Enabled)

Web Interface

To enable or disable MAC address learning:

1. Click MAC Address, Learning Status.
2. Set the learning status for any interface.
3. Click Apply.

Figure 84: Configuring MAC Address Learning



Port	Status
1	☐ Enabled
2	☒ Enabled
3	☒ Enabled
4	☒ Enabled
5	☒ Enabled

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.

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:

Add Static Address

- ◆ **VLAN** – ID of configured VLAN. (Range: 1-4094)
- ◆ **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.)

Show Static Address

The following additional fields are displayed on this web page:

Type – Displays the address configuration method. (Values: CPU, Config, or Security, the last of which indicates Port Security)

Life Time – The duration for which this entry applies. (Values: Delete On Reset, Delete On Timeout, Permanent)

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 85: Configuring Static MAC Addresses

MAC Address > Static

Action: Add

VLAN

1

Interface

Port 1

Trunk

MAC Address

00-11-3B-11-22-34

(xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)

Static Status

Permanent

Apply

Revert

To show the static addresses in MAC address table:

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

Figure 86: Displaying Static MAC Addresses

MAC Address > Static

Action: Show

Static MAC Address to Interface Mapping Table Total: 2

	MAC Address	VLAN	Interface	Type	Life Time
☐	00-11-3B-11-22-33	1	CPU	CPU	Delete on Reset
☐	00-11-3B-11-22-34	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.

Parameters

These parameters are displayed:

- ◆ **Aging Status** – Enables/disables the function.
- ◆ **Aging Time** – The time after which a learned entry is discarded. (Range: 6-7200 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 87: Setting the Address Aging Time

The screenshot shows the 'MAC Address > Dynamic' configuration page. At the top, the title 'MAC Address > Dynamic' is displayed. Below it, there is a dropdown menu labeled 'Action:' with 'Configure Aging' selected. The main configuration area contains two settings: 'Aging Status' with a checked checkbox labeled 'Enabled', and 'Aging Time (6-7200)' with a text input field containing '300' and a unit label 'sec'. At the bottom right of the form, there are two buttons: 'Apply' and '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.

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 (1-4094).
- ◆ **Interface** – Indicates a port or trunk.
- ◆ **Type** – Shows that the entries in this table are learned.
(Values: Learned or Security, the last of which indicates Port Security)
- ◆ **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 88: Displaying the Dynamic MAC Address Table

The screenshot shows the 'MAC Address > Dynamic' web interface. At the top, the 'Action' dropdown is set to 'Show Dynamic MAC'. Below this, the 'Query by:' section has a 'Sort Key' dropdown set to 'MAC Address'. There are checkboxes for 'MAC Address', 'VLAN', and 'Interface'. The 'VLAN' checkbox is selected, and its value is set to '1'. The 'Interface' checkbox is also selected, with 'Port' and 'Trunk' sub-options, both set to '1'. A 'Query' button is located below the search parameters. Below the query section, the 'Dynamic MAC Address List' is displayed with a 'Total: 2' count. The table has five columns: 'MAC Address', 'VLAN', 'Interface', 'Type', and 'Life Time'. It contains two rows of data, both with 'Learn' type and 'Delete on Timeout' life time.

MAC Address	VLAN	Interface	Type	Life Time
00-11-3B-11-22-33	1	Unit 1 / Port 1	Learn	Delete on Timeout
00-11-3B-11-22-34	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.

Parameters

These parameters are displayed:

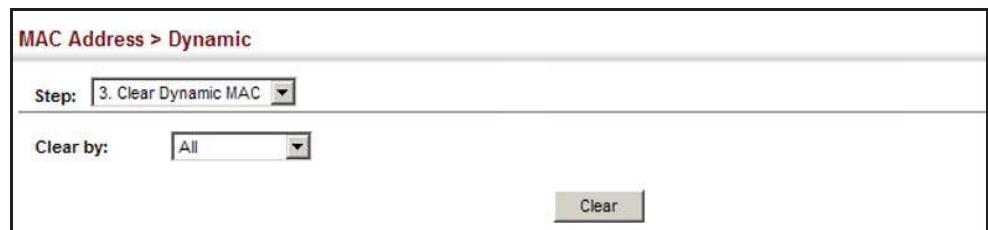
- ◆ **Clear by** – All entries can be cleared; or you can clear the entries for a specific MAC address, all the entries in a VLAN, or all the entries associated with a port or trunk.

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 89: Clearing Entries in the Dynamic MAC Address Table



The screenshot shows a web interface titled "MAC Address > Dynamic". Below the title, there is a "Step:" label followed by a dropdown menu showing "3. Clear Dynamic MAC". Below this, there is a "Clear by:" label followed by a dropdown menu showing "All". A "Clear" button is located at the bottom right of the form.

Issuing MAC Address Traps

Use the MAC Address > MAC Notification pages to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed.

Parameters

These parameters are displayed:

Configure Global

- ◆ **MAC Notification Traps** – Issues a trap when a dynamic MAC address is added or removed. (Default: Disabled)
- ◆ **MAC Notification Trap Interval** – Specifies the interval between issuing two consecutive traps. (Range: 1-3600 seconds; Default: 1 second)

Configure Interface

- ◆ **Port** – Port Identifier. (Range: 1-28)
- ◆ **MAC Notification Trap** – Enables MAC authentication traps on the current interface. (Default: Disabled)

MAC authentication traps must be enabled at the global level for this attribute to take effect.

Web Interface

To enable MAC address traps at the global level:

1. Click MAC Address, MAC Notification.
2. Select Configure Global from the Step list.
3. Configure MAC notification traps and the transmission interval.
4. Click Apply.

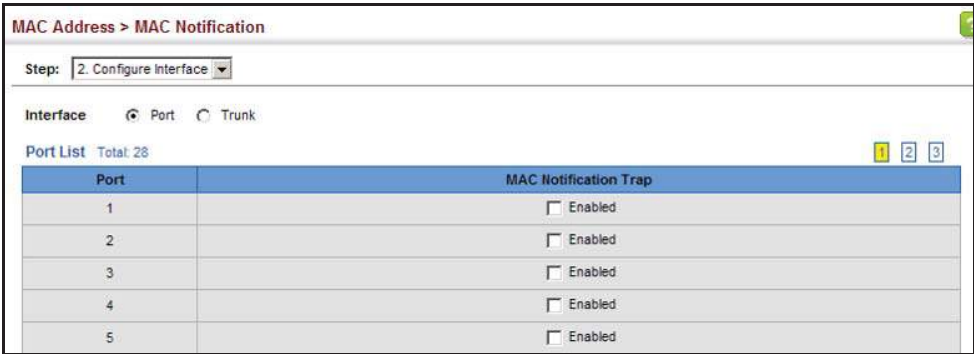
Figure 90: Issuing MAC Address Traps (Global Configuration)

The screenshot shows the 'MAC Address > MAC Notification' web interface. At the top, there is a breadcrumb trail 'MAC Address > MAC Notification'. Below it, a 'Step:' dropdown menu is set to '1. Configure Global'. The main configuration area contains two settings: 'MAC Notification Traps' with an 'Enabled' checkbox (currently unchecked), and 'MAC Notification Trap Interval (1-3600)' with a text input field containing the value '1' and a 'sec' label. At the bottom right of the form are two buttons: 'Apply' and 'Revert'.

To enable MAC address traps at the interface level:

- 1. Click MAC Address, MAC Notification.
- 2. Select Configure Interface from the Step list.
- 3. Enable MAC notification traps for the required ports.
- 4. Click Apply.

Figure 91: Issuing MAC Address Traps (Interface Configuration)



Spanning Tree Algorithm

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

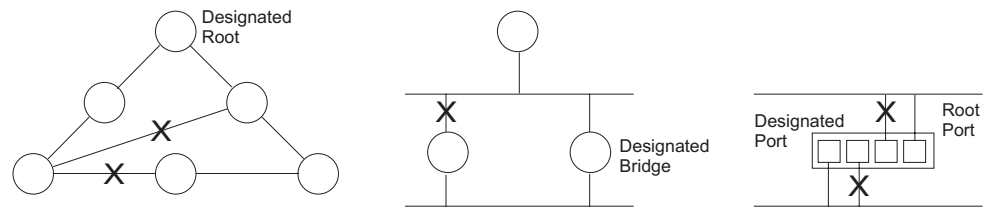
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only 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 92: STP Root Ports and Designated Ports

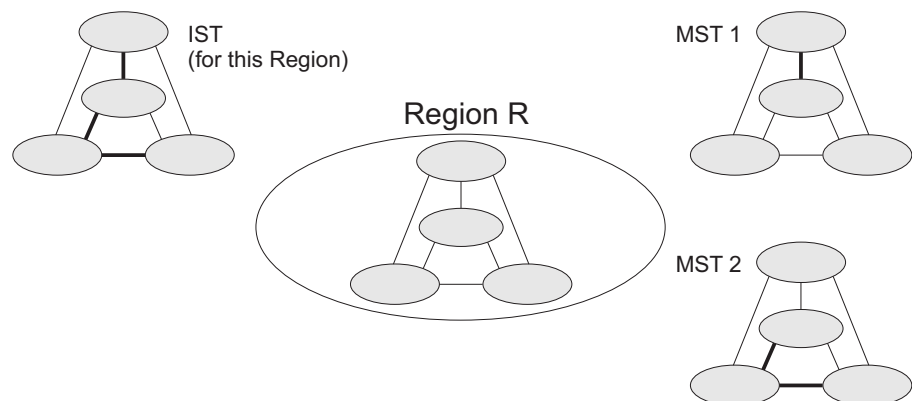


Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge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

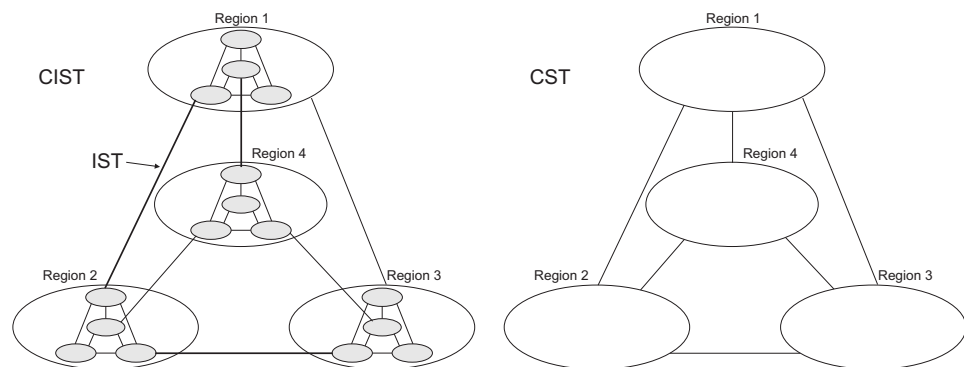
MSTP – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN 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 93: 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 224). 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 94: Spanning Tree – Common Internal, Common, Internal



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.

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 shut down the interface. (Default: Shutdown)
- ◆ **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.

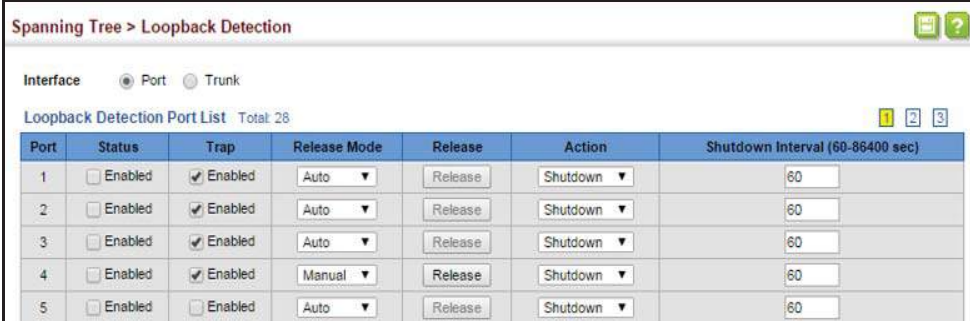
If an interface is shut down due to a detected loopback, and the release mode is set to “Manual,” the interface can be re-enabled using the Release button.

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 95: Configuring Port Loopback Detection



Port	Status	Trap	Release Mode	Release	Action	Shutdown Interval (60-86400 sec)
1	☐ Enabled	☒ Enabled	Auto	Release	Shutdown	60
2	☐ Enabled	☒ Enabled	Auto	Release	Shutdown	60
3	☐ Enabled	☒ Enabled	Auto	Release	Shutdown	60
4	☐ Enabled	☒ Enabled	Manual	Release	Shutdown	60
5	☐ Enabled	☐ Enabled	Auto	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.

Command Usage

◆ Spanning Tree Protocol³

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 Protocol³

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,

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

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.
- 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: Disabled)

When spanning tree is enabled globally or enabled on an interface ([Configuring Interface Settings for STA](#)), loopback detection is disabled.
- ◆ **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"](#)).

- ◆ **Cisco Prestandard Status** – Configures spanning tree operation to be compatible with Cisco prestandard versions. (Default: Disabled)

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. This command forces the spanning tree protocol to function in a manner compatible with Cisco prestandard versions.

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**⁴ – The revision for this MSTI. (Range: 0-65535; Default: 0)
- ◆ **Region Name**⁴ – The name for this MSTI. (Maximum length: 32 characters; Default: 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)



NOTE: Region Revision and Region Name are both required to uniquely identify an MST region.

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

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

Figure 96: Configuring Global Settings for STA (STP)

The screenshot shows the 'Spanning Tree > STA' configuration page. At the top, there is a 'Step:' dropdown set to '1. Configure Global' and an 'Action:' dropdown set to 'Configure'. The main configuration area includes the following settings:

- Spanning Tree Status:** ☒ Enabled
- Spanning Tree Type:** STP (selected from a dropdown)
- Priority (0-61440, in steps of 4096):** 32768
- BPDU Flooding:** To VLAN (selected from a dropdown)
- Cisco Prestandard Status:** ☐ Enabled
- Advanced:**
 - Path Cost Method:** Long (selected from a dropdown)
 - 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

Below these settings is a note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$. At the bottom right are 'Apply' and 'Revert' buttons.

Figure 97: Configuring Global Settings for STA (RSTP)

The screenshot shows the 'Spanning Tree > STA' configuration page, identical in layout to Figure 96 but with the 'Spanning Tree Type' set to RSTP. The settings are as follows:

- Spanning Tree Status:** ☒ Enabled
- Spanning Tree Type:** RSTP (selected from a dropdown)
- Priority (0-61440, in steps of 4096):** 32768
- BPDU Flooding:** To VLAN (selected from a dropdown)
- Cisco Prestandard Status:** ☐ Enabled
- Advanced:**
 - Path Cost Method:** Long (selected from a dropdown)
 - 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

The same note and buttons are present at the bottom.

Figure 98: 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

Cisco Prestandard Status

☐ Enabled

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

64

Configuration Digest

0xAC36177F50283CD4B83821D8AB26DE62

Region Revision (0-65535)

0

Region Name

00 E0 0C 00 00 FD

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.

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 99: 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.)

Parameters

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled)
When spanning tree is enabled globally ([Configuring Global Settings for STA](#)) or enabled on an interface by this command, loopback detection is disabled.
- ◆ **BPDU Flooding** – Enables/disables the flooding of BPDUs to other ports when global spanning tree is disabled ([page 210](#)) 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 210](#)). (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 method⁵, 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 802.1w standard exceeds 65,535, the default is set to 65,535.

Table 13: 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

5. Refer to "[Configuring Global Settings for STA](#)" on [page 210](#) for information on setting the path cost method. The range displayed on the STA interface configuration page shows the maximum value for path cost. However, note that the switch still enforces the rules for path cost based on the specified path cost method (long or short)

Table 13: Recommended STA Path Cost Range (Continued)

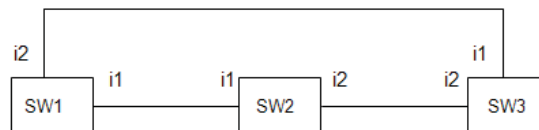
Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

Table 14: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (IEEE 802.1D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

Administrative path cost cannot be used to directly determine the root port on a switch. Connections to other devices use IEEE 802.1Q-2005 to determine the root port as in the following example.

Figure 100: Determining the Root Port



For BPDU messages received by i1 on SW3, the path cost is 0.

For BPDU messages received by i2 on SW3, the path cost is that of i1 on SW2.

The root path cost for i1 on SW3 used to compete for the role of root port is 0 + path cost of i1 on SW3; 0 since i1 is directly connected to the root bridge.

If the path cost of i1 on SW2 is never configured/changed, it is 10000.

Then the root path cost for i2 on SW3 used to compete for the role of root port is 10000 + path cost of i2 on SW3.

The path cost of i1 on SW3 is also 10000 if not configured/changed.

Then even if the path cost of i2 on SW3 is configured/changed to 0, these ports will still have the same root path cost, and it will be impossible for i2 to become the root port just by changing its path cost on SW3.

For RSTP mode, the root port can be determined simply by adjusting the path cost of i1 on SW2. However, for MSTP mode, it is impossible to achieve this only by changing the path cost because external path cost is not added in the same region, and the regional root for i1 is SW1, but for i2 is SW2.

◆ **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 210](#)).

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

- If spanning tree mode is set to STP ([page 210](#)), edge-port mode cannot automatically transition to operational edge-port state using the automatic setting.
- If loopback detection is enabled ([page 208](#)) 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 221](#)).

When edge port is set as auto, the operational state is determined automatically by the Bridge Detection State Machine described in 802.1D-2004, where the edge port state may change dynamically based on environment changes (e.g., receiving a BPDU or not within the required interval).

- ◆ **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 guard can only be configured on an interface if the edge port attribute is not disabled (that is, if edge port is set to enabled or auto).

- ◆ **BPDU Guard Auto Recovery** – Automatically re-enables an interface after the specified interval. (Range: 30-86400 seconds; Default: Disabled)
- ◆ **BPDU Guard Auto Recovery Interval** – The time to wait before re-enabling an interface. (Range: 30-86400 seconds; Default: 300 seconds)
- ◆ **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)

BPDU filter can only be configured on an interface if the edge port attribute is not disabled (that is, if edge port is set to enabled or auto).

- ◆ **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)
- ◆ **TC Propagate Stop** – Stops the propagation of topology change notifications (TCN). (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 101: 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's a tabbed interface with 'Port' selected. A 'Port List' section shows 'Total: 28'. The main table displays settings for 5 ports. Each row has columns for Port, Spanning Tree, BPDU Flooding, Priority, Admin Path Cost, Admin Link Type, Root Guard, Admin Edge Port, BPDU Guard, BPDU Guard Auto Recovery, BPDU Guard Auto Recovery Interval, BPDU Filter, Migration, and TC Propagate Stop. All settings are currently set to 'Enabled' or 'Auto'.

Port	Spanning Tree	BPDU Flooding	Priority (0-248, in steps of 16)	Admin Path Cost (0-250000000, 0: Auto)	Admin Link Type	Root Guard	Admin Edge Port	BPDU Guard	BPDU Guard Auto Recovery	BPDU Guard Auto Recovery Interval (30-86400)	BPDU Filter	Migration	TC Propagate Stop
1	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
2	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
3	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
4	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
5	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	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.

Parameters

These parameters are displayed:

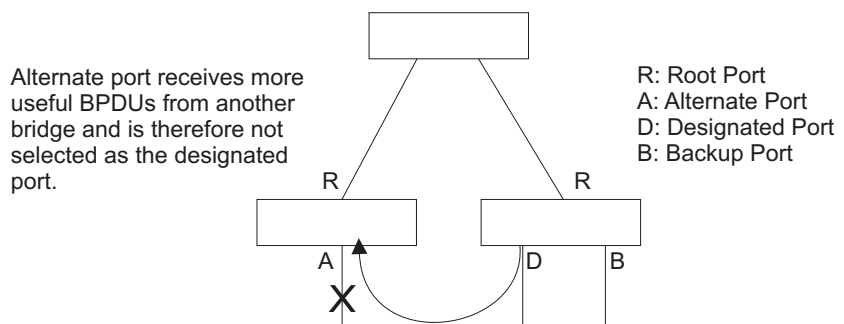
- ◆ **Spanning Tree** – Shows if STA has been enabled on this interface.
- ◆ **BPDU Flooding** – Shows if BPDUs will be flooded to other ports when spanning tree is disabled globally on the switch or disabled on a specific port.
- ◆ **STA Status** – Displays current state of this port within the Spanning 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.

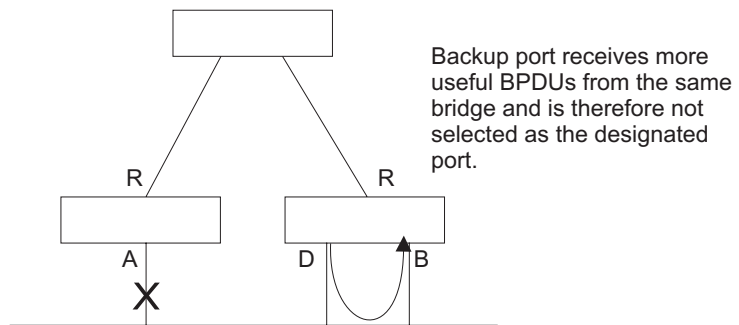
The rules defining port status are:

- 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 216](#).
- ◆ **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on [page 216](#) (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 102: STA Port Roles





The criteria used for determining the port role is based on root bridge ID, root path cost, designated bridge, designated port, port priority, and port number, in that order and as applicable to the role under question.

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 103: Displaying Interface Settings for STA

Spanning Tree > STA

Step: 2. Configure Interface Action: Show Information

Interface ☒ Port ☐ Trunk

Spanning Tree Port List Total: 28

123

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.

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 210](#)) 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 210](#)).
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: 1-4094)
- ◆ **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 104: Creating an MST Instance

The screenshot shows the 'Spanning Tree > MSTP' configuration page. At the top, there is a 'Step:' dropdown menu set to '1. Configure Global' and an 'Action:' dropdown menu set to 'Add'. Below these, there are three input fields: 'MST ID (0-4094)' with the value '1', 'VLAN ID (1-4094)' 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 105: Displaying MST Instances

The screenshot shows the 'Spanning Tree > MSTP' configuration page. At the top, there is a 'Step:' dropdown menu set to '1. Configure Global' and an 'Action:' dropdown menu set to 'Show'. Below these, there is a table titled 'MST List' with a 'Total: 2' indicator. The table has two columns: a checkbox column and an 'MST ID' column. The table contains two rows: one with MST ID '0' and one with MST ID '1'. At the bottom right, there are two buttons: 'Delete' and 'Revert'.

	MST ID
☐	0
☐	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 106: 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 a table titled '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 215](#).

Figure 107: 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 a dropdown for 'MST ID' set to '1'. The page displays various global settings for the selected MST ID in two columns.

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 108: Adding a VLAN to an MST Instance

Spanning Tree > MSTP

Step: 1. Configure Global Action: Add Member

MST ID 1

VLAN ID (1-4094) 1

Apply 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 109: Displaying Members of an MST Instance

Spanning Tree > MSTP

Step: 1. Configure Global Action: Show Member

MST ID 0

Member List Total: 4094

	VLAN
☐	1
☐	2
☐	3
☐	4
☐	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.

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 221](#) 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 210](#)), 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 13 on page 217](#).

The default path costs are listed in [Table 14 on page 218](#).

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 110: Configuring MSTP Interface Settings

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 111: Displaying MSTP Interface Settings

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

Congestion Control

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.

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.

Parameters

These parameters are displayed:

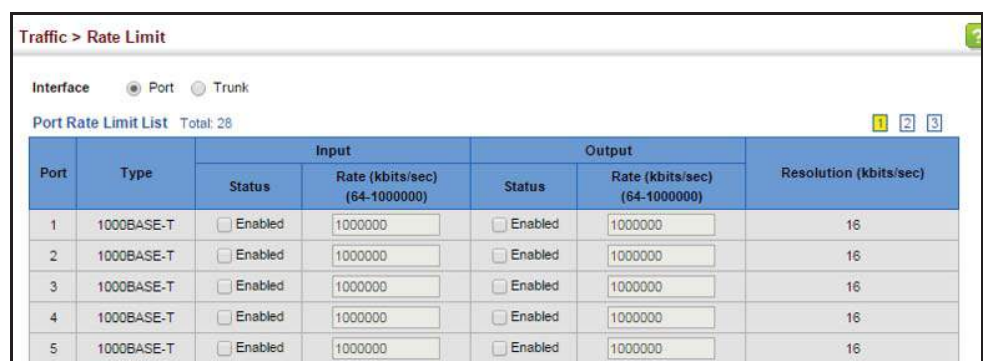
- ◆ **Interface** – Displays the switch's ports or trunks.
- ◆ **Type** – Indicates the port type. (1000BASE-T, 10GBASE SFP+, or 1000BASE SFP).
- ◆ **Status** – Enables or disables the rate limit. (Default: Disabled)
- ◆ **Rate** – Sets the rate limit level.
(Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports;
64 - 10,000,000 kbits per second for 10 Gigabit Ethernet ports)
- ◆ **Resolution** – Indicates the resolution at which the rate can be configured.

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 required interfaces.
5. Click Apply.

Figure 112: 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, it says 'Port Rate Limit List Total: 28'. The main part of the page is a table with columns for Port, Type, Input Status, Input Rate (kbits/sec), Output Status, Output Rate (kbits/sec), and Resolution (kbits/sec). The table lists five ports, all of type 1000BASE-T, with their status set to 'Enabled' and a rate limit of 1000000 kbits/sec. The resolution for all ports is 16 kbits/sec.

Port	Type	Input		Output		Resolution (kbits/sec)
		Status	Rate (kbits/sec) (64-1000000)	Status	Rate (kbits/sec) (64-1000000)	
1	1000BASE-T	☒ Enabled	1000000	☒ Enabled	1000000	16
2	1000BASE-T	☒ Enabled	1000000	☒ Enabled	1000000	16
3	1000BASE-T	☒ Enabled	1000000	☒ Enabled	1000000	16
4	1000BASE-T	☒ Enabled	1000000	☒ Enabled	1000000	16
5	1000BASE-T	☒ Enabled	1000000	☒ Enabled	1000000	16

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.

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.
- ◆ Using both rate limiting and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these features on the same interface.

Parameters

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Type** – Indicates the port type. (1000BASE-T or 1000BASE 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: Disabled)
- ◆ **Rate** – Threshold level in packets per second.
(Range: 500-262142 pps; Default: 500 pps)
- ◆ **Resolution** – Indicates the resolution at which the rate can be configured.

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 113: Configuring Storm Control

Port	Type	Unknown Unicast		Multicast		Broadcast		Resolution (packets/sec)
		Status	Rate (packets/sec) (500-262142)	Status	Rate (packets/sec) (500-262142)	Status	Rate (packets/sec) (500-262142)	
1	1000BASE-T	☒ Enabled	500	☒ Enabled	500	☒ Enabled	500	1
2	1000BASE-T	☒ Enabled	500	☒ Enabled	500	☒ Enabled	500	1
3	1000BASE-T	☒ Enabled	500	☒ Enabled	500	☒ Enabled	500	1
4	1000BASE-T	☒ Enabled	500	☒ Enabled	500	☒ Enabled	500	1
5	1000BASE-T	☒ Enabled	500	☒ Enabled	500	☒ Enabled	500	1

Class of Service

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.

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:

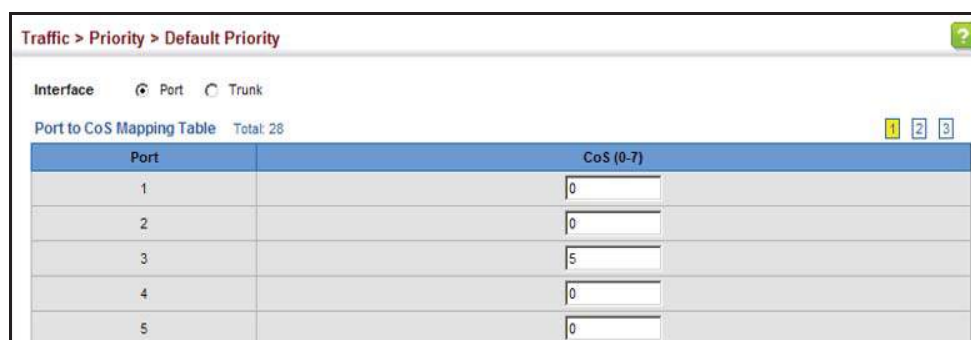
- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **CoS** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)

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 114: 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.

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.

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 when using the strict-weighted queuing mode. (Default: Disabled)
- ◆ **Weight** – Sets a weight for each queue which is used by the WRR scheduler. (Range: 1-127; 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 115: 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. There are 'Apply' and 'Revert' buttons at the bottom right.

Figure 116: Setting the Queue Mode (WRR)

The screenshot shows the 'Traffic > Priority > Queue' configuration page. The 'Port' is set to '1' and the 'Queue Mode' is set to 'WRR'. Below the settings is a table titled 'Queue Setting Table' with 'Total: 8' entries. The table has two columns: 'Queue ID' and 'Weight (1-127)'. The 'Queue ID' column lists values from 0 to 7. The 'Weight' column lists values: 1, 2, 4, 6, 8, 10, 12, and 14. There are 'Apply' and 'Revert' buttons at the bottom right.

Queue ID	Weight (1-127)
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

Figure 117: Setting the Queue Mode (Strict and WRR)

Traffic > Priority > Queue

Port: 1

Queue Mode: Strict and WRR

Queue Setting Table Total: 8

Queue ID	Strict Mode	Weight (1-127)
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

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.

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 233](#)) 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 233](#)) is used for priority processing.

Parameters

These parameters are displayed:

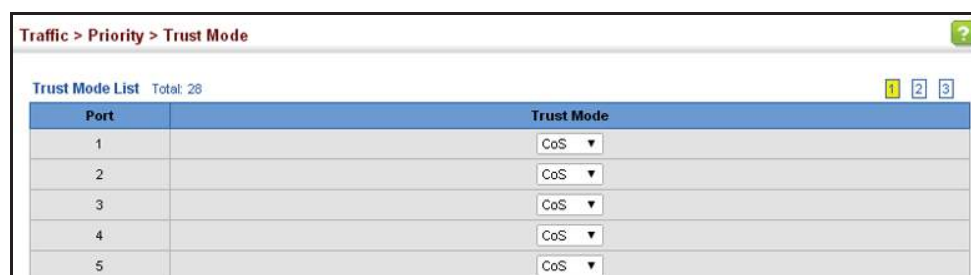
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Trust Mode**
 - **CoS** – Maps layer 3/4 priorities using Class of Service values. (This is the default setting.)
 - **DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point values.

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 118: Setting the Trust Mode



Port	Trust Mode
1	CoS ▼
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.

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 238](#)), 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 15: 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, $\text{ingress-dscp} = \text{ingress-dscp10} * 10 + \text{ingress-dscp1}$); 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 the port to configure.
4. Set the PHB and drop precedence for any DSCP value.
5. Click Apply.

Figure 119: Configuring DSCP to DSCP Internal Mapping

Traffic > Priority > DSCP to DSCP

Action: Configure

Port: 1

DSCP (0-63):

PHB (0-7):

Drop Precedence: 0: Green

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.

Figure 120: Showing DSCP to DSCP Internal Mapping

	DSCP	PHB	Drop Precedence
☐	0	0	0: Green
☐	1	1	1: Red
☐	2	0	0: Green
☐	3	0	3: Yellow
☐	4	0	0: Green
☐	5	0	1: Red
☐	6	0	0: Green
☐	7	0	3: Yellow
☐	8	1	0: Green
☐	9	1	1: Red

Mapping CoS Priorities to Internal DSCP Values

Use the Traffic > Priority > CoS to DSCP page to maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing.

Command Usage

- ◆ The default mapping of CoS to PHB values is shown in [Table 16 on page 242](#).
- ◆ 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.

Parameters

These parameters are displayed:

- ◆ **Port** – Specifies a port. (Range: 1-28)
- ◆ **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 16: 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. Set the PHB and drop precedence for any of the CoS/CFI combinations.
4. Click Apply.

Figure 121: Configuring CoS to DSCP Internal Mapping

Traffic > Priority > CoS to DSCP

Action: Configure

Port 1

CoS (0-7)

CFI (0-1)

PHB (0-7)

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.

Figure 122: Showing CoS to DSCP Internal Mapping

Traffic > Priority > CoS to DSCP

Action: Show

CoS to DSCP Mapping List Total: 16

	CoS	CFI	PHB	Drop Precedence
☐	0	0	0	0: Green
☐	0	1	0	0: Green
☐	1	0	1	0: Green
☐	1	1	1	0: Green
☐	2	0	2	0: Green
☐	2	1	2	0: Green
☐	3	0	3	0: Green
☐	3	1	3	0: Green
☐	4	0	4	0: Green
☐	4	1	4	0: Green

Default Revert

Quality of Service

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, 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 249](#)).

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, a VLAN, or a CoS value.
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.



Note: Up to 16 classes can be included in a policy map.

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.

Command Usage

- ◆ The class map is used with a policy map ([page 249](#)) to create a service policy ([page 253](#)) 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** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.

- ◆ **Description** – A brief description of a class map. (Range: 1-64 characters)

Add Rule

- ◆ **Class Name** – Name of the class map.
- ◆ **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- ◆ **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:1-4094)
- ◆ **CoS** – A CoS value. (Range: 0-7)

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. Enter a description.
6. Click Add.

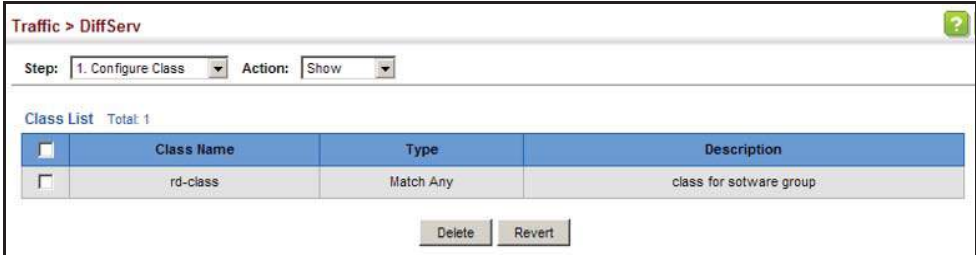
Figure 123: Configuring a Class Map

The screenshot shows a web interface for configuring a class map. At the top, it says 'Traffic > DiffServ'. Below that, there are two dropdown menus: 'Step: 1. Configure Class' and 'Action: Add'. The main form has three fields: 'Class Name' with the value 'rd-class', 'Type' with the value '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 124: Showing Class Maps



The screenshot shows the 'Traffic > DiffServ' configuration page. At the top, there is a breadcrumb 'Traffic > DiffServ' and a green help icon. Below this, there are two dropdown menus: 'Step: 1. Configure Class' and 'Action: Show'. Underneath, the 'Class List' is displayed with a 'Total: 1' count. The table has four columns: a checkbox, 'Class Name', 'Type', and 'Description'. One row is visible with the class name 'rd-class', type 'Match Any', and description 'class for software group'. At the bottom right of the table, there are 'Delete' and 'Revert' buttons.

	Class Name	Type	Description
☐	rd-class	Match Any	class for software group

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, or CoS value. You can specify up to 16 items to match when assigning ingress traffic to a class map.
6. Click Apply.

Figure 125: Adding Rules to a Class Map

Traffic > DiffServ

Step: 2. Configure Policy Action: Add Rule

Policy Name: rd-policy

Rule:

Class Name: rd-class

☒ Action: Set CoS (0-7)

☐ Meter

Meter Mode: Flow

Committed Information Rate (16-1000000): kbps

Committed Burst Size (128-8388608): bytes

Excess Burst Size (128-8388608): bytes

Peak Information Rate (16-1000000): kbps

Peak Burst Size (128-8388608): bytes

Conform: Transmit

Exceed: Set IP DSCP (0-63)

Violate: Set IP DSCP (0-63)

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 126: Showing the Rules for a Class Map

Traffic > DiffServ

Step: 1. Configure Class Action: Show Rule

Class Name: rd-class

Type: Match Any

Rule List Total: 2

	Rule
☐	IP DSCP 3
☐	IP Precedence 3

Delete Revert

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 245](#)). A policy map can then be bound by a service policy to one or more interfaces ([page 253](#)).

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 a specific VLAN. A policy map is then configured which indicates the boundary parameters used for monitoring inbound 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.

Meter Mode – Defines the committed information rate (maximum throughput).

- ◆ Policing is based on a token bucket, where bucket depth is the maximum burst before the bucket overflows, and the average rate tokens that are added to the bucket is by specified by the *committed-rate* option. Note that the token bucket functions similar to that described in RFC 2697 and RFC 2698.
- ◆ The behavior of the meter is specified in terms of 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 packets 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 $Te(t)-B \geq 0$, the packets 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.

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: 1-64 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. A policy map can contain up to 32 class maps.
- ◆ **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 16, “Default Mapping of CoS/CFI to Internal PHB/Drop Precedence,” on page 242](#)).
 - **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 15, “Default Mapping of DSCP Values to Internal PHB/Drop Values,” on page 240](#)).
 - **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.
 - **Meter Mode (Rate)** – Defines the committed information rate. Policing is based on a token bucket, where the average rate tokens that are removed from the bucket is specified by the “Rate” option. The committed rate is in kilobits per second. (Range: 16-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

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 Apply.

Figure 127: Configuring a Policy Map

Traffic > DiffServ

Step: 2. Configure Policy Action: Add

Policy Name: rd-policy

Description: for the software group

Apply 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 128: Showing Policy Maps

Traffic > DiffServ

Step: 2. Configure Policy Action: Show

Policy List Total: 1

	Policy Name	Description
☐	rd-policy	for the software group

Delete Revert

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. Click on the Action field, and set the CoS or per-hop behavior for matching packets to specify the quality of service to be assigned to the matching traffic class.
6. Use the metering option to define the maximum throughput.
7. Click Apply.

Figure 129: Adding Rules to a Policy Map

The screenshot shows the 'Traffic > DiffServ' configuration page. At the top, there are two dropdown menus: 'Step: 2. Configure Policy' and 'Action: Add Rule'. Below these, the 'Policy Name' is set to 'rd'. Under the 'Rule:' section, the 'Class Name' is 'tpd'. The 'Action' checkbox is checked, and the 'Set' dropdown is set to 'CoS (0-7)'. The 'Meter' checkbox is unchecked. Under the 'Meter Mode' section, the 'Rate (16-1000000)' is set to '16-1000000' and the 'Rate Limit' is set to 'kbps'. At the bottom right, there are 'Apply' and 'Revert' buttons.

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 130: Showing the Rules for a Policy Map

The screenshot shows the 'Traffic > DiffServ' configuration page. The 'Step' is set to '2. Configure Policy' and the 'Action' is 'Show Rule'. The 'Policy Name' is 'rd'. Below this, the 'Rule List' is displayed with a total of 1 rule. The table has columns for Class Name, Action, and Meter (which is further divided into Meter Mode and Rate (kbps)).

	Class Name	Action	Meter	
			Meter Mode	Rate (kbps)
☐	tpd		Rate Limit	16

At the bottom of the table, there are 'Delete' and 'Revert' buttons.

Attaching a Policy Map to a Port

Use the Traffic > DiffServ (Configure Interface) page to bind a policy map to a port.

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. (Range: 1-10)
- ◆ **Ingress** – Applies the selected rule to ingress 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 131: Attaching a Policy Map to a Port

Traffic > DiffServ

Step: 3. Configure Interface

Port Service Policy List Total: 28

Port	Ingress
1	☐ rd-policy ▼
2	☐ rd-policy ▼
3	☐ rd-policy ▼
4	☐ rd-policy ▼
5	☐ rd-policy ▼
6	☐ rd-policy ▼
7	☐ rd-policy ▼
8	☐ rd-policy ▼
9	☐ rd-policy ▼
10	☐ rd-policy ▼

Apply Revert

VoIP Traffic Configuration

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.

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 186](#)).

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: 1-4094)
- ◆ **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 132: 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.

Parameters

These parameters are displayed:

- ◆ **Telephony OUI** – Specifies a MAC address range to add to the list.
(Format: xx-xx-xx-xx-xx-xx)
- ◆ **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 a mask of FF-FF-FF-FF-FF-FF specifies a single MAC address. (Format: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx;
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 133: 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 134: Showing an OUI Telephony List

Traffic > VoIP

Step: 2. Configure OUI Action: Show

Telephony OUI List Total: 3

	Telephony OUI	Mask	Description
☐	00-E0-BB-00-00-00	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

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.

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 186](#)).

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 359](#) 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.

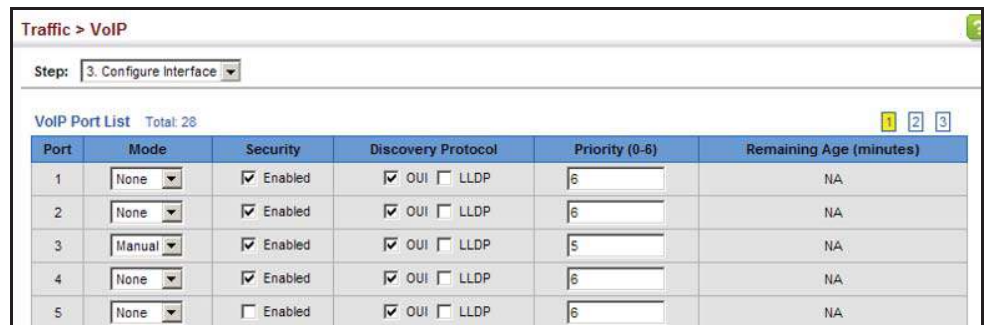
When VoIP Mode is set to Auto, the Remaining Age will be displayed.
Otherwise, if the VoIP Mode is Disabled or set to Manual, the remaining age will display "NA."

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 135: Configuring Port Settings for a Voice VLAN



The screenshot shows the 'Traffic > VoIP' configuration page. At the top, there is a 'Step:' dropdown menu set to '3. Configure Interface'. Below this is a 'VoIP Port List' section with a 'Total: 28' indicator and three numbered tabs (1, 2, 3). The main table displays the configuration for five ports. The columns are: Port, Mode, Security, Discovery Protocol, Priority (0-6), and Remaining Age (minutes). Port 1 has Mode 'None', Security 'Enabled', Discovery Protocol 'OUI' and 'LLDP' checked, Priority '6', and Remaining Age 'NA'. Port 2 has Mode 'None', Security 'Enabled', Discovery Protocol 'OUI' and 'LLDP' checked, Priority '6', and Remaining Age 'NA'. Port 3 has Mode 'Manual', Security 'Enabled', Discovery Protocol 'OUI' and 'LLDP' checked, Priority '5', and Remaining Age 'NA'. Port 4 has Mode 'None', Security 'Enabled', Discovery Protocol 'OUI' and 'LLDP' checked, Priority '6', and Remaining Age 'NA'. Port 5 has Mode 'None', Security 'Enabled', Discovery Protocol 'OUI' and 'LLDP' checked, Priority '6', and Remaining Age 'NA'.

Port	Mode	Security	Discovery Protocol	Priority (0-6)	Remaining Age (minutes)
1	None	☒ Enabled	☒ OUI ☐ LLDP	6	NA
2	None	☒ Enabled	☒ OUI ☐ LLDP	6	NA
3	Manual	☒ Enabled	☒ OUI ☐ LLDP	5	NA
4	None	☒ Enabled	☒ OUI ☐ LLDP	6	NA
5	None	☐ Enabled	☒ OUI ☐ LLDP	6	NA

Security Measures

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.
- ◆ [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.
- ◆ [DHCP Snooping](#) – Filter IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping.
- ◆ [DoS Protection](#) – Protects against Denial-of-Service attacks.
- ◆ [IPv4 Source Guard](#) – Filters IPv4 traffic on insecure ports for which the source address cannot be identified via DHCPv4 snooping nor static source bindings.



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 263](#).
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.

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:

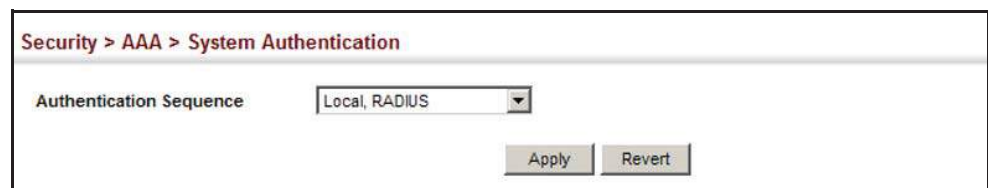
- ◆ **Authentication Sequence** – Select the authentication, or authentication sequence required:
 - **Local** – User authentication is performed only locally by the switch.
 - **RADIUS** – User authentication is performed using a RADIUS server only.
 - **TACACS** – User authentication is performed using 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 136: Configuring the Authentication Sequence

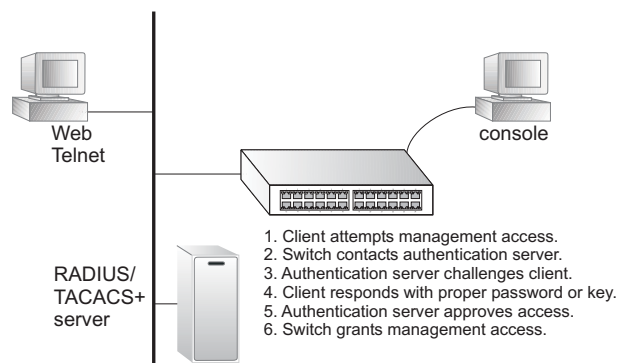


**Configuring
Remote Logon
Authentication
Servers**

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 137: 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.

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. Enclose any string containing blank spaces in double quotes.
(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. Enclose any string containing blank spaces in double quotes.
(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 263](#)).

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 138: Configuring Remote Authentication Server (RADIUS)

The screenshot displays the 'Security > AAA > Server' configuration page. At the top, 'Server Type' is set to 'RADIUS' (selected with a radio button) and 'TACACS+' is unselected. Below this, 'Global' is unselected and 'Server Index' is set to '1' (selected with a radio button). The configuration fields are as follows:

Field	Value
Server IP Address	10.1.1.1
Accounting Server UDP Port (1-65535)	1813
Authentication Server UDP Port (1-65535)	1815
Authentication Timeout (1-65535)	10 sec
Authentication Retries (1-30)	5
Set Key	☒
Authentication Key	
Confirm Authentication Key	

At the bottom right, there are 'Apply' and 'Revert' buttons.

Figure 139: 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

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 140: 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

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 141: 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. Below this, a section titled 'RADIUS Group List' indicates a total of 3 groups. A table lists the groups with columns for 'Group Name' and 'Member Index'. Each row has a checkbox on the left. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Group Name	Member Index
☐	radius	1, 2, 3, 5
☐	radius1	3, 5, 1
☐	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.

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 263](#)). 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 or SSH.
- ◆ **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 and SSH 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 142: Configuring Global Settings for AAA Accounting

The screenshot shows the Cisco Web Interface for configuring AAA Accounting. The breadcrumb navigation at the top reads "Security > AAA > Accounting". Below this, there is a "Step:" dropdown menu currently set to "1. Configure Global". The main configuration area contains a "Periodic Update (1-2147483647)" label, a checked checkbox, and a text input field containing the value "1", followed by the unit "min". At the bottom right of the form are two buttons: "Apply" and "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 143: Configuring AAA Accounting Methods

The screenshot shows a web-based configuration interface for AAA Accounting. The breadcrumb navigation at the top reads "Security > AAA > Accounting". Below this, there are two dropdown menus: "Step:" set to "2. Configure Method" and "Action:" set to "Add". The main configuration area contains four fields: "Accounting Type" is a dropdown menu currently showing "802.1X"; "Method Name" is a text input field containing "default"; "Accounting Notice" is a dropdown menu showing "Start-Stop"; and "Server Group Name" consists of a radio button selected next to a dropdown menu showing "radius", and another radio button next to an empty text input field. At the bottom right of the form are two buttons: "Apply" and "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 144: Showing AAA Accounting Methods

Accounting Type	Method Name	Accounting Notice	Server Group Name
802.1X	default	Start-Stop	radius
Command 0	default	Start-Stop	tacacs+
Command 1	default	Start-Stop	tacacs+
Command 2	default	Start-Stop	tacacs+
Command 3	default	Start-Stop	tacacs+
Command 4	default	Start-Stop	tacacs+
Command 5	default	Start-Stop	tacacs+
Command 6	default	Start-Stop	tacacs+
Command 7	default	Start-Stop	tacacs+
Command 8	default	Start-Stop	tacacs+

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 145: Configuring AAA Accounting Service for 802.1X Service

Port	Method Name
1	default
2	default
3	default
4	
5	

Figure 146: 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 147: Configuring AAA Accounting Service for Exec Service

Security > AAA > Accounting

Step: 3. Configure Service

Accounting Type ☐ 802.1X ☐ Command ☒ EXEC

Console Method Name default

VTY Method Name default

Apply Revert

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 148: Displaying a Summary of Applied AAA Accounting Methods

Security > AAA > Accounting

Step: 4. Show Information

Summary Statistics

Method List Total: 18

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 149: Displaying Statistics for AAA Accounting Sessions

Security > AAA > Accounting

Step: 4. Show Information

Summary 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.

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:
 - **Command** – Administrative authorization to apply to commands entered at specific CLI privilege levels.
 - **Exec** – 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 263](#)). 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 and SSH 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 150: Configuring AAA Authorization Methods

Security > AAA > Authorization

Step: 1. Configure Method Action: Add

Authorization Type EXEC

Method Name default

Server Group Name ☒ tacacs+ ☐

Apply 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 151: Showing AAA Authorization Methods

Security > AAA > Authorization

Step: 1. Configure Method Action: Show

Method List Total: 2

☐	Authorization Type	Method Name	Server Group Name
☐	EXEC	default	tacacs+
☐	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 152: 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 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 153: 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.

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 command access privileges. (Range: 0-15)

Level 0, 8 and 15 are designed for users (guest), managers (network maintenance), and administrators (top-level access). The other levels can be used to configured specialized access profiles.

Level 0-7 provide the same default access to a limited number of commands which display the current status of the switch, as well as several database clear and reset functions. These commands are equivalent to those available under Normal Exec command mode in the CLI.

Level 8-14 provide the same default access privileges, including additional commands beyond those provided for Levels 0-7 (equivalent to CLI Normal Exec command mode), and a subset of the configuration commands provided for Level 15 (equivalent to CLI Privileged Exec command mode).

Level 15 provides full access to all commands.

The privilege level associated with any command can be changed using the "[privilege](#)" command described on [page 627](#).

Any privilege level can access all of the commands assigned to lower privilege levels. For example, privilege level 8 can access all commands assigned to privilege levels 7-0 according to default settings, and to any other commands assigned to levels 7-0 using the "[privilege](#)" command.
- ◆ **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.

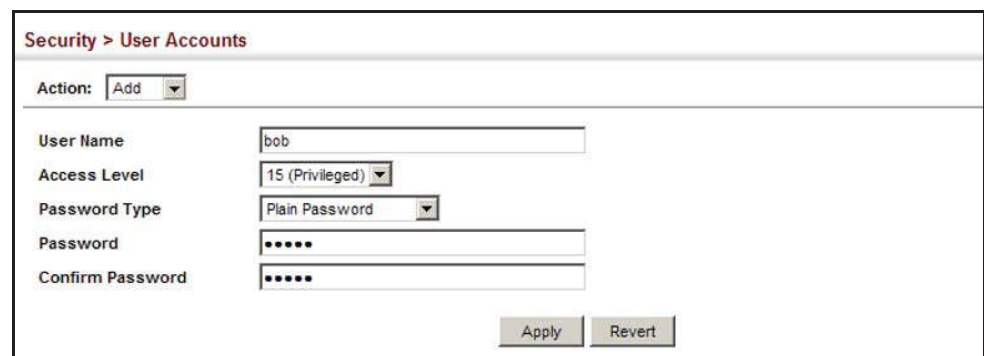
- ◆ **Password** – Specifies the user password. (Range: 0-32 characters, case sensitive)
- ◆ **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.

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 154: Configuring User Accounts

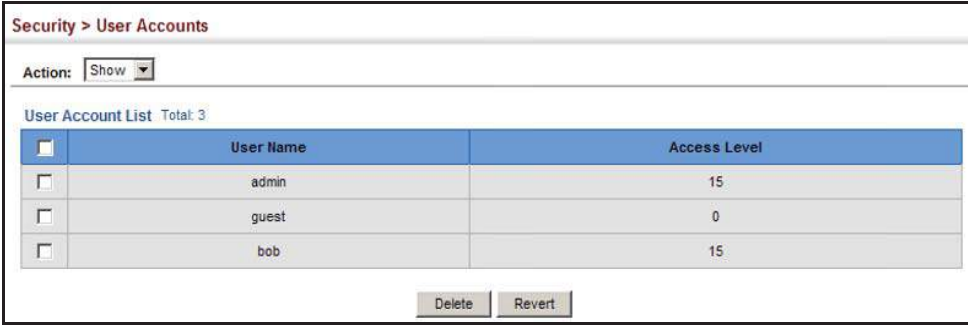


The screenshot shows a web interface titled "Security > User Accounts". At the top, there is an "Action:" dropdown menu with "Add" selected. Below this, there are several form fields: "User Name" with the value "bob", "Access Level" with a dropdown menu showing "15 (Privileged)", "Password Type" with a dropdown menu showing "Plain Password", "Password" with a masked input field (dots), and "Confirm Password" with a masked input field (dots). At the bottom right, there are two buttons: "Apply" and "Revert".

To show user accounts:

1. Click Security, User Accounts.
2. Select Show from the Action list.

Figure 155: Showing User Accounts



Security > User Accounts		
Action: Show		
User Account List Total: 3		
☐	User Name	Access Level
☐	admin	15
☐	guest	0
☐	bob	15

Delete 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 264.)

Note: MAC authentication cannot be configured on trunk ports.

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 17: 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)
	rate-limit-output = <i>rate</i>	rate-limit-output=200 (kbps)
802.1p	switchport-priority-default = <i>value</i>	switchport-priority-default=2
IP ACL	ip-access-group-in = <i>ip-acl-name</i>	ip-access-group-in=ipv4acl
IPv6 ACL	ipv6-access-group-in = <i>ipv6-acl-name</i>	ipv6-access-group-in=ipv6acl
MAC ACL	mac-access-group-in = <i>mac-acl-name</i>	mac-access-group-in=macAcl

- ◆ 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.

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 332](#)).

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.

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 156: Configuring Global Settings for Network Access



Security > Network Access

Step: 1. Configure Global

Aging Status ☐ Enabled

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.

Parameters

These parameters are displayed:

- ◆ **Guest VLAN** – Specifies the VLAN to be assigned to the port when 802.1X Authentication or MAC authentication fails. (Range: 0-4094, where 0 means disabled; Default: Disabled)

The VLAN must already be created and active (see [“Configuring VLAN Groups” on page 184](#)). 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 332](#)).

A port can only be assigned to the guest VLAN in case of failed authentication, and switchport mode is set to Hybrid. (See [“Adding Static Members to VLANs” on page 186](#).)
- ◆ **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 (to the 802.1X authentication process), 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.

- ◆ **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. Set the guest VLAN to use when MAC Authentication or 802.1X Authentication fails, the dynamic VLAN, and the MAC filter.
5. Click Apply.

Figure 157: Configuring Interface Settings for Network Access

The screenshot shows the 'Security > Network Access' configuration page. The 'Step' dropdown is set to '2. Configure Interface'. Below this is a 'Port List' table with 5 ports. Each port has a 'Guest VLAN' field (set to 0), a 'Dynamic VLAN' checkbox (checked), and a 'MAC Filter (1-64)' field (empty). The table has a 'Total: 28' indicator and three tabs (1, 2, 3) at the top right.

Port	Guest VLAN (0-4094, 0: Disabled)	Dynamic VLAN	MAC Filter (1-64)
1	0	☒ Enabled	
2	0	☒ Enabled	
3	0	☒ Enabled	
4	0	☒ Enabled	
5	0	☒ Enabled	

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.

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. (Range: 1-64)
- ◆ **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.

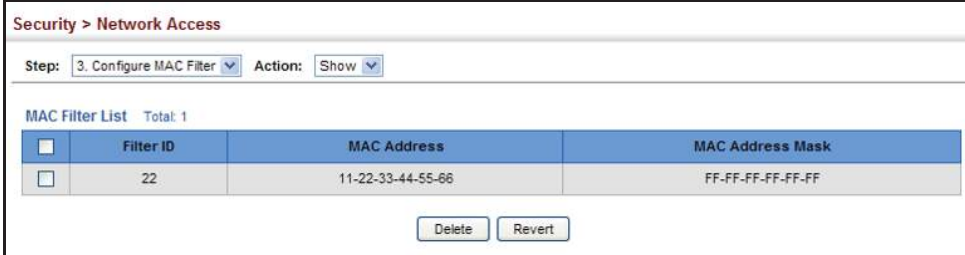
Figure 158: Configuring a MAC Address Filter for Network Access

The screenshot shows the 'Security > Network Access' configuration page. At the top, the breadcrumb 'Security > Network Access' is displayed. Below it, the 'Step' dropdown is set to '3. Configure MAC Filter' and the 'Action' dropdown is set to 'Add'. The main configuration area contains three input fields: 'Filter ID (1-64)' with the value '22', 'MAC Address' with the value '11-22-33-44-55-66', and 'MAC Address Mask' with the value 'FFFFFFFF'. At the bottom right of the form are two buttons: 'Apply' and '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 159: Showing the MAC Address Filter Table for Network Access



The screenshot shows the 'Security > Network Access' configuration page. At the top, there is a breadcrumb trail 'Security > Network Access'. Below it, there are two dropdown menus: 'Step: 3. Configure MAC Filter' and 'Action: Show'. The main content area is titled 'MAC Filter List' with a 'Total: 1' indicator. It contains a table with the following data:

☐	Filter ID	MAC Address	MAC Address Mask
☐	22	11-22-33-44-55-66	FF-FF-FF-FF-FF-FF

Below the table, there are two buttons: 'Delete' and '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.

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 160: 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
☐	00-00-86-45-F2-23	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 16m 12s	Dynamic
☐	00-00-E8-5E-E1-DD	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 32m 24s	Dynamic
☐	00-00-E8-81-93-30	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 40m 32s	Dynamic
☐	00-01-80-31-B8-30	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 18m 51s	Dynamic
☐	00-01-80-36-95-D8	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 32m 22s	Dynamic
☐	00-01-80-3B-D3-7F	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 22m 28s	Dynamic
☐	00-01-80-3C-3C-19	Unit 2 / Port 23	10.2.2.10	2008y 20m 12d 11h 15m 19s	Dynamic
☐	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 TCP port used for this service.

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 TCP port. (HTTP can only be configured through the CLI using the ["ip http server"](#) command.)
- ◆ 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 9, Mozilla Firefox 39, or Google Chrome 44, or more recent versions.
- ◆ The following web browsers and operating systems currently support HTTPS:

Table 18: HTTPS System Support

Web Browser	Operating System
Internet Explorer 9.x or later	Windows 7, 8, 10
Mozilla Firefox 39 or later	Windows 7, 8, 10, Linux
Google Chrome 44 or later	Windows 7, 8, 10

- ◆ To specify a secure-site certificate, see ["Replacing the Default Secure-site Certificate"](#) on page 290.



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 TCP 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 161: 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 133](#) or type “reload” at the command prompt: `Console#reload`

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 162: Downloading the Secure-Site Certificate

The screenshot shows a web-based configuration interface for HTTPS settings. At the top, it says "Security > HTTPS". Below this, there is a section titled "Action:" with a dropdown menu set to "Copy Certificate". Underneath, there are five input fields: "TFTP Server IP Address" (containing "192.168.2.99"), "Certificate Source File Name" (containing "SP6528-site-certificate"), "Private Key Source File Name" (containing "SP6528-private-key"), "Private Password" (containing "*****"), and "Confirm Password" (containing "*****"). 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 263). 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
595664104869574278881462065194174677298486546861571773939016477935594230357741
309802273708779454524083971752646358058176716709574804776117
```

3. *Import Client's Public Key to the Switch* – See [“Importing User Public Keys” on page 297](#) 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 279](#).) 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
134108168560989392104094492015542534763164192187295892114317388005553616163105
17759408386863110929123226828519254374603100937187721199696317813662774141689
851320491172048303392543241016379975923714490119380060902539484084827178194372
288402533115952134861022902978982721353267131629432532818915045306393916643
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: You must generate DSA and RSA host keys before enabling the SSH server. See [“Generating the Host Key Pair” on page 296](#).

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 163: 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 fields are as follows:

Parameter	Value
SSH Server Status	☒ 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 'Apply' and 'Revert' buttons.

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 297.



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 294.

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** – 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 from the Show page. (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. Click Apply.

Figure 164: Generating the SSH Host Key Pair

The screenshot shows the 'Security > SSH' configuration page. At the top, there's a breadcrumb 'Security > SSH'. Below it, there are two dropdown menus: 'Step:' set to '2. Configure Host Key' and 'Action:' set to 'Generate'. Underneath, there's a 'Host-Key Type' dropdown menu set to 'Both'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

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 option to save the host key from memory to flash by clicking Save, or select the host-key type to clear and click Clear.

Figure 165: Showing the SSH Host Key Pair

Security > SSH

Step: 2. Configure Host Key Action: Show

Public-Key of Host-Key

☒ RSA

```
1024 65537
133939690967068772691132582542091118069946187790543050435991419159456328108424510227003
175806564056474112418102266589753060303978654741958937882157740680884883800146758464583
403760868973720460189697876570213012247127554124148560753905598712710960791931537404447
966097709515788354636277697671184100501439926741
```

☐ DSA

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAlY4Beu1CFOPsrgqEeW89esSV0snL8VSBwmiY7r6n8GksbwJJ6wLA9z+4kUAFK3FG
3WLVHMA1dj62o3W777PspGzgyH1CD4KEWHNHu0oLuGozeZ5HzpDH76zkYwfzIJuKwS7FntQTD+//1wPCmNy1
cQdwJICTnRs1YYpVh4YKYfAAAAFQDwt5uUQHcC8qaFQ3DhNFPZ9wCX5wAAAIACzKDORASvv91v6WHYBbc9GX6
PH4V+15Lm+Eq87jiOUAYxUGat1q8071h16RRR5XH44CIOHC4VJjhSI873weYO/IULCZSAEa9GczPpWhZ9EA1
```

Clear

Save Click this button to Save All Host-Key from Memory to Flash.

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.

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 279](#)).
- ◆ **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 166: 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 167: 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
AAAAAB3NzaC1kc3MAAACBAKM4i8EgUe89W+vh1+y4z12YpyK8cpCNz30rhCriv1ClKmdgE/fiZFsqrYH/ClAB/
sJ1rNAX0sJTUxtb8e2GLk+x8UmQJVuSDdklwZ9ZRoFwWAl0Yyi57V1TK3tUnT9ocCbVJNGckJkXdiuac4OP09
tAPEAuXBuAWGpDAGSmg6pHAAAFQCPzwn0rSaLiTq53jx1tsj0RILZwAAABiL0Cr7GC7ARztGE9dRkT9oh9
uhuiAzcXrAcZTmxhjGsEtM1AtxKm+r1O6pnz2aX9KEzMEwJEMuDphOTRnSpMv39XtSW1aSXWtKoGAcQgDsFqK
```

Clear

Access Control Lists

Access Control Lists (ACL) provide packet filtering for IPv4/IPv6 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 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.

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.

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:

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

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 168: Showing TCAM Utilization

Security > ACL

Step: 2. Configure ACL Action: Show TCAM

Pool Capability Code:

AM - MAC ACL, A4 - IPv4 ACL, A6S - IPv6 Standard ACL,
A6E - IPv6 extended ACL, DM - MAC diffServ, D4 - IPv4 diffServ,
D6S - IPv6 standard diffServ, D6E - IPv6 extended diffServ,
I - IP source guard, C - CPU interface, L - Link local,
Reserved - Reserved, ALL - All supported function.

TCAM List Total: 12

Unit	Device	Pool	Total	Used	Free	Capability
1	0	0	64	0	64	A6S
1	0	1	64	0	64	A6E
1	0	2	128	0	128	A4
1	0	3	128	0	128	AM
1	0	4	64	0	64	D6S D6E
1	0	5	128	0	128	D4
1	0	6	128	0	128	DM
1	0	7	128	128	0	Reserved
1	0	8	64	64	0	I
1	0	9	64	64	0	C
1	0	10	64	64	0	Reserved
1	0	11	64	64	0	L

Setting the ACL Name and Type

Use the Security > ACL (Configure ACL - Add) page to create an ACL.

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 317).

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 169: Creating an ACL

The screenshot shows the 'Security > ACL' configuration page. The 'Step' dropdown is set to '2. Configure ACL' and the 'Action' dropdown is set to 'Add'. The 'ACL Name' field contains 'R&D' and the 'Type' dropdown is set to 'IP Standard'. At the bottom right, there are 'Apply' and 'Revert' buttons.

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 170: Showing a List of ACLs

The screenshot shows the 'Security > ACL' configuration page with the 'Action' dropdown set to 'Show'. Below the configuration fields, there is a table titled 'ACL List' with a 'Total: 10' indicator. The table lists various ACLs with their names and types. At the bottom right, there are 'Delete' and 'Revert' buttons.

	ACL Name	Type
☐	aclStandard1	IP Standard
☐	aclStandard2	IP Standard
☐	aclExtended1	IP Extended
☐	aclExtended2	IP Extended
☐	aclMAC1	MAC
☐	aclMAC2	MAC
☐	aclMAC2	MAC
☐	aclIPv6Standard	IPv6 Standard
☐	aclIPv6Extended	IPv6 Extended
☐	aclARP	ARP

Configuring a Standard IPv4 ACL Use the Security > ACL (Configure ACL - Add Rule - IP Standard) page to configure a Standard IPv4 ACL.

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 171: Configuring a Standard IPv4 ACL

Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type ☒ IP Standard ☐ IP Extended ☐ MAC ☐ IPv6 Standard ☐ IPv6 Extended ☐ ARP

Name R&D

Action Permit

Address Type Host

Source IP Address 10.1.1.21

Source Subnet Mask 255.255.255.255

☒ Time-Range R&D

Apply Revert

Configuring an Extended IPv4 ACL Use the Security > ACL (Configure ACL - Add Rule - IP Extended) page to configure an Extended IPv4 ACL.

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 304](#).)
- ◆ **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)

The following items are under TCP

- **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

◆ **Service Type** – Packet priority settings based on the following criteria:

- **Precedence** – IP precedence level. (Range: 0-7)
- **DSCP** – DSCP priority level. (Range: 0-63)

◆ **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 172: Configuring an Extended IPv4 ACL

The screenshot shows the 'Security > ACL' configuration window. 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' with 'Source IP Address' '10.7.1.0' and 'Source Subnet Mask' '255.255.255.0'. The 'Destination Address Type' is 'Any' with 'Destination IP Address' '0.0.0.0' and 'Destination Subnet Mask' '0.0.0.0'. The 'Protocol' is 'TCP (6)' with 'Control Code (0-63)' and 'Control Code Bit Mask (0-63)' fields. The 'Service Type' is 'Precedence (0-7)'. The 'Time-Range' is 'R&D'. The 'Apply' and 'Revert' buttons are at the bottom.

Configuring a Standard IPv6 ACL Use the Security > ACL (Configure ACL - Add Rule - IPv6 Standard) page to configure a Standard IPv6 ACL.

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 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 173: Configuring a Standard IPv6 ACL

The screenshot shows the 'Security > ACL' configuration page. The 'Step' dropdown is set to '1. Configure ACL' and the 'Action' dropdown is set to 'Add Rule'. Under the 'Type' section, 'IPv6 Standard' is selected with a radio button. The 'Name' field contains '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 '2000:4:213:19ff:fe7b:5004'. The 'Source Prefix Length (0-128)' field contains '128'. There is an unchecked checkbox for 'Time-Range' and a dropdown menu next to it. At the bottom right, there 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.

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 Address Type** – Specifies the source IP address type. 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)
- ◆ **Destination Address Type** – Specifies the 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 prefix; 0-8 bits for the destination prefix)
- ◆ **DSCP** – DSCP traffic class. (Range: 0-63)
- ◆ **Source Port** – Protocol⁶ source port number. (Range: 0-65535)
- ◆ **Source Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- ◆ **Destination Port** – Protocol⁶ destination port number. (Range: 0-65535)
- ◆ **Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- ◆ **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

6. Includes TCP, UDP or other protocol types.

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)

◆ **Time Range** – Name of a time range.

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 174: Configuring an Extended IPv6 ACL

The screenshot shows the 'Security > ACL' configuration window. At the top, it says 'Step: 2. Configure ACL' and 'Action: Add Rule'. The configuration fields are as follows:

- Action:** Permit (dropdown)
- Source Address Type:** Any (dropdown)
- Source IPv6 Address:** :: (text field)
- Source Prefix Length (0-128):** 0 (text field)
- Destination Address Type:** Any (dropdown)
- Destination IPv6 Address:** :: (text field)
- Destination Prefix Length (0-128):** 0 (text field)
- DSCP (0-63):** (empty text field)
- Next-Header (0-255):** (empty text field)
- Source Port (0-65535):** (empty text field)
- Source Port Bit Mask (0-65535):** (empty text field)
- Destination Port (0-65535):** (empty text field)
- Destination Port Bit Mask (0-65535):** (empty text field)
- Time-Range:** ☐ (checkbox)
- R&D:** R&D (dropdown)

At the bottom right, there are 'Apply' and 'Revert' buttons.

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.

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)
- ◆ **CoS** – CoS value. (Range: 0-7, where 7 is the highest priority)
- ◆ **CoS Bit Mask** – CoS bitmask. (Range: 0-7)
- ◆ **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 175: Configuring a MAC ACL

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 318](#)).

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 304](#).)

- ◆ **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 176: Configuring a ARP ACL

The screenshot shows the 'Security > ACL' configuration page. The 'Step' is '2. Configure ACL' and the 'Action' is 'Add Rule'. The 'Type' is 'ARP'. The 'Name' is 'R&F#7ARP'. The 'Action' is 'Permit'. The 'Source IP Address Type' is 'Any', 'Source IP Address' is '0.0.0.0', and 'Source IP Subnet Mask' is '0.0.0.0'. The 'Source MAC Address Type' is 'Any', 'Source MAC Address' is '00-00-00-00-00-00', and 'Source MAC Bit Mask' is '00-00-00-00-00-00'. The 'Destination IP Address Type' is 'Any', 'Destination IP Address' is '0.0.0.0', and 'Destination IP Subnet Mask' is '0.0.0.0'. The 'Destination MAC Address Type' is 'Any', 'Destination MAC Address' is '00-00-00-00-00-00', and 'Destination MAC Bit Mask' is '00-00-00-00-00-00'. There is a 'Log' checkbox and 'Apply' and 'Revert' buttons at the bottom.

Binding a Port to an Access Control List After configuring ACLs, use the Security > ACL (Configure Interface – Configure) page to bind the ports that need to filter traffic to the appropriate ACLs.

Parameters

These parameters are displayed:

- ◆ **Type** – Selects the type of ACLs to bind to a port.
- ◆ **Port** – Port identifier. {Range: 1-28}
- ◆ **ACL** – ACL used for ingress 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 Configure from the Action list.
4. Select IP, MAC or IPv6 from the Type options.
5. Select a port.

6. Select the name of an ACL from the ACL list.
7. Click Apply.

Figure 177: Binding a Port to an ACL

The screenshot shows a web interface for configuring ACLs. The breadcrumb is 'Security > ACL'. The 'Step' is '3. Configure Interface' and the 'Action' is 'Configure'. Under the 'Type' section, 'IP' is selected with a radio button. The 'Port' is set to '1'. Under the 'Ingress' section, 'ACL' is set to 'R&D', 'Time-Range' is set to 'R&D', and 'Counter' is unchecked. At the bottom right, there are 'Apply' and 'Revert' buttons.

Showing ACL Hardware Counters Use the Security > ACL > Configure Interface (Show Hardware Counters) page to show statistics for ACL hardware counters.

Parameters

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **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.
- ◆ **Time-Range** – Name of a time range.
- ◆ **Hit** – Shows the number of packets matching this ACL.
- ◆ **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.

Figure 178: Showing ACL Statistics

The screenshot shows the 'Security > ACL' configuration page. The 'Step' is set to '3. Configure Interface' and the 'Action' is 'Show Hardware Counter'. The 'Port' is '1', 'Type' is 'IP Standard', and 'Direction' is 'Ingress'. The 'ACL Name' is 'rd'. A 'Query' button is present. Below the form, it says 'Total: 1'. A table displays the hardware counter 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 Global Configuration” on page 340](#)). 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 313](#)).

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.

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.
 - **Allow Zeros** – Allows sender IP address to be 0.0.0.0.
 - **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 179: Configuring Global Settings for ARP Inspection

The screenshot shows the 'Security > ARP Inspection' configuration page. The 'Step' dropdown is set to '1. Configure General'. The 'ARP Inspection Status' section has the 'Enabled' checkbox checked. The 'ARP Inspection Validation' section has four checkboxes: 'Dst-MAC', 'IP', 'Allow Zeros', and 'Src-MAC', all of which are checked. The 'Log Message Number (0-256)' is set to 20, and the 'Log Interval (0-86400)' is set to 10 seconds. At the bottom right, there are 'Apply' and 'Revert' buttons.

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.

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 313](#)).
- ◆ 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:

- ◆ **VLAN** – Identifier for configured VLANs.
- ◆ **DAI Status** – Enables Dynamic ARP Inspection for the selected VLAN. (Default: Disabled)
- ◆ **ACL Name** – 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 180: Configuring VLAN Settings for ARP Inspection

Security > ARP Inspection

Step: 2. Configure VLAN

ARP Inspection VLAN List Total: 2

VLAN	DAI Status	ACL Name	ACL Status
1	☐ Enabled	☐ arp ▼	☐ Static
2	☐ Enabled	☐ arp ▼	☐ Static

Apply Revert

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.

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 181: Configuring Interface Settings for ARP Inspection

Port	Trust Status	Packet Rate Limit (0-2048 pps)
1	☒ Enabled	☒ 15
2	☐ Enabled	☒ 15
3	☐ Enabled	☒ 15
4	☐ Enabled	☒ 15
5	☐ Enabled	☒ 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.

Parameters

These parameters are displayed:

Table 19: 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 182: 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.

Parameters

These parameters are displayed:

Table 20: 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 183: 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.

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

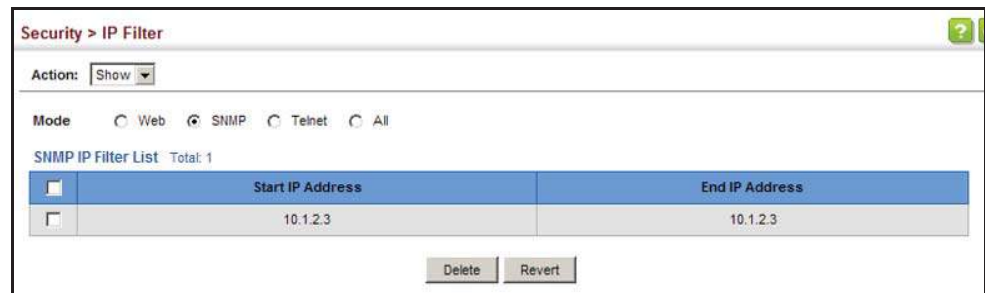
Figure 184: Creating an IP Address Filter for Management Access

The screenshot shows the 'Security > IP Filter' web interface. At the top, there is a breadcrumb trail 'Security > IP Filter'. Below it, the 'Action:' dropdown menu is set to 'Add'. Under the 'Mode' section, four radio buttons are present: 'Web' (selected), 'SNMP', 'Telnet', and 'All'. Below the mode selection, there are two text input fields: 'Start IP Address' containing '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 185: 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.

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, and then 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 199](#)).

- ◆ 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 137](#)).
- ◆ 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.
 - RSPAN and port security are mutually exclusive functions. If port security is enabled on a port, that port cannot be set as an RSPAN uplink port. Also, when a port is configured as an RSPAN uplink port, source port, or destination port, port security cannot be enabled on that port.

Parameters

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Security Status** – Enables or disables port security on a port. (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 286](#).
- ◆ **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 186: Configuring Port Security

Security > Port Security									
Port Security List Total: 26									
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	☒ Enabled	Secure/Down	Trap and Shutdown	0	1	Disabled	0	NA	NA
2	☒ Enabled	Secure/Down	Trap	0	0	Disabled	1	NA	NA
3	☐ Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA

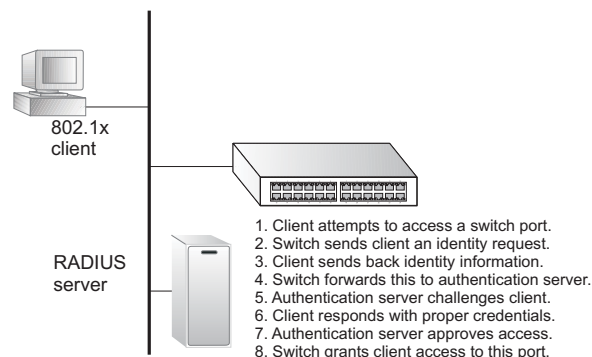
Configuring 802.1X Port Authentication

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 187: Configuring Port Authentication



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 8, 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.

Parameters

These parameters are displayed:

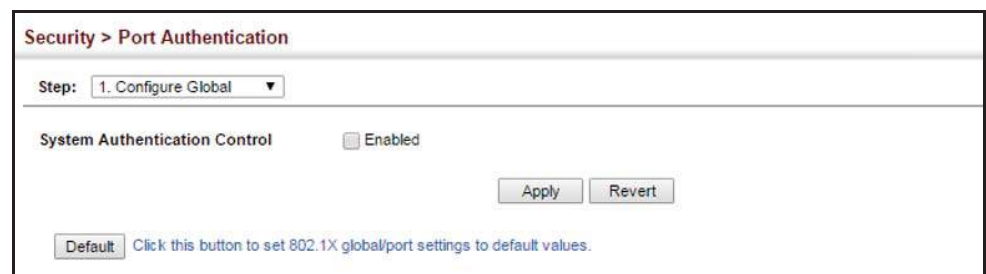
- ◆ **System Authentication Control** – Sets the global setting for 802.1X. (Default: Disabled)
- ◆ **Default** – Sets all configurable 802.1X global and port settings to their default values.

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.
4. Click Apply

Figure 188: Configuring Global Settings for 802.1X Port Authentication



The screenshot shows a web interface titled "Security > Port Authentication". Below the title is a "Step:" dropdown menu set to "1. Configure Global". The main content area contains a "System Authentication Control" label followed by a checked checkbox and the text "Enabled". At the bottom right of this section are "Apply" and "Revert" buttons. At the bottom left is a "Default" button, and next to it is a tooltip 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.

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.
- ◆ 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 264.)

- ◆ **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 184](#)) and mapped on each port (See [“Configuring Network Access for Ports” on page 284](#)).

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. Modify the authentication settings for each port as required.
4. Click Apply

Figure 189: 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

Displaying 802.1X Statistics Use the Security > Port Authentication (Show Statistics) page to display statistics for dot1x protocol exchanges for any port.

Parameters

These parameters are displayed:

Table 21: 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.
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.

Table 21: 802.1X Statistics (Continued)

Parameter	Description
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.

Figure 190: Showing Statistics for 802.1X Port Authenticator

Security > Port Authentication

Step: 3. Show Statistics

Port: 1

Port Authentication Authenticator Statistics

Rx EAPOL Start	0	Rx EAP Resp/Id	0
Rx EAPOL Logoff	0	Rx EAP Resp/Oth	0
Rx EAPOL Invalid	0	Rx EAP LenError	0
Rx EAPOL Total	0	Tx EAP Req/Id	0
Rx Last EAPOLVer	0	Tx EAP Req/Oth	0
Rx Last EAPOLSrc	00-00-00-00-00-00	Tx EAPOL Total	0

Refresh

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 is 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 Global Configuration Use the Security > DHCP Snooping (Configure Global) page to enable DHCP Snooping globally on the switch, or to configure MAC Address Verification.

Parameters

These parameters are displayed:

General

- ◆ **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)

Information

- ◆ **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 Security, 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 snooping information option.
4. Click Apply

Figure 191: Configuring Global Settings for DHCP Snooping

The screenshot shows the 'Security > DHCP Snooping' configuration page. The 'Step' dropdown is set to '1. Configure Global'. The 'General' section has 'DHCP Snooping Status' set to 'Enabled' and 'DHCP Snooping MAC-Address Verification' checked and set to 'Enabled'. The 'Information' section has 'DHCP Snooping Information Option Status' set to 'Enabled', 'DHCP Snooping Information Option Sub-option Format' set to 'Extra Subtype Included', 'DHCP Snooping Information Option Remote ID' set to 'MAC Address (Hex Encoded)', and 'DHCP Snooping Information Option Policy' set to 'Replace'. There are 'Apply' and 'Revert' buttons at the bottom right.

DHCP Snooping VLAN Configuration Use the Security > DHCP Snooping (Configure VLAN) page to enable or disable DHCP snooping on specific VLANs.

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: 1-4094)
- ◆ **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 Security, DHCP Snooping.
2. Select Configure VLAN from the Step list.
3. Enable DHCP Snooping on any existing VLAN.
4. Click Apply

Figure 192: Configuring DHCP Snooping on a VLAN

The screenshot shows a web interface titled "Security > DHCP Snooping". Below the title is a "Step:" dropdown menu with "2. Configure VLAN" selected. The main area contains two fields: "VLAN" with a dropdown menu showing "1", and "DHCP Snooping Status" with a checked checkbox labeled "Enabled". At the bottom right, there are two buttons: "Apply" and "Revert".

Configuring Ports for DHCP Snooping

Use the Security > DHCP Snooping (Configure Interface) page to configure switch ports as trusted or untrusted.

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)
- ◆ **Max Number** – The maximum number of DHCP clients which can be supported per interface. (Range: 1-32; Default: 16)
- ◆ **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 Security, DHCP Snooping.
2. Select Configure Interface from the Step list.
3. Display the list of ports or trunks.
4. Configure the trust status, maximum number of supported clients, and the circuit identifier.
5. Click Apply

Figure 193: Configuring the Port Mode for DHCP Snooping

Security > DHCP Snooping

Step: 3. Configure Interface

Interface: ☒ Port ☐ Trunk

DHCP Snooping Port List Total: 28

Port	Trust Status	Max Number (1 - 32)	Circuit ID	
			Mode	Value
1	☐ Enabled	16	VLAN-Unit-Port	
2	☐ Enabled	16	VLAN-Unit-Port	
3	☐ Enabled	16	VLAN-Unit-Port	
4	☐ Enabled	16	VLAN-Unit-Port	
5	☐ Enabled	16	VLAN-Unit-Port	

Displaying DHCP Snooping Binding Information

Use the Security > DHCP Snooping (Show Information) page to display entries in the binding table.

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 Security, DHCP Snooping.
2. Select Show Information from the Step list.
3. Use the Store or Clear function if required.

Figure 194: Displaying the Binding Table for DHCP Snooping

Security > DHCP Snooping

Step: 4. Show Information

DHCP Snooping Binding List Total: 6

	MAC Address	IP Address	Lease Time (seconds)	Type	VLAN	Interface
☐	00-11-3B-F4-00-01	10.2.44.96	5	DHCP-Snooping	1	Trunk 1
☐	00-11-3B-F4-00-02	10.3.44.96	15	BOOTP-Snooping	1	Unit 1 / Port 2
☐	00-11-3B-F4-00-03	10.4.44.96	25	DHCP-Snooping	1	Unit 1 / Port 3
☐	00-11-3B-F4-00-04	10.5.44.96	10	BOOTP-Snooping	1	Trunk 4
☐	00-11-3B-F4-00-05	10.6.44.96	10	DHCP-Snooping	1	Unit 1 / Port 5
☐	00-11-3B-F4-00-06	10.7.44.96	5	BOOTP-Snooping	1	Unit 1 / Port 6

Clear

Store To Flash

Clear From Flash

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.

Parameters

These parameters are displayed:

- ◆ **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: Disabled)
- ◆ **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: Disabled)
- ◆ **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: Disabled)

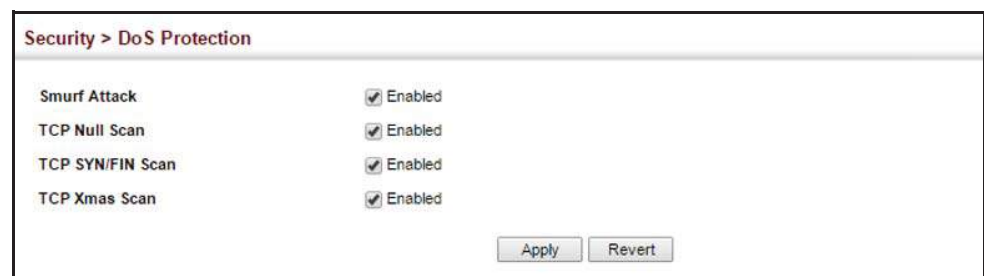
- ◆ **TCP Xmas Scan** – A so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. (Default: Disabled)

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 195: Protecting Against DoS Attacks



IPv4 Source Guard

IPv4 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 337](#)). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IPv4 address of a neighbor to access the network. This section describes how to configure IPv4 Source Guard.

Configuring Ports for IPv4 Source Guard

Use the Security > IP Source Guard > General page to set the filtering type based on source IP address, or source IP address and MAC address pairs. It also specifies lookup within the ACL binding table or the MAC address binding table, as well as the maximum number of allowed binding entries for the lookup tables.

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.

Command Usage

Filter Type

- ◆ 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 337](#)), 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.
- ◆ An entry with same MAC address and a different VLAN ID cannot be added to the binding table.
- ◆ Filtering rules are implemented as follows:
 - If DHCP snooping is disabled (see [page 340](#)), 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 allowed by DHCP snooping.

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)
 - **Disabled** – 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.
- ◆ **Filter Table** – Sets the source guard learning model to search for addresses in the ACL binding table or the MAC address binding table. (Default: ACL binding table)
- ◆ **Max Binding Entry** – The maximum number of entries that can be bound to an interface. (ACL Table: 1-5, Default: 5; MAC Table: 1-32, Default: 16)

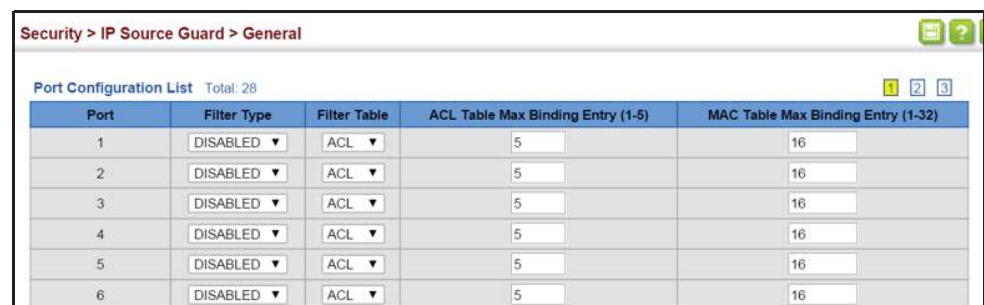
This parameter sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping (see [“DHCP Snooping” on page 337](#)) and static entries set by IP source guard (see [“Configuring Static Bindings for IPv4 Source Guard” on page 349](#)).

Web Interface

To set the IP Source Guard filter for ports:

1. Click Security, IP Source Guard, General.
2. Set the required filtering type, set the table type to use ACL or MAC address binding, and then set the maximum binding entries for each port.
3. Click Apply.

Figure 196: Setting the Filter Type for IPv4 Source Guard



The screenshot shows the 'Security > IP Source Guard > General' configuration page. It features a 'Port Configuration List' with a total of 28 ports. The table below displays the first six ports, all of which are currently disabled and configured to use the ACL filter table.

Port	Filter Type	Filter Table	ACL Table Max Binding Entry (1-5)	MAC Table Max Binding Entry (1-32)
1	DISABLED ▼	ACL ▼	5	16
2	DISABLED ▼	ACL ▼	5	16
3	DISABLED ▼	ACL ▼	5	16
4	DISABLED ▼	ACL ▼	5	16
5	DISABLED ▼	ACL ▼	5	16
6	DISABLED ▼	ACL ▼	5	16

Configuring Static Bindings for IPv4 Source Guard

Use the Security > IP Source Guard > Static Binding (Configure ACL Table and Configure MAC Table) pages 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.

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.
- ◆ Static addresses entered in the source guard binding table are automatically configured with an infinite lease time.
- ◆ 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.
- ◆ An entry with same MAC address and a different VLAN ID cannot be added to the binding table.
- ◆ Static bindings are processed as follows:
 - A valid static IP source guard entry will be added to the binding table in ACL mode if one of the following conditions is true:
 - If there is no 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.
 - A valid static IP source guard entry will be added to the binding table in MAC mode if one of the following conditions are true:
 - If there is no binding entry with the same IP address and MAC address, a new entry will be added to the binding table using the type of static IP source guard binding entry.
 - If there is a binding entry with same IP address and MAC address, then the new entry shall replace the old one.
 - Only unicast addresses are accepted for static bindings.

Parameters

These parameters are displayed:

Add – Configure ACL Table

- ◆ **Port** – The port to which a static entry is bound.
- ◆ **VLAN** – ID of a configured VLAN (Range: 1-4094)
- ◆ **MAC Address** – A valid unicast MAC address.
- ◆ **IP Address** – A valid unicast IP address, including classful types A, B or C.

Add – Configure MAC Table

- ◆ **MAC Address** – A valid unicast MAC address.
- ◆ **VLAN** – ID of a configured VLAN or a range of VLANs. (Range: 1-4094)
- ◆ **IP Address** – A valid unicast IP address, including classful types A, B or C.
- ◆ **Port** – The port to which a static entry is bound. Specify a 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)

Show

- ◆ **MAC Address** – Physical address associated with the entry.
- ◆ **IP Address** – IP address corresponding to the client.
- ◆ **VLAN** – VLAN to which this entry is bound.
- ◆ **Interface** – The port to which this entry is bound.

Web Interface

To configure static bindings for IP Source Guard:

1. Click Security, IP Source Guard, Static Binding.
2. Select Configure ACL Table or Configure MAC Table from the Step list.
3. Select Add from the Action list.
4. Enter the required bindings for each port.
5. Click Apply

Figure 197: Configuring Static Bindings for IPv4 Source Guard

To display static bindings for IP Source Guard:

1. Click Security, IP Source Guard, Static Binding.
2. Select Configure ACL Table or Configure MAC Table from the Step list.
3. Select Show from the Action list.

Figure 198: Showing Static Bindings for IPv4 Source Guard

MAC Address	IP Address	VLAN	Interface
00-11-3B-F4-D0-01	10.2.44.96	1	Unit 1 / Port 1

Displaying Information for Dynamic IPv4 Source Guard Bindings

Use the Security > IP Source Guard > Dynamic Binding page to display the source-guard binding table for a selected interface.

Parameters

These parameters are displayed:

Query by

- ◆ **Port** – A port on this switch. (Range: 1-28)
- ◆ **VLAN** – ID of a configured VLAN (Range: 1-4094)
- ◆ **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.
- ◆ **Type** – Entry types include DHCP-Snooping or BOOTP-Snooping.

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 199: Showing the IPv4 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	Type
1	00-11-3B-F4-00-11	Unit 1 / Port 2	10.2.44.96	DHCP
1	00-11-3B-F4-00-12	Unit 1 / Port 4	10.2.44.97	DHCP
2	00-11-3B-F4-00-13	Unit 1 / Port 7	10.2.44.98	DHCP

Basic Administration Protocols

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.
- ◆ **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.
- ◆ **Time Range** – Sets a time range during which various functions are applied, including applied ACLs or PoE
- ◆ **Loopback Detection (LBD)** – Detects general loopback conditions caused by hardware problems or faulty protocol settings.

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.

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 22: 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).

- ◆ **Command Log Status** – Records the commands executed from the CLI, including the execution time and information about the CLI user including the user name, user interface (console port, telnet or SSH), and user IP address. The severity level for this record type is 6 (a number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service).

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 200: 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

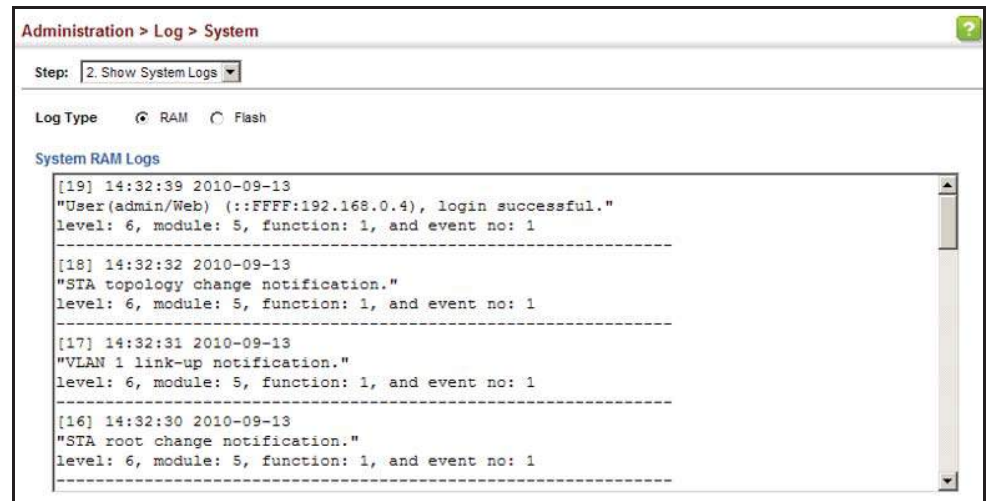
To show the error messages logged to system or flash memory:

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 201: 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.

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** - Specifies the UDP port number used by the remote server.
(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 202: Configuring Settings for Remote Logging of Error Messages

The screenshot shows the 'Administration > Log > Remote' configuration page. It includes the following fields and controls:

- Remote Log Status:** A checkbox labeled 'Enabled' which is currently unchecked.
- Logging Facility:** A dropdown menu showing '23 - Local use 7'.
- Logging Trap Level:** A dropdown menu showing '0 - System unusable'.
- Server IP Address 1:** A text input field containing '192.168.0.4'.
- Port:** A text input field containing '514'.
- Server IP Address 2:** An empty text input field.
- Port:** An empty text input field.
- Server IP Address 3:** An empty text input field.
- Port:** An empty text input field.
- Server IP Address 4:** An empty text input field.
- Port:** An empty text input field.
- Server IP Address 5:** An empty text input field.
- Port:** An empty text input field.

At the bottom right, there are two buttons: 'Apply' and '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.

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 354](#)) 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. (Range: 1-41 characters)
- ◆ **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 203: Configuring SMTP Alert Messages

The screenshot shows the 'Administration > Log > SMTP' configuration page. It includes the following fields and controls:

- SMTP Status:** A checkbox labeled 'Enabled' which is checked.
- Severity:** A dropdown menu currently set to '3 - Error'.
- E-mail Source Address:** A text input field containing 'big-wheels@matel.com'.
- E-mail Destination Address 1:** A text input field containing 'chris@matel.com'.
- E-mail Destination Address 2:** An empty text input field.
- E-mail Destination Address 3:** An empty text input field.
- E-mail Destination Address 4:** An empty text input field.
- E-mail Destination Address 5:** An empty text input field.
- Server IP Address 1:** A text input field containing '192.168.1.4'.
- Server IP Address 2:** An empty text input field.
- Server IP Address 3:** An empty text input field.

At the bottom right of the form are two buttons: 'Apply' and '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.

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 $4 \times 30 = 120$ 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 `IldpStatsRemTableLastChangeTime` to detect any `IldpRemTablesChange` 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 204: Configuring LLDP Timing Attributes

The screenshot shows the 'Administration > LLDP' configuration page. At the top, there is a breadcrumb trail 'Administration > LLDP'. Below it, a 'Step:' dropdown menu is set to '1. Configure Global'. The main configuration area is titled 'LLDP' and includes a checkbox labeled 'Enabled' which is checked. Below this, several timing attributes are listed with input fields and units:

- 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

At the bottom, there is a note: 'Note: The Transmission Interval must be greater than or equal to 4 times the Delay Interval.' and two buttons: 'Apply' and 'Revert'.

Configuring LLDP Interface Attributes

Use the Administration > LLDP (Configure Interface - Configure General) 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.

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: Enabled)

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 402.

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.

- ◆ **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. (Default: Enabled)

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. (Default: Enabled)
- **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. (Default: Enabled)
- **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. (Default: Enabled)
- **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 104](#). (Default: Enabled)

◆ **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 190](#)). (Default: Enabled)

- **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 181](#)). (Default: Enabled)
- **VLAN Name** – The name of all VLANs to which this interface has been assigned (see [“IEEE 802.1Q VLANs” on page 181](#)). (Default: Enabled)
- **Port and Protocol VLAN ID** – The port-based protocol VLANs configured on this interface (see [“Protocol VLANs” on page 190](#)). (Default: Enabled)
- ◆ **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. (Default: Enabled)
 - **Max Frame Size** – The maximum frame size. (See [“Configuring Support for Jumbo Frames” on page 106](#) for information on configuring the maximum frame size for this switch. (Default: Enabled)
 - **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. (Default: Enabled)
 - **PoE** – 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. (Default: Enabled)
- ◆ **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. (Default: Enabled)
 - **Extended Power** – 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). (Default: Enabled)
 - **Inventory** – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information. (Default: Enabled)
 - **Location** – This option advertises location identification details. (Default: Enabled)

- **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. (Default: Enabled)
- ◆ **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.)

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 205: Configuring LLDP Interface Attributes

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.

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 23: 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

Table 23: LLDP MED Location CA Types (Continued)

CA Type	Description	CA Value Example
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:

- ◆ **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.

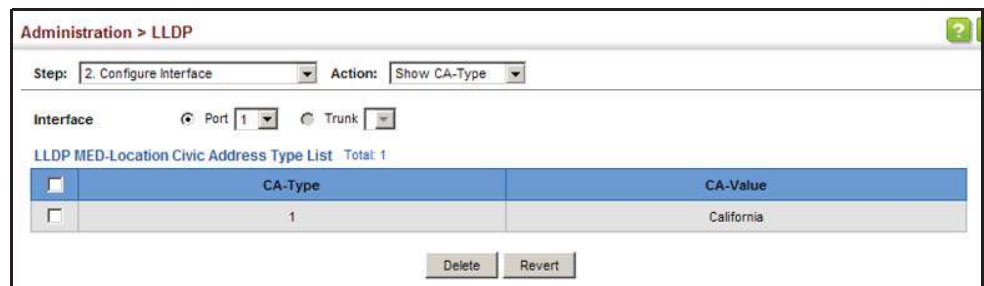
Figure 206: Configuring the Civic Address for an LLDP Interface

The screenshot shows the 'Administration > LLDP' configuration page. At the top, the 'Step' is set to '2. Configure Interface' and the 'Action' is 'Add CA-Type'. Below this, there are two radio buttons for 'Interface': 'Port' (selected) and 'Trunk'. The 'Port' dropdown shows '1'. The 'CA-Type (0-255)' field contains the value '1'. The 'CA-Value' field contains the text 'California'. At the bottom right, there are 'Apply' and 'Revert' buttons.

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 207: Showing the Civic Address for an LLDP Interface



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.

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 24: 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 104).
- ◆ **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 25: 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 26: 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 208: Displaying Local Device Information for LLDP (General)

Administration > LLDP

Step: 3. Show Local Device Information ▼

☒ General
 ☐ Port
 ☐ Port Details
 ☐ Trunk
 ☐ Trunk Details

LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	00-11-3B-11-22-33
System Name	
System Description	SP6528
System Capabilities Supported	Bridge
System Capabilities Enabled	Bridge
Management Address	192.168.2.10 (IPv4)

Figure 209: Displaying Local Device Information for LLDP (Port)

Administration > LLDP

Step: 3. Show Local Device Information ▼

☐ General
 ☒ Port
 ☐ Port Details
 ☐ Trunk
 ☐ Trunk Details

LLDP Local Device Port List Total: 28

Port	Port Description	Port ID
1	Ethernet Port on unit 1, port 1	00-11-3B-11-22-34
2	Ethernet Port on unit 1, port 2	00-11-3B-11-22-35
3	Ethernet Port on unit 1, port 3	00-11-3B-11-22-36
4	Ethernet Port on unit 1, port 4	00-11-3B-11-22-37
5	Ethernet Port on unit 1, port 5	00-11-3B-11-22-38

Figure 210: Displaying Local Device Information for LLDP (Port Details)

Administration > LLDP

Step: 3. Show Local Device Information ▼

☐ General
 ☐ Port
 ☒ Port Details
 ☐ Trunk
 ☐ Trunk Details

Port 1 ▼

LLDP Local Port Information Details

Local Port	1
Port ID Type	MAC Address
Port ID	00-11-3B-11-22-34
Port Description	Ethernet Port on unit 1, port 1
MED Capability	LLDP-MED Capabilities, Network Policy, Location Identification, Inventory

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.

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. (Range: 1-28)
- ◆ **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 24, "Chassis ID Subtype," on page 367.](#))
- ◆ **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 26, "Port ID Subtype," on page 369.](#)
- ◆ **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 25, "System Capabilities," on page 368.](#))
- ◆ **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. (See [Table 25, "System Capabilities," on page 368.](#))
- ◆ **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 27: 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

Table 27: Remote Port Auto-Negotiation Advertised Capability (Continued)

Bit	Capability
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 Capability⁷

- ◆ **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 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.

7. These fields are only displayed for end-node devices advertising LLDP-MED TLVs.

Port Details – Network Policy⁷

- ◆ **Application Type** – The primary application 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 Identification⁷

- ◆ **Location Data Format** – Any of these location ID data formats:
 - Coordinate-based LCI⁸ – Defined in RFC 3825, includes latitude resolution, latitude, longitude resolution, longitude, altitude type, altitude resolution, altitude, and datum.
 - Civic Address LCI⁸ – 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 and described under [“Configuring LLDP Interface Civic-Address.”](#)

8. Location Configuration Information

- 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 – Inventory⁷

- ◆ **Hardware Revision** – The hardware revision of the end-point device.
- ◆ **Software Revision** – The software revision of the end-point device.
- ◆ **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 211: 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 menu set to "4. Show Remote Device Information". Below this, there are four radio buttons: "Port" (selected), "Port Details", "Trunk", and "Trunk Details". A table titled "LLDP Remote Device Port List" with "Total: 1" is displayed. The table has four columns: "Local Port", "Chassis ID", "Port ID", and "System Name".

Local Port	Chassis ID	Port ID	System Name
1	00-11-3B-32-DD-FD	00-11-3B-32-DD-FF	RD93

Bottom Screenshot: This screenshot shows the same breadcrumb and step dropdown. The radio buttons are the same, but "Port Details" is selected. Below the radio buttons, there are two dropdown menus: "Port" with the value "1" and "Remote Index" with the value "2". A "Query" button is located at the bottom right of the form.

Figure 212: Displaying Remote Device Information for LLDP (Port Details)

Administration > LLDP

Step: 4. Show Remote Device Information

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	00-11-3B-00-00-01	Port ID	00-11-3B-00-00-02
System Name		System Capabilities Supported	Bridge
System Description	SP6528	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 213: 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.

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 214: Displaying LLDP Device Statistics (General)

The screenshot shows the 'Administration > LLDP' configuration page. The 'Step' dropdown is set to '5. Show Device Statistics'. Under the 'General' tab, the 'LLDP Device Statistics' section displays the following data:

Statistic	Value
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 215: Displaying LLDP Device Statistics (Port)

The screenshot shows the 'Administration > LLDP' configuration page with the 'Port' tab selected. The 'Step' dropdown is set to '5. Show Device Statistics'. The 'Port' dropdown is set to '3'. The 'LLDP Device Port Statistics' section displays the following data:

Statistic	Value	Statistic	Value
Frames Discarded	0	TLVs Unrecognized	0
Frames Invalid	0	TLVs Discarded	0
Frames Received	97	Neighbor Ageouts	0
Frames Sent	104		

A 'Refresh' button is located at the bottom right of the statistics section.

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 28: 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.

Parameters

These parameters are displayed:

- ◆ **Agent Status** – Enables SNMP on the switch. (Default: Enabled)
- ◆ **Authentication Traps⁹** – Issues a notification message to specified IP trap managers whenever an invalid community string is submitted during the SNMP access authentication process. (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 216: Configuring Global Settings for SNMP

The screenshot shows a web interface for configuring SNMP. The breadcrumb is 'Administration > SNMP'. Below it, a 'Step:' dropdown menu is set to '1. Configure Global'. There are two rows of settings: 'Agent Status' and 'Authentication Traps', each with a checked checkbox and the text 'Enabled'. 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.

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 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 Engine ID was last configured.

9. 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 387](#)).

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 217: Configuring the Local Engine ID for SNMP

The screenshot shows the 'Administration > SNMP' web interface. At the top, there is a breadcrumb trail 'Administration > SNMP'. Below it, there are two dropdown menus: 'Step: 3. Configure Engine' and 'Action: Set Engine ID'. The main form area contains two fields: 'Engine ID' with the value '800041ad03cc37abda6840000' and 'Engine Boots' with the value '6'. At the bottom right of the form, there are two buttons: 'Default' and '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.

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 399.](#))

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 IPv4 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 at least 9 hexadecimal characters, and the IP address of the remote host.
5. Click Apply

Figure 218: Configuring a Remote Engine ID for SNMP

The screenshot shows the 'Administration > SNMP' web interface. The 'Step' dropdown is set to '2. Configure Engine' and the 'Action' dropdown is set to 'Add Remote Engine'. There are two input fields: 'Remote Engine ID' with the value '5432100000' and 'Remote IP Host' with the value '192.168.1.19'. At the bottom right, there 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 219: Showing Remote Engine IDs for SNMP

The screenshot shows the 'Administration > SNMP' web interface. The 'Step' dropdown is set to '2. Configure Engine' and the 'Action' dropdown is set to 'Show Remote Engine'. Below the dropdowns, it says 'SNMPv3 Remote Engine List Total: 1'. There is a table with two columns: 'Remote Engine ID' and 'Remote IP Host'. The table contains one row with the values '5432100000' and '192.168.1.19'. At the bottom right, 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.

Parameters

These parameters are displayed:

Add View

- ◆ **View Name** – The name of the SNMP view. (Range: 1-32 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: 1-32 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 220: 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 221: Showing SNMP Views

Administration > SNMP

Step: 3. Configure View Action: Show View

SNMPv3 View List Total: 2

☐	View Name
☐	ifEntry.a
☐	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 222: Adding an OID Subtree to an SNMP View

The screenshot shows the 'Administration > SNMP' configuration page. The 'Step' dropdown is set to '3. Configure View' and the 'Action' dropdown is set to 'Add OID Subtree'. The 'View Name' dropdown is set to 'ifEntry.a'. The 'OID Subtree' text field contains '1.3.6.1.2.1.2.2.1.2.*'. The 'Type' dropdown is set to 'Included'. At the bottom right, there are 'Apply' and 'Revert' buttons.

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 223: Showing the OID Subtree Configured for SNMP Views

The screenshot shows the 'Administration > SNMP' configuration page. The 'Step' dropdown is set to '3. Configure View' and the 'Action' dropdown is set to 'Show OID Subtree'. The 'View Name' dropdown is set to 'ifEntry.a'. Below the dropdowns, the text 'SNMPv3 View OID Subtree List Total: 2' is displayed. A table with two columns, 'OID Subtree' and 'Type', shows two entries. Each entry has a checkbox in the first column. At the bottom right, there are 'Delete' and 'Revert' buttons.

	OID Subtree	Type
☐	1.3.6.1.2.1.2.2.1.1.*	Included
☐	1.3.6.1.2.1.2.2.1.2.*	Included

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.

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 29: 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.

Table 29: Supported Notification Messages (Continued)

Model	Level	Group
<i>Private Traps</i>		
swPowerStatusChangeTrap	1.3.6.1.4.1.16813.26.2.1.0.1	This trap is sent when the power state changes.
swPortSecurityTrap	1.3.6.1.4.1.16813.26.2.1.0.36	This trap is sent when the port is being intruded. This trap will only be sent when the portSecActionTrap is enabled.
swIpFilterRejectTrap	1.3.6.1.4.1.16813.26.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.
pethPsePortOnOffNotification	1.3.6.1.4.1.16813.26.2.1.0.43	This notification indicates if a PSE port is delivering power to the PD. This notification should be sent on every status change except in searching mode.
pethMainPowerUsageOnNotification	1.3.6.1.4.1.16813.26.2.1.0.45	This notification indicates PSE threshold usage indication is on; and the power usage is above the threshold.
pethMainPowerUsageOffNotification	1.3.6.1.4.1.16813.26.2.1.0.46	This notification indicates that the PSE threshold usage indication is off; and the usage power is below the threshold.
swAtcBcastStormAlarmFireTrap	1.3.6.1.4.1.16813.26.2.1.0.70	When broadcast traffic is detected as a storm, this trap is fired.
swAtcBcastStormAlarmClearTrap	1.3.6.1.4.1.16813.26.2.1.0.71	When a broadcast storm is detected as normal traffic, this trap is fired.
swAtcBcastStormTcApplyTrap	1.3.6.1.4.1.16813.26.2.1.0.72	When ATC is activated, this trap is fired.
swAtcBcastStormTcReleaseTrap	1.3.6.1.4.1.16813.26.2.1.0.73	When ATC is released, this trap is fired.
swAtcMcastStormAlarmFireTrap	1.3.6.1.4.1.16813.26.2.1.0.74	When multicast traffic is detected as the storm, this trap is fired.
swAtcMcastStormAlarmClearTrap	1.3.6.1.4.1.16813.26.2.1.0.75	When multicast storm is detected as normal traffic, this trap is fired.
swAtcMcastStormTcApplyTrap	1.3.6.1.4.1.16813.26.2.1.0.76	When ATC is activated, this trap is fired.
swAtcMcastStormTcReleaseTrap	1.3.6.1.4.1.16813.26.2.1.0.77	When ATC is released, this trap is fired.
stpBpduGuardPortShutdownTrap	1.3.6.1.4.1.16813.26.2.1.0.91	This trap will be sent when an interface is shut down because of BPDU guard.
swLoopbackDetectionTrap	1.3.6.1.4.1.16813.26.2.1.0.95	This trap is sent when loopback BPDUs have been detected.
dot1agCfmMepUpTrap	1.3.6.1.4.1.16813.26.2.1.0.97	This trap is sent when a new remote MEP is discovered.
dot1agCfmMepDownTrap	1.3.6.1.4.1.16813.26.2.1.0.98	This trap is sent when port status or interface status TLV received from remote MEP indicates it is not up.
dot1agCfmConfigFailTrap	1.3.6.1.4.1.16813.26.2.1.0.99	This trap is sent when a MEP receives a CCM with MPID which already exists on the same MA in this switch.
dot1agCfmLoopFindTrap	1.3.6.1.4.1.16813.26.2.1.0.100	This trap is sent when a MEP receives its own CCMs.
dot1agCfmMepUnknownTrap	1.3.6.1.4.1.16813.26.2.1.0.101	This trap is sent when a CCM is received from an unexpected MEP.

Table 29: Supported Notification Messages (Continued)

Model	Level	Group
dot1agCfmMepMissingTrap	1.3.6.1.4.1.16813.26.2.1.0.102	This trap is sent when the cross-check enable timer expires and no CCMs were received from an expected (configured) MEP.
dot1agCfmMaUpTrap	1.3.6.1.4.1.16813.26.2.1.0.103	This trap is sent when all expected remote MEPs are up.
autoUpgradeTrap	1.3.6.1.4.1.16813.26.2.1.0.104	This trap is sent when auto upgrade is executed.
swCpuUtiRisingNotification	1.3.6.1.4.1.16813.26.2.1.0.107	This notification indicates that the CPU utilization has risen from <code>cpuUtiFallingThreshold</code> to <code>cpuUtiRisingThreshold</code> .
swCpuUtiFallingNotification	1.3.6.1.4.1.16813.26.2.1.0.108	This notification indicates that the CPU utilization has fallen from <code>cpuUtiRisingThreshold</code> to <code>cpuUtiFallingThreshold</code> .
swMemoryUtiRisingThreshold Notification	1.3.6.1.4.1.16813.26.2.1.0.109	This notification indicates that the memory utilization has risen from <code>memoryUtiFallingThreshold</code> to <code>memoryUtiRisingThreshold</code> .
swMemoryUtiFallingThreshold Notification	1.3.6.1.4.1.16813.26.2.1.0.110	This notification indicates that the memory utilization has fallen from <code>memoryUtiRisingThreshold</code> to <code>memoryUtiFallingThreshold</code> .
dhcpRogueServerAttackTrap	1.3.6.1.4.1.16813.26.2.1.0.114	This trap is sent when receiving a DHCP packet from a rouge server.
macNotificationTrap	1.3.6.1.4.1.16813.26.2.1.0.138	This trap is sent when there are changes of the dynamic MAC addresses on the switch.
lbdDetectionTrap	1.3.6.1.4.1.16813.26.2.1.0.141	This trap is sent when a loopback condition is detected by LBD.
lbdRecoveryTrap	1.3.6.1.4.1.16813.26.2.1.0.142	This trap is sent when a recovery is done by LBD.
sfpThresholdAlarmWarnTrap	1.3.6.1.4.1.16813.26.2.1.0.189	This trap is sent when the SFP's A/D quantity is not within alarm/warning thresholds.
userAuthenticationFailureTrap	1.3.6.1.4.1.16813.26.2.1.0.199	This trap will be triggered if authentication fails.
userAuthenticationSuccessTrap	1.3.6.1.4.1.16813.26.2.1.0.200	This trap will be triggered if authentication is successful.
loginTrap	1.3.6.1.4.1.16813.26.2.1.0.201	This trap is sent when user logs in.
logoutTrap	1.3.6.1.4.1.16813.26.2.1.0.202	This trap is sent when user logs out.
fileCopyTrap	1.3.6.1.4.1.16813.26.2.1.0.208	This trap is sent when file copy is executed. If the copy action is triggered by the system, the login user information (<code>trapVarLoginUserName/</code> <code>trapVarSessionType/</code> <code>trapVarLoginInetAddressTypes/</code> <code>trapVarLoginInetAddress</code>) will be a null value.
userauthCreateUserTrap	1.3.6.1.4.1.16813.26.2.1.0.209	This trap is sent when a user account is created.
userauthDeleteUserTrap	1.3.6.1.4.1.16813.26.2.1.0.210	This trap is sent when a user account is deleted.
userauthModifyUserPrivilegeTrap	1.3.6.1.4.1.16813.26.2.1.0.211	This trap is sent when user privilege is modified.

Table 29: Supported Notification Messages (Continued)

Model	Level	Group
cpuGuardControlTrap	1.3.6.1.4.1.16813.26.2.1.0.213	This trap is sent when CPU utilization rises above the high-watermark the first time or when CPU utilization rises from below the low-watermark to above the high-watermark.
cpuGuardReleaseTrap	1.3.6.1.4.1.16813.26.2.1.0.214	This trap is sent when CPU utilization falls from above the high-watermark to below the low-watermark.

* 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 224: Creating an SNMP Group

Administration > SNMP

Step: 4. Configure Group Action: Add

Group Name:

Security Model:

Security Level:

Read View: ☒ ifEntry.a ☐

Write View: ☒ ifEntry.a ☐

Notify View: ☒ ifEntry.a ☐

Apply Revert

To show SNMP groups:

1. Click Administration, SNMP.
2. Select Configure Group from the Step list.
3. Select Show from the Action list.

Figure 225: Showing SNMP Groups

Administration > SNMP

Step: 4. Configure Group Action: Show

SNMPv3 Group List Total: 4

	Group Name	Model	Level	Read View	Write View	Notify View
☐	public	v1	noAuthNoPriv	defaultview	No writeview specified	No notifyview specified
☐	public	v2c	noAuthNoPriv	defaultview	No writeview specified	No notifyview specified
☐	private	v1	noAuthNoPriv	defaultview	defaultview	No notifyview specified
☐	private	v2c	noAuthNoPriv	defaultview	defaultview	No notifyview specified

Delete Revert

Setting Community Access Strings

Use the Administration > SNMP (Configure Community – Add) 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.

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 Community from the Step list.
3. Select Add 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 226: Setting Community Access Strings

The screenshot shows a web interface for configuring SNMP community strings. At the top, it says 'Administration > SNMP'. Below that, there's a 'Step:' dropdown menu set to '2. Configure Community' and an 'Action:' dropdown menu set to 'Add'. The main form has two fields: 'Community String' with the value 'spiderman' and 'Access Mode' with a dropdown menu set to 'Read/Write'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

To show the community access strings:

1. Click Administration, SNMP.
2. Select Configure Community from the Step list.
3. Select Show from the Action list.

Figure 227: Showing Community Access Strings

	Community String	Access Mode
☐	public	Read-Only
☐	private	Read/Write
☐	spiderman	Read/Write

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.

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. (Range: 8-32 characters)
- ◆ **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 228: Configuring Local SNMPv3 Users

The screenshot shows a web interface for configuring a local SNMPv3 user. The breadcrumb navigation at the top reads "Administration > SNMP". Below this, there are two dropdown menus: "Step:" set to "5. Configure User" and "Action:" set to "Add SNMPv3 Local User". The main configuration area is titled "SNMPv3 User" and contains several sections:

- SNMPv3 User**
 - User Name:** A text input field containing "chris".
 - Group Name:** Two radio buttons are present. The first is labeled "public" and is selected. The second is labeled "r&d".
 - Security Model:** A dropdown menu set to "v3".
 - Security Level:** A dropdown menu set to "authPriv".
- User Authentication**
 - Authentication Protocol:** A dropdown menu set to "MD5".
 - Authentication Password:** A text input field containing "greenpeace".
- Data Privacy**
 - Privacy Protocol:** A dropdown menu set to "DES56".
 - Privacy Password:** A text input field containing "einstien".

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

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 229: Showing Local SNMPv3 Users

Administration > SNMP

Step: 5. Configure User Action: Show SNMPv3 Local User

SNMPv3 Local User List Total: 1

	User Name	Group Name	Model	Level	Authentication	Privacy
☐	chris	r&d	v3	authPriv	MD5	DES56

Delete Revert

To change a local SNMPv3 local user group:

1. Click Administration, SNMP.
2. Select Change SNMPv3 Local User Group from the Action list.
3. Select the User Name.
4. Enter a new group name.
5. Click Apply

Figure 230: Changing a Local SNMPv3 User Group

Administration > SNMP

Step: 5. Configure User Action: Change SNMPv3 Local User Group

User Name: chris

Group Name: ☒ bart ☐ public

Apply 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.

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 402](#) and [“Specifying a Remote Engine ID” on page 385.](#))

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** – IPv4 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 231: Configuring Remote SNMPv3 Users

The screenshot shows the 'Administration > SNMP' configuration page. At the top, the 'Step' is set to '5. Configure User' and the 'Action' is 'Add SNMPv3 Remote User'. The configuration is divided into three sections: 'SNMPv3 User', 'User Authentication', and 'Data Privacy'. In the 'SNMPv3 User' section, 'User Name' is 'mark', 'Group Name' is 'public' (selected with a radio button), 'Remote IP' is '192.168.1.19', 'Security Model' is 'v3', and 'Security Level' is 'authPriv'. In the 'User Authentication' section, 'Authentication Protocol' is 'MD5' and 'Authentication Password' is 'greenpeace'. In the 'Data Privacy' section, 'Privacy Protocol' is 'DES56' and 'Privacy Password' is 'einstien'. 'Apply' and 'Revert' buttons are at the bottom right.

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 232: Showing Remote SNMPv3 Users

Administration > SNMP

Step: 5. Configure User Action: Show SNMPv3 Remote User

SNMPv3 Remote User List Total: 1

☐	User Name	Group Name	Engine ID	Model	Level	Authentication	Privacy
☐	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.

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 383](#)).
2. Create a view with the required notification messages ([page 387](#)).
3. Configure the group (matching the community string specified on the Configure Trap - Add page) to include the required notify view ([page 389](#)).
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 383](#)).
2. Create a remote SNMPv3 user to use in the message exchange process ([page 397](#)). 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 remote user, and default settings for the read, write, and notify view.
3. Create a view with the required notification messages ([page 387](#)).
4. Create a group that includes the required notify view ([page 389](#)).
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 397](#)), 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 399](#)), 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 233: Configuring Trap Managers (SNMPv1)

The screenshot shows the 'Administration > SNMP' web interface. At the top, there is a breadcrumb trail. Below it, a 'Step:' dropdown is set to '6. Configure Trap' and an 'Action:' dropdown is set to 'Add'. The main configuration area contains four 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 'Apply' and 'Revert' buttons.

Figure 234: Configuring Trap Managers (SNMPv2c)

The screenshot shows the 'Administration > SNMP' web interface for SNMPv2c. The 'Step:' dropdown is set to '6. Configure Trap' and the 'Action:' dropdown is set to 'Add'. The configuration fields include: 'IP Address' with '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 'centiseconds' unit, 'Retry Times (0-255)' with an empty field, 'Community String' with 'venus', and 'UDP Port (1-65535)' with an empty field. 'Apply' and 'Revert' buttons are at the bottom right.

Figure 235: 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 236: 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
☐	192.168.0.4	v3	steve	162	noAuthNoPriv		
☐	192.168.0.5	v3	bobby	162	noAuthNoPriv		
☐	192.168.0.6	v3	betty	162	authNoPriv		
☐	192.168.2.9	v2c	venue	162		1600	5
☐	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.

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 Inform messages 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 110](#). 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 402](#), a default notify filter will be created.

Parameters

These parameters are displayed:

- ◆ **IP Address** – The IPv4 or IPv6 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 237: 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 238: Showing SNMP Notification Logs

Administration > SNMP

Step: 7. Configure Notify Filter Action: Show

SNMP Notify Filter List Total: 1

	Filter profile name	IP Address
☐	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.

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 239: 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.

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: 1-32 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 240: Configuring an RMON Alarm

The screenshot shows the 'Administration > RMON' web interface. At the top, there are two dropdown menus: 'Step: 1. Configure Global' and 'Action: Add'. Below these, there are two radio buttons: 'Alarm' (selected) and 'Event'. The main configuration area contains several fields with labels and values:

Index (1-65535)	1
Variable	6.1
Interval (1-31622400)	15 sec
Sample Type	Delta
Rising Threshold (0-2147483647)	100
Rising Event Index (0-65535)	30
Falling Threshold (0-2147483647)	1
Falling Event Index (0-65535)	2
Owner	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 241: Showing Configured RMON Alarms

	Index	Status	Variable	Interval	Type	Last Value	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner
☐	1	Valid	1.3.6.1.2.1.16.1.1.1.6.1	30	Delta	0	892800	0	446400	0	
☐	2	Valid	1.3.6.1.2.1.16.1.1.1.6.2	30	Delta	0	892800	0	446400	0	
☐	3	Valid	1.3.6.1.2.1.16.1.1.1.6.3	30	Delta	0	892800	0	446400	0	
☐	4	Valid	1.3.6.1.2.1.16.1.1.1.6.4	30	Delta	0	892800	0	446400	0	
☐	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.

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 354](#)).
 - **Trap** – Sends a trap message to all configured trap managers (see [“Specifying Trap Managers” on page 402](#)).
 - **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 396](#)) prior to configuring it here. (Range: 1-32 characters)
- ◆ **Description** – A comment that describes this event. (Range: 1-127 characters)
- ◆ **Owner** – Name of the person who created this entry. (Range: 1-32 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 242: Configuring an RMON Event

The screenshot shows the 'Administration > RMON' configuration page. At the top, the 'Step' is set to '1. Configure Global' and the 'Action' is 'Add'. Below this, there are radio buttons for 'Alarm' and 'Event', with 'Event' selected. The configuration fields are as follows:

- Index (1-65535): 2
- Type: Log and Trap
- Community: private
- Description: for software group
- Owner: david

At the bottom right, there are 'Apply' and 'Revert' buttons.

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 243: Showing Configured RMON Events

The screenshot shows the 'Administration > RMON' configuration page with the 'Action' set to 'Show'. Below the configuration fields, there is a table titled 'RMON Event List' with a total of 4 events. The table has columns for Index, Status, Type, Community, Description, Owner, and Last Fired. Below the table are 'Delete' and 'Revert' buttons.

	Index	Status	Type	Community	Description	Owner	Last Fired
☐	1	Valid	None		None	None	00:00:00
☐	2	Valid	Log		Log	Log	00:00:00
☐	3	Valid	Trap	Trap	Trap	Trap	00:00:00
☐	4	Valid	Log and Trap	Log and Trap	Log and Trap	Log and Trap	00:00:00

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.

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 142](#).
- ◆ 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. (Range: 1-28)
- ◆ **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: 8)

The number of buckets granted are displayed on the Show page.
- ◆ **Owner** - Name of the person who created this entry. (Range: 1-32 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 244: 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 245: 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
☐	1	Valid	1800	8	8	
☐	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 246: 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.

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:

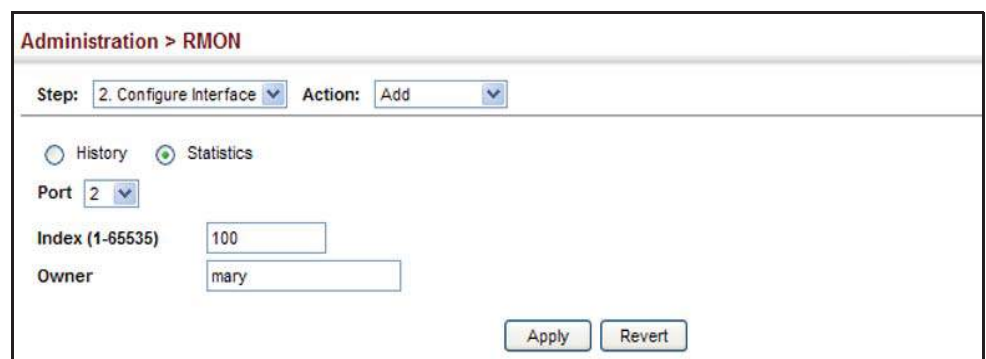
- ◆ **Port** – The port number on the switch. (Range: 1-28)
- ◆ **Index** - Index to this entry. (Range: 1-65535)
- ◆ **Owner** - Name of the person who created this entry. (Range: 1-32 characters)

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 247: Configuring an RMON Statistical Sample



The screenshot shows a web interface for configuring RMON. The breadcrumb navigation at the top reads "Administration > RMON". Below this, there are two dropdown menus: "Step:" set to "2. Configure Interface" and "Action:" set to "Add". Underneath, there are two radio buttons: "History" (unselected) and "Statistics" (selected). Below the radio buttons, there are three input fields: "Port" with a dropdown menu showing "2", "Index (1-65535)" with a text box containing "100", and "Owner" with a text box containing "mary". 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 248: Showing Configured RMON Statistical Samples

The screenshot shows the 'Administration > RMON' page. At the top, there's a breadcrumb 'Administration > RMON'. Below it, a 'Step:' dropdown is set to '2. Configure Interface' and an 'Action:' dropdown is set to 'Show'. There are radio buttons for 'History' and 'Statistics', with 'Statistics' selected. A 'Port' dropdown is set to '2'. Below this, a section titled 'RMON Statistics Port List' shows 'Total: 2'. It contains a table with columns: Index, Status, and Owner. The table has two rows: Index 1 with Status 'Valid' and Owner 'abc'; Index 2 with Status 'Valid' and Owner 'test'. At the bottom right, there are 'Delete' and 'Revert' buttons.

Index	Status	Owner
1	Valid	abc
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 249: Showing Collected RMON Statistical Samples

The screenshot shows the 'Administration > RMON' page. At the top, there's a breadcrumb 'Administration > RMON'. Below it, a 'Step:' dropdown is set to '2. Configure Interface' and an 'Action:' dropdown is set to 'Show Details'. There are radio buttons for 'History' and 'Statistics', with 'Statistics' selected. A 'Port' dropdown is set to '2'. Below this, a section titled 'RMON Statistics Port Details' displays various statistics in two columns. The first column lists statistics like 'Received Octets', 'Received Packets', 'Broadcast Packets', etc. The second column lists statistics like 'Collisions', 'Drop Events', 'Frames of 64 Octets', etc. At the bottom right, there is a 'Refresh' button.

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		

Setting a Time Range

Use the Administration > Time Range page to set a time range during which various functions are applied, including applied ACLs.

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.
- ◆ A maximum of eight rules can be configured for a time range.

Parameters

These parameters are displayed:

Add

- ◆ **Time-Range Name** – Name of a time range. (Range: 1-32 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 Administration, Time Range.
2. Select Add from the Action list.
3. Enter the name of a time range.
4. Click Apply.

Figure 250: Setting the Name of a Time Range

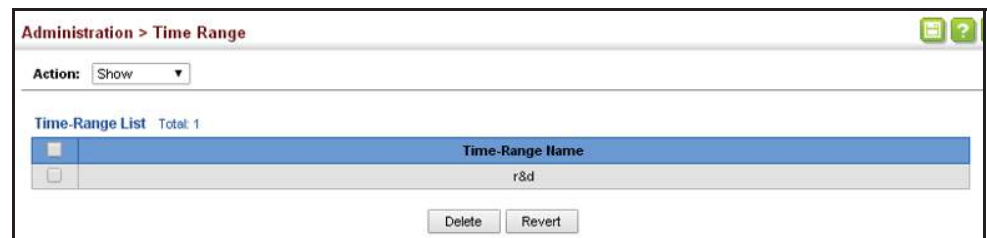


The screenshot shows the 'Administration > Time Range' page. At the top, there is a breadcrumb trail. Below it, an 'Action:' dropdown menu is set to 'Add'. Underneath, the 'Time-Range Name' label is followed by a text input field containing the text 'r&d'. At the bottom right of the form, there are two buttons: 'Apply' and 'Revert'.

To show a list of time ranges:

1. Click Administration, Time Range.
2. Select Show from the Action list.

Figure 251: Showing a List of Time Ranges



The screenshot shows the 'Administration > Time Range' page with the 'Action:' dropdown set to 'Show'. Below the dropdown, there is a section titled 'Time-Range List' with a 'Total: 1' indicator. A table displays the list with one entry: 'r&d'. The table has a checkbox in the first column and a 'Time-Range Name' header. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Time-Range Name
☐	r&d

To configure a rule for a time range:

1. Click Administration, Time Range.
2. Select Add Rule from the Action list.
3. Select the name of time range from the drop-down list.
4. Select a mode option of Absolute or Periodic.
5. Fill in the required parameters for the selected mode.
6. Click Apply.

Figure 252: Add a Rule to a Time Range

Administration > Time Range

Action: Add Rule ▼

Time-Range: r&d ▼

Mode: Periodic ▼

Start

Days of the week: vWeekend ▼

Hours (0-23): 5

Minutes (0-59): 0

To

Days of the week: Sunday ▼

Hours (0-23): 6

Minutes (0-59): 0

Apply Revert

To show the rules configured for a time range:

1. Click Administration, Time Range.
2. Select Show Rule from the Action list.

Figure 253: Showing the Rules Configured for a Time Range

Administration > Time Range

Action: Show Rule ▼

Time-Range: r&d ▼

Time-Range Rule List Total: 1

	Mode	Start	End
☐	Periodic	Weekend 05:00	Weekend 06:00

Delete Revert

LBD Configuration

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.

Usage Guidelines

- ◆ The default settings for the control frame transmit interval and recover time may be adjusted to improve performance for your specific environment. The shutdown mode may also need to be changed once you determine what kind of packets are being looped back.
- ◆ General loopback detection provided by the commands described in this section and loopback detection provided by the spanning tree protocol cannot both be enabled at the same time. If loopback detection is enabled for the

spanning tree protocol, general loopback detection cannot be enabled on the same interface.

- ◆ When a loopback event is detected on an interface or when a interface is released from a shutdown state caused by a loopback event, a trap message is sent and the event recorded in the system log.
- ◆ Loopback detection must be enabled both globally and on an interface for loopback detection to take effect.

Configuring Global Settings for LBD

Use the Administration > LBD (Configure Global) page to enable loopback detection globally, specify the interval at which to transmit control frames, the interval to wait before releasing an interface from shutdown state, the response to a detected loopback, and the traps to send.

Parameters

These parameters are displayed:

- ◆ **Global Status** – Enables loopback detection globally on the switch. (Default: Enabled)
- ◆ **Transmit Interval** – Specifies the interval at which to transmit loopback detection control frames. (Range: 1-32767 seconds; Default: 10 seconds)
- ◆ **Recover Time** – Specifies the interval to wait before the switch automatically releases an interface from shutdown state. (Range: 60-1,000,000 seconds; Default: 60 seconds)

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 recover time is not enabled (checkbox unmarked), all ports placed in shutdown state can be restored to operation using the Release button. To restore a specific port, re-enable Admin status on the Configure Interface page.

- ◆ **Action** – Specifies the protective action the switch takes when a loopback condition is detected. (Options: None, Shutdown; Default: Shutdown)
 - **None** - No action is taken.
 - **Shutdown** – When the response to a detected loopback condition is set to shut down a port, and a port receives a control frame sent by itself, this means that the port is in looped state, and the VLAN in the frame payload is also in looped state with the wrong VLAN tag. The looped port is therefore shut down.

When the loopback detection response is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.

- ◆ **Trap** – Sends a trap when a loopback condition is detected, or when the switch recovers from a loopback condition. (Options: Both, Detect, None, Recover; Default: None)
 - **Both** – Sends an SNMP trap message when a loopback condition is detected, or when the switch recovers from a loopback condition.
 - **Detect** – Sends an SNMP trap message when a loopback condition is detected.
 - **None** – Does not send an SNMP trap for loopback detection or recovery.
 - **Recover** – Sends an SNMP trap message when the switch recovers from a loopback condition.
- ◆ **Release** – Releases all interfaces currently shut down by the loopback detection feature.

Web Interface

To configure global settings for LBD:

1. Click Administration, LBD, Configure Global.
2. Make the required configuration changes.
3. Click Apply.

Figure 254: Configuring Global Settings for LBD

The screenshot displays the 'Administration > LBD' configuration page. At the top, a 'Step:' dropdown menu is set to '1. Configure Global'. The main configuration area includes the following fields:

- Global Status:** A checkbox labeled 'Enabled' which is currently unchecked.
- Transmit Interval (1-32767):** A text input field containing the value '10', followed by the unit 'sec'.
- Recover Time (60-1000000):** A checked checkbox followed by a text input field containing the value '60', followed by the unit 'sec'.
- Action:** A dropdown menu currently showing 'Shutdown'.
- Trap:** A dropdown menu currently showing 'None'.

At the bottom right of the configuration area are two buttons: 'Apply' and 'Revert'. Below the main configuration area, there is a 'Release' button and a link that says 'Click this button to release all looped ports manually'.

Configuring Interface Settings for LBD

Use the Administration > LBD (Configure Interface) page to enable loopback detection on an interface, to display the loopback operational state, and the VLANs which are looped back.

Parameters

These parameters are displayed:

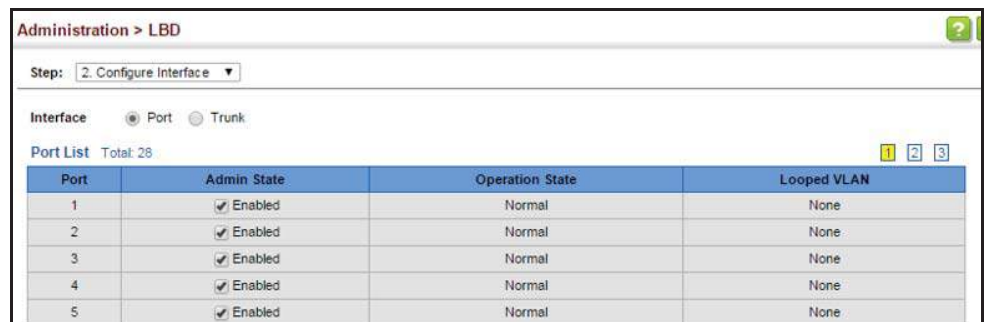
- ◆ **Interface** – Displays a list of ports or trunks.
 - **Port** – Port Identifier. (Range: 1-28)
 - **Trunk** – Trunk Identifier. (Range: 1-8)
- ◆ **Admin State** – Manually enables or disables an interface. (Default: Enabled)
- ◆ **Operation State** – Valid states include Normal or Looped.
- ◆ **Looped VLAN** – Shows the VLANs which are in looped state.

Web Interface

To configure interface settings for LBD:

1. Click Administration, LBD, Configure Interface.
2. Make the required configuration changes.
3. Click Apply.

Figure 255: Configuring Interface Settings for LBD



Port	Admin State	Operation State	Looped VLAN
1	✓ Enabled	Normal	None
2	✓ Enabled	Normal	None
3	✓ Enabled	Normal	None
4	✓ Enabled	Normal	None
5	✓ Enabled	Normal	None

Multicast Filtering

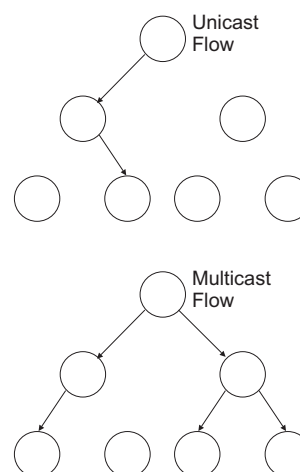
This chapter describes how to configure the following multicast services:

- ◆ **IGMP Snooping** – Configures snooping and query parameters.
- ◆ **Filtering and Throttling** – Filters specified multicast service, or throttles the maximum of multicast groups allowed on an interface.
- ◆ **MLD Snooping** – Configures snooping and query parameters for IPv6.

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 256: 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.

Layer 2 IGMP (Snooping and Query for IPv4)

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 430](#)) 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 434](#)). 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 430](#)).

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 434](#)). 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 436](#)).

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.

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: Disabled)

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 438](#)).

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: 0-7, where 7 is the highest priority; Default: Disabled)

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 257: Configuring General Settings for IGMP Snooping

Multicast > IGMP Snooping > General	
IGMP Snooping Status	☒ Enabled
Proxy Reporting Status	☐ Enabled
TCN Flood	☐ Enabled
TCN Query Solicit	☐ Enabled
Router Alert Option	☐ Enabled
Unregistered Data Flooding	☐ Enabled
Forwarding Priority (0-7)	☐
Version Exclusive	☐ Enabled
IGMP Unsolicited Report Interval (1-65535)	400 seconds
Router Port Expire Time (1-65535)	300 seconds
IGMP Snooping Version (1-3)	2
Querier Status	☐ Enabled

Specifying Static Interfaces for a Multicast Router

Use the Multicast > IGMP Snooping > Multicast Router (Add Static Multicast Router) 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.

Command Usage

IGMP Snooping must be enabled globally on the switch (see [“Configuring IGMP Snooping and Query Parameters” on page 430](#)) before a multicast router port can take effect.

Parameters

These parameters are displayed:

Add Static Multicast Router

- ◆ **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4094)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Trunk** – Specifies the interface attached to a multicast router.

Show Static Multicast Router

- ◆ **VLAN** – Selects the VLAN for which to display any configured static multicast routers.
- ◆ **Interface** – Shows the interface to which the specified static multicast routers are attached.

Show Current Multicast Router

- ◆ **VLAN** – Selects the VLAN for which to display any currently active multicast routers.
- ◆ **Interface** – Shows the interface to which an active multicast router is attached.
- ◆ **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 258: 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 radio buttons: 'Port' (selected) and 'Trunk'. The 'Port' radio button is followed by a dropdown menu showing '1'. There are 'Apply' and 'Revert' buttons at the bottom right.

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 259: 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'. There are 'Delete' and 'Revert' buttons at the bottom right.

	Interface
☐	Unit 1 / Port 1
☐	Unit 1 / Port 2
☐	Unit 1 / Port 3
☐	Trunk 2
☐	Trunk 5
☐	Unit 1 / Port 4

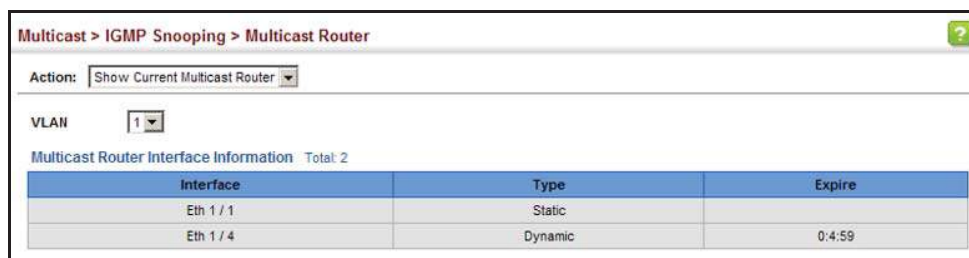
Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol (such as PIM) to support IP

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 260: Showing Current Interfaces Attached a Multicast Router



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 430](#)). 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.

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: 1-4094)
- ◆ **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 261: Assigning an Interface to a Multicast Service

The screenshot shows a web interface titled "Multicast > IGMP Snooping > IGMP Member". It contains a form with the following fields and options:

- Action:** A dropdown menu with "Add Static Member" selected.
- VLAN:** A dropdown menu with "1" selected.
- Interface:** Two radio buttons. The "Port" radio button is selected, and it is followed by a dropdown menu with "1" selected. The "Trunk" radio button is unselected, and it is followed by a dropdown menu with "1" selected.
- Multicast IP:** A text input field containing "224.1.1.1".
- Buttons:** "Apply" and "Revert" buttons at the bottom right.

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 262: 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
☐	Unit 1 / Port 1	224.1.1.1
☐	Unit 1 / Port 2	224.1.2.2
☐	Unit 1 / Port 3	230.1.1.1
☐	Trunk 2	230.1.2.2
☐	Trunk 5	239.1.1.1
☐	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 430.

Command Usage

Multicast Router Discovery

There have been many mechanisms used in the past to identify multicast routers. This has lead 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: 1-4094)
- ◆ **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 430](#)), 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. (Options: Enabled, Using Global Status; Default: Using Global Status)

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 or IGMPv3 snooping is used.

If immediate leave is enabled, the following options are provided:

- **By Group** – 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.
 - **By Host IP** – The switch will not send out a group-specific query when an IGMPv2/v3 leave message is received. But will check if there are other hosts joining the multicast group. Only when all hosts on that port leave the group will the member port be deleted.
- ◆ **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. (Options: Enabled, Disabled, Using Global Status; Default: Using Global Status)

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. (Options: 1-3, Using Global Version; Default: Using Global Version)

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 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 430](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 430](#)).

- ◆ **Query Response Interval** – The maximum time the system waits for a response to general queries. (Range: 10-31740 tenths of a second in multiples of 10; Default: 10 seconds)

This attribute applies when the switch is serving as the querier ([page 430](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 430](#)).

- ◆ **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 430](#)) or IGMP querier is enabled ([page 430](#)).

- ◆ **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 263: Configuring IGMP Snooping on a VLAN

Multicast > IGMP Snooping > Interface

Action: Configure VLAN

VLAN: 1

IGMP Snooping Status: ☒ Enabled

Version Exclusive: Using Global Status

Immediate Leave Status: ☐ Enabled By-Group

Multicast Router Discovery: ☐ Enabled

General Query Suppression: ☐ Enabled

Proxy Reporting: Using Global Status

Interface Version: Using Global Version

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 264: 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 or multicast data packets.

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.
- ◆ **Multicast Data Drop** – Configures an interface to stop multicast services from being forwarded to users attached to the downstream port (i.e., the interfaces specified by this command).

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 265: Dropping IGMP Query or Multicast Data Packets

Multicast > IGMP Snooping > Interface

Action: Configure Interface

Interface: ☒ Port ☐ Trunk

Port List Total: 28

Port	IGMP Query Drop	Multicast Data Drop
1	☐ Enabled	☐ Enabled
2	☐ Enabled	☐ Enabled
3	☐ Enabled	☐ Enabled
4	☐ Enabled	☐ Enabled
5	☐ Enabled	☐ 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.

Command Usage

To display information about multicast groups, IGMP Snooping must first be enabled on the switch (see [page 430](#)).

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.

Figure 266: Showing Multicast Groups Learned by IGMP Snooping

Multicast > IGMP Snooping > Forwarding Entry						
IGMP Snooping Forwarding Entry List Total: 10						
VLAN	Group Address	Source Address	Interface	Up Time	Expire	Count
1	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)
1	224.1.1.2	192.168.1.2	Eth 1 / 9 (Router Port)		02:24	1 (Port)
2	224.1.1.3	*	Eth 1 / 9 (Router Port)	00:00:16:14		1 (Port)
2	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.

Parameters

These parameters are displayed:

- ◆ **VLAN** – VLAN identifier. (Range: 1-4094)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Trunk** – Trunk identifier. (Range: 1-8)

Query Statistics

- ◆ **Other Querier** – IP address of remote querier on this interface.
- ◆ **Other Querier Expire** – Time after which remote querier is assumed to have expired.
- ◆ **Other Querier Uptime** – Time remote querier has been up.
- ◆ **Self Querier** – IP address of local querier on this interface.
- ◆ **Self Querier Expire** – Time after which local querier is assumed to have expired.
- ◆ **Self Querier Uptime** – Time local querier has been up.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Warn Rate Limit** – The rate at which received query messages of the wrong version type cause the Vx warning count to increment. Note that “0 sec” means that the Vx warning count is incremented for each wrong message version received.
- ◆ **V1 Warning Count** – The number of times the query version received (Version 1) does not match the version configured for this interface.
- ◆ **V2 Warning Count** – The number of times the query version received (Version 2) does not match the version configured for this interface.

- ◆ **V3 Warning Count** – The number of times the query version received (Version 3) does not match the version configured for this interface.

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 267: Displaying IGMP Snooping Statistics – Query

Action: Show Query Statistics

VLAN1

Query Statistics

Other Querier	None
Other Querier Expire	00(m):00(s)
Other Querier Uptime	00(h):00(m):00(s)
Self Querier	192.168.1.1
Self Querier Expire	00(m):00(s)
Self Querier Uptime	00(h):00(m):00(s)
General Query Received	0
General Query Sent	0
Specific Query Received	0
Specific Query Sent	0
Warn Rate Limit	0 sec.
V1 Warning Count	0
V2 Warning Count	0
V3 Warning Count	0

Clear All

Click this button to clear all IGMP Snooping statistics.

Refresh

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 268: Displaying IGMP Snooping Statistics – VLAN

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	0	Drop	0
Leave	0	Group	0
G Query	0		
G(-S)-S Query	0		

Clear 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 269: Displaying IGMP Snooping Statistics – Port

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.

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 270: 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.

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 271: Creating an IGMP Filtering Profile

The screenshot shows the 'Multicast > IGMP Snooping > Filter' configuration page. The 'Step' dropdown is set to '2. Configure Profile' and the 'Action' dropdown is set to 'Add'. The 'Profile ID (1-4294967295)' field contains the value '19'. The 'Access Mode' dropdown is set to 'Permit'. At the bottom right, there are 'Apply' and 'Revert' buttons.

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 272: Showing the IGMP Filtering Profiles Created

The screenshot shows the 'Multicast > IGMP Snooping > Filter' configuration page. The 'Step' dropdown is set to '2. Configure Profile' and the 'Action' dropdown is set to 'Show'. Below the configuration fields, there is a table titled 'IGMP Snooping Filter Profile List' with a 'Total: 1' count. The table has two columns: 'Profile ID' and 'Action Mode'. A single row is displayed with '19' in the 'Profile ID' column and 'Permit' in the 'Action Mode' column. At the bottom right, there are 'Delete' and 'Revert' buttons.

Profile ID	Action Mode
19	Permit

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 273: 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: 230.8.8.1

End Multicast IP Address: 230.8.8.200

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 274: 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
	230.8.8.1	230.8.8.200

Delete Revert

Configuring IGMP Filtering and Throttling for Interfaces

Use the Multicast > IGMP Snooping > Filter (Configure Interface) page to assign and 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.

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: 1-511; Default: 511)
- ◆ **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 275: 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 (1-511)	Current Multicast Groups	Throttling Action Mode	Throttling Status
1	19	511	0	Deny	False
2	(none)	511	0	Deny	False
3	(none)	511	0	Deny	False
4	(none)	511	0	Deny	False
5	(none)	511	0	Deny	False

MLD Snooping (Snooping and Query for IPv4)

Multicast Listener Discovery (MLD) snooping operates on IPv6 traffic and performs a similar function to IGMP snooping for IPv4. That is, MLD snooping dynamically configures switch ports to limit IPv6 multicast traffic so that it is forwarded only to ports with users that want to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs.

There are two versions of the MLD protocol, version 1 and version 2. MLDv1 control packets include Listener Query, Listener Report, and Listener Done messages (equivalent to IGMPv2 query, report, and leave messages). MLDv2 control packets include MLDv2 query and report messages, as well as MLDv1 report and done messages.

Remember that IGMP Snooping and MLD Snooping are independent functions, and can therefore both function at the same time.

Configuring MLD Snooping and Query Parameters

Use the Multicast > MLD Snooping > General page to configure the switch to forward multicast traffic intelligently. Based on the MLD 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.

Parameters

These parameters are displayed:

- ◆ **MLD Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. (Default: Disabled)
- ◆ **Querier Status** – When enabled, the switch can serve as the querier for MLDv2 snooping if elected. The querier is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)

An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses this IPv6 address as the query source address.

The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.

- ◆ **Robustness** – MLD Snooping robustness variable. A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report. (Range: 2-10 Default: 2)
- ◆ **Query Interval** – The interval between sending MLD general queries. (Range: 60-125 seconds; Default: 125 seconds)

This attribute applies when the switch is serving as the querier.

An MLD general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.
- ◆ **Query Max Response Time** – The maximum response time advertised in MLD general queries. (Range: 5-25 seconds; Default: 10 seconds)

This attribute controls how long the host has to respond to an MLD Query message before the switch deletes the group if it is the last member.
- ◆ **Router Port Expiry Time** – The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired. (Range: 300-500 seconds; Default: 300 seconds)
- ◆ **MLD Snooping Version** – The protocol version used for compatibility with other devices on the network. This is the MLD version the switch uses to send snooping reports. (Range: 1-2; Default: 2)
- ◆ **Unknown Multicast Mode** – The action for dealing with unknown multicast packets. Options include:
 - **Flood** – Floods any received IPv6 multicast packets that have not been requested by a host to all ports in the VLAN.
 - **To Router Port** – Forwards any received IPv6 multicast packets that have not been requested by a host to ports that are connected to a detected multicast router. (This is the default action.)

Web Interface

To configure general settings for MLD Snooping:

1. Click Multicast, MLD Snooping, General.
2. Adjust the settings as required.

3. Click Apply.

Figure 276: Configuring General Settings for MLD Snooping

Multicast > MLD Snooping > General

MLD Snooping Status	☐ Enabled
Querier Status	☐ Enabled
Robustness (2-10)	2
Query Interval (60-125)	125 seconds
Query Max Response Time (5-25)	10 seconds
Router Port Expiry Time (300-500)	300 seconds
MLD Snooping Version (1-2)	2
Unknown Multicast Mode	To Router Port

Apply Revert

Setting Immediate Leave Status for MLD Snooping per Interface

Use the Multicast > MLD Snooping > Interface page to configure Immediate Leave status for a VLAN.

Parameters

These parameters are displayed:

- ◆ **VLAN** – A VLAN identification number. (Range: 1-4094)
- ◆ **Immediate Leave Status** – Immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled)

If MLD immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.

If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.

Web Interface

To configure immediate leave for MLD Snooping:

1. Click Multicast, MLD Snooping, Interface.
2. Select a VLAN, and set the status for immediate leave.
3. Click Apply.

Figure 277: Configuring Immediate Leave for MLD Snooping



Multicast > MLD Snooping > Interface

VLAN 1

Immediate Leave Status ☐ Enabled

Apply Revert

Specifying Static Interfaces for an IPv6 Multicast Router

Use the Multicast > MLD Snooping > Multicast Router (Add Static Multicast Router) page to statically attach an interface to an IPv6 multicast router/switch.

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

Command Usage

MLD Snooping must be enabled globally on the switch (see [“Configuring MLD Snooping and Query Parameters” on page 455](#)) before a multicast router port can take effect.

Parameters

These parameters are displayed:

- ◆ **VLAN** – Selects the VLAN which is to propagate all IPv6 multicast traffic coming from the attached multicast router. (Range: 1-4094)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Trunk** – Specifies the interface attached to a multicast router.

Web Interface

To specify a static interface attached to a multicast router:

1. Click Multicast, MLD Snooping, Multicast Router.
2. Select Add Static Multicast Router from the Action list.
3. Select the VLAN which will forward all the corresponding IPv6 multicast traffic, and select the port or trunk attached to the multicast router.
4. Click Apply.

Figure 278: Configuring a Static Interface for an IPv6 Multicast Router

The screenshot shows the 'Multicast > MLD Snooping > Multicast Router' configuration page. The 'Action' dropdown is set to 'Add Static Multicast Router'. Below this, there is a 'VLAN' dropdown set to '1' and an 'Interface' section with radio buttons for 'Port' and 'Trunk'. The 'Port' radio button is selected, and a dropdown next to it is set to '1'. At the bottom right, there are 'Apply' and 'Revert' buttons.

To show the static interfaces attached to a multicast router:

1. Click Multicast, MLD Snooping, Multicast Router.
2. Select Show Static Multicast Router from the Action list.
3. Select the VLAN for which to display this information.

Figure 279: Showing Static Interfaces Attached an IPv6 Multicast Router

The screenshot shows the 'Multicast > MLD Snooping > Multicast Router' configuration page. The 'Action' dropdown is set to 'Show Static Multicast Router'. Below this, there is a 'VLAN' dropdown set to '1'. A table titled 'Static Multicast Router Interface List' with 'Total: 2' is displayed. The table has two columns: 'Interface' and 'Type'. The first column contains two entries: 'Unit 1 / Port 1' and 'Unit 1 / Port 2'. The second column is empty. At the bottom right, there are 'Delete' and 'Revert' buttons.

Interface	Type
Unit 1 / Port 1	
Unit 1 / Port 2	

To show all the interfaces attached to a multicast router:

1. Click Multicast, MLD 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 280: Showing Current Interfaces Attached an IPv6 Multicast Router

The screenshot shows the 'Multicast > MLD Snooping > Multicast Router' configuration page. The 'Action' dropdown is set to 'Show Current Multicast Router'. Below this, there is a 'VLAN' dropdown set to '1'. A table titled 'Multicast Router Interface Information' with 'Total: 4' is displayed. The table has two columns: 'Interface' and 'Type'. The first column contains four entries: 'Unit 1 / Port 4', 'Unit 1 / Port 5', 'Trunk 2', and 'Trunk 3'. The second column contains the corresponding types: 'Static', 'Dynamic', 'Dynamic', and 'Dynamic'.

Interface	Type
Unit 1 / Port 4	Static
Unit 1 / Port 5	Dynamic
Trunk 2	Dynamic
Trunk 3	Dynamic

Assigning Interfaces to IPv6 Multicast Services

Use the Multicast > MLD Snooping > MLD Member (Add Static Member) page to statically assign an IPv6 multicast service to an interface.

Multicast filtering can be dynamically configured using MLD snooping and query messages (see [“Configuring MLD Snooping and Query Parameters” on page 455](#)). 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.

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: 1-4094)
- ◆ **Multicast IPv6 Address** – The IP address for a specific multicast service.
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Trunk** – Specifies the interface assigned to a multicast group.
- ◆ **Type** (Show Current Member) – Shows if this multicast stream was statically configured by the user, discovered by MLD Snooping, or is a data stream to which no other ports are subscribing (i.e., the stream is flooded onto VLAN instead of being trapped to the CPU for processing, or is being processed by MVR6).

Web Interface

To statically assign an interface to an IPv6 multicast service:

1. Click Multicast, MLD Snooping, MLD 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 MLD-enabled switch or multicast router), and enter the multicast IP address.
4. Click Apply.

Figure 281: Assigning an Interface to an IPv6 Multicast Service

Multicast > MLD Snooping > MLD Member

Action: Add Static Member

VLAN: 1

Multicast IPv6 Address: FF00:0:0:0:0:10C

Interface: Port 1

Apply Revert

To show the static interfaces assigned to an IPv6 multicast service:

1. Click Multicast, MLD Snooping, MLD Member.
2. Select Show Static Member from the Action list.
3. Select the VLAN for which to display this information.

Figure 282: Showing Static Interfaces Assigned to an IPv6 Multicast Service

Multicast > MLD Snooping > MLD Member

Action: Show Static Member

VLAN: 1

MLD Member Interface List Total: 8

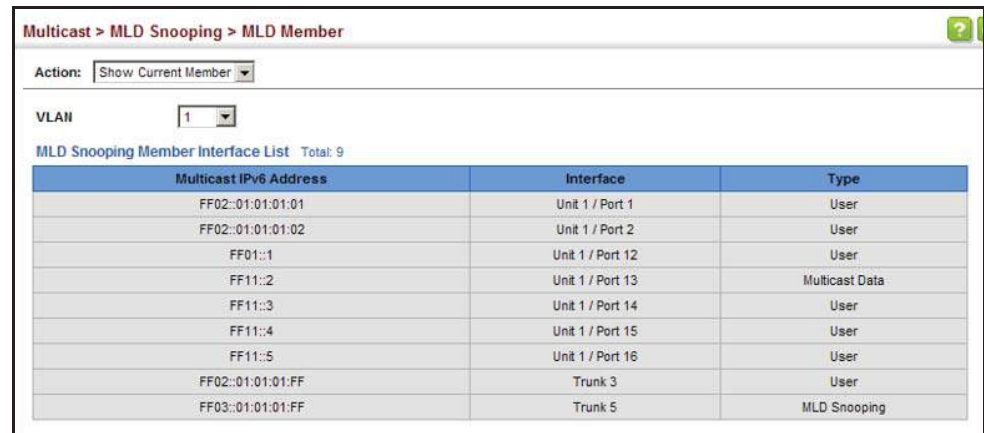
	Multicast IPv6 Address	Interface
☐	FF02::01:01:01:01	Unit 1 / Port 1
☐	FF02::01:01:01:02	Unit 1 / Port 2
☐	FF01::1	Unit 1 / Port 12
☐	FF01::2	Unit 1 / Port 13
☐	FF01::3	Unit 1 / Port 14
☐	FF01::4	Unit 1 / Port 15
☐	FF01::5	Unit 1 / Port 16
☐	FF02::01:01:01:FF	Trunk 3

Delete Revert

To display information about all IPv6 multicast groups, MLD Snooping or multicast routing must first be enabled on the switch. To show all of the interfaces statically or dynamically assigned to an IPv6 multicast service:

1. Click Multicast, MLD Snooping, MLD Member.
2. Select Show Current Member from the Action list.
3. Select the VLAN for which to display this information.

Figure 283: Showing Current Interfaces Assigned to an IPv6 Multicast Service



Multicast IPv6 Address	Interface	Type
FF02::01:01:01:01	Unit 1 / Port 1	User
FF02::01:01:01:02	Unit 1 / Port 2	User
FF01::1	Unit 1 / Port 12	User
FF11::2	Unit 1 / Port 13	Multicast Data
FF11::3	Unit 1 / Port 14	User
FF11::4	Unit 1 / Port 15	User
FF11::5	Unit 1 / Port 16	User
FF02::01:01:01:FF	Trunk 3	User
FF03::01:01:01:FF	Trunk 5	MLD Snooping

Showing MLD Snooping Groups and Source List

Use the Multicast > MLD Snooping > Group Information page to display known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.

Parameters

These parameters are displayed:

- ◆ **VLAN** – VLAN identifier. (Range: 1-4094)
- ◆ **Interface** – Port or trunk identifier.
- ◆ **Group Address** – The IP address for a specific multicast service.
- ◆ **Type** – The means by which each group was learned – MLD Snooping or Multicast Data.
- ◆ **Filter Mode** – The filter mode is used to summarize the total listening state of a multicast address to a minimum set such that all nodes' listening states are respected. In Include mode, the router only uses the request list, indicating that the reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the hosts' source-list. In Exclude mode, the router uses both the request list and exclude list, indicating that the reception of packets sent to the given multicast address is requested from all IP source addresses, except for those listed in the exclude source-list and for any other sources where the source timer status has expired.
- ◆ **Filter Timer Elapse** – The Filter timer is only used when a specific multicast address is in Exclude mode. It represents the time for the multicast address filter mode to expire and change to Include mode.
- ◆ **Request List** – Sources included on the router's request list.
- ◆ **Exclude List** – Sources included on the router's exclude list.

Web Interface

To display known MLD multicast groups:

1. Click Multicast, MLD Snooping, Group Information.
2. Select the port or trunk, and then select a multicast service assigned to that interface.

Figure 284: Showing IPv6 Multicast Services and Corresponding Sources

Multicast > MLD Snooping > Group Information

VLAN: 1

Interface: ☒ Port 1 ☐ Trunk 1

Group Address: FF02::01:01:01:01

Type: MLD Snooping

Filter Mode: Exclude

Filter Timer: 10 seconds

Elapse:

Request List Total: 3

IPv6 Address
::01:02:03:01
::01:02:03:02
::01:02:03:03

Exclude List Total: 3

IPv6 Address
::02:02:03:01
::02:02:03:02
::02:02:03:03

This chapter provides information on network functions including:

- ◆ **Ping** – Sends ping message to another node on the network.
- ◆ **Trace Route** – 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.

Using the Ping Function

Use the Tools > Ping page to send ICMP echo request packets to another node on the network.

Parameters

These parameters are displayed:

- ◆ **Host Name/IP Address** – Alias or IPv4/IPv6 address 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 Tools, Ping.
2. Specify the target device and ping parameters.
3. Click Apply.

Figure 285: Pinging a Network Device

The screenshot shows a web interface titled "Tool > Ping". It contains several input fields: "Host Name/IP Address" (empty), "Probe Count (1-16)" (set to 5), and "Data Size (IPv4 : 32-512, IPv6 : 0-1500)" (empty). Below these fields is a note: "Note: For IPv4 Data Size, 0 - 31 changed to 32 bytes, 32 - 512 is valid input, 513 - 1500 changed to 512 bytes, < 0 or > 1500 not valid input". There are "Apply" and "Revert" buttons. Below the configuration section is a "Result" section containing the following text:

```
PING to 192.168.2.99, by 5 of 32-byte payload ICMP packets, timeout is 3 seconds

response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms

Ping statistics for 192.168.2.99:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms
```

Using the Trace Route Function

Use the Tools > Trace Route page to show the route packets take to the specified destination.

Parameters

These parameters are displayed:

- ◆ **Destination IP Address** – Alias or IPv4/IPv6 address of the host.

- ◆ **IPv4 Max Failures** – The maximum number of failures before which the trace route is terminated. (Fixed: 5)
- ◆ **IPv6 Max Failures** – The maximum number of failures before which the trace route is terminated. (Range: 1-255; Default: 5)

Command Usage

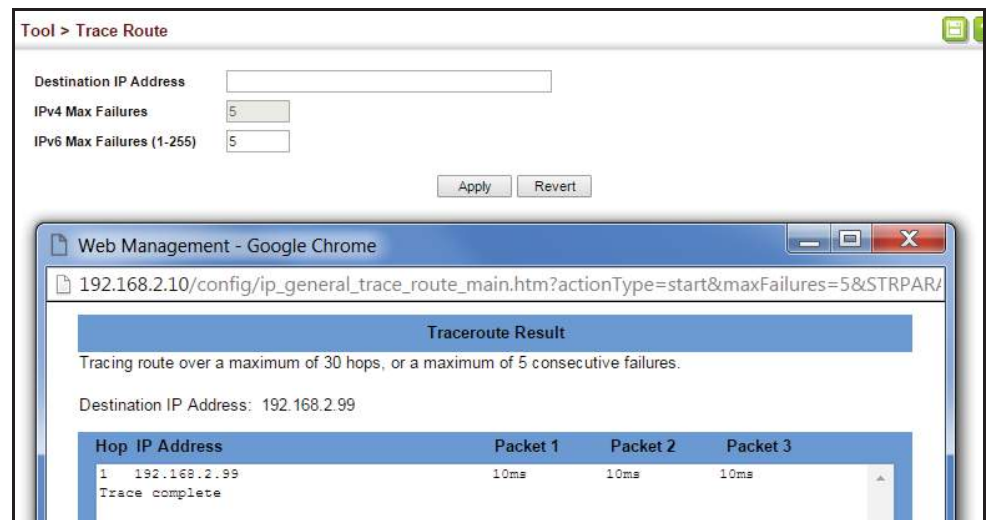
- ◆ Use the trace route function to determine the path taken to reach a specified destination.
- ◆ A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- ◆ The trace route function first sends probe datagrams with the 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 from which the trace route is sent.

Web Interface

To trace the route to another device on the network:

1. Click Tools, Trace Route.
2. Specify the target device.
3. Click Apply.

Figure 286: Tracing the Route to a Network Device



Address Resolution Protocol

If IP routing is enabled (page 673), 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 30: 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.

Displaying Dynamic or Local ARP Entries

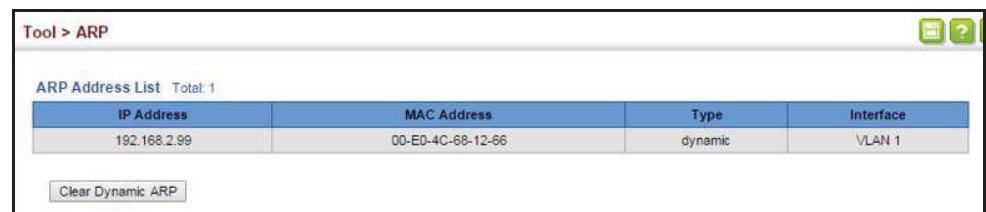
Use the Tools > ARP page to display dynamic or local entries in the ARP cache. The ARP cache contains static entries, and entries for local interfaces, including subnet, host, and broadcast addresses. However, most entries will be dynamically learned through replies to broadcast messages.

Web Interface

To display all dynamic and local entries in the ARP cache:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click ARP Addresses.

Figure 287: Displaying ARP Entries



The screenshot shows a web interface titled 'Tool > ARP'. Below the title is a sub-header 'ARP Address List Total: 1'. A table with four columns is displayed: 'IP Address', 'MAC Address', 'Type', and 'Interface'. The table contains one entry with IP Address '192.168.2.99', MAC Address '00-E0-4C-68-12-66', Type 'dynamic', and Interface 'VLAN 1'. Below the table is a button labeled 'Clear Dynamic ARP'.

IP Address	MAC Address	Type	Interface
192.168.2.99	00-E0-4C-68-12-66	dynamic	VLAN 1

IP Services

This chapter describes the following IP services:

- ◆ [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 for attached host devices, including DHCP option 82 information, and defines the servers to which client requests are forwarded.
- ◆ [DHCP Dynamic Provision](#) – Enables dynamic provision via DHCP.



Note: For information on DHCP snooping which is included in this folder, see [“DHCP Snooping” on page 337](#).

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.

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 472](#)).
- ◆ If one or more name servers are configured, but DNS is not yet enabled and the switch receives a DHCP packet containing a DNS field with a list of DNS servers,

then the switch will automatically enable DNS host name-to-address translation.

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 288: 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.

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 469](#)). 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 472](#)).
- ◆ If all name servers are deleted, DNS will automatically be disabled.

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 289: Configuring a List of Domain Names for DNS



The screenshot shows a web interface for configuring DNS. The breadcrumb trail at the top is "IP Service > DNS > General". Below this, there is a section titled "Action:" with a dropdown menu currently set to "Add Domain Name". Underneath, there is a "Domain Name" label followed by a text input field containing the text "sample.com.uk". At the bottom right of the form, there are two buttons: "Apply" and "Revert".

To show the list domain names:

1. Click IP Service, DNS.
2. Select Show Domain Names from the Action list.

Figure 290: Showing the List of Domain Names for DNS



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.

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 469](#)).
- ◆ 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 291: Configuring a List of Name Servers for DNS

IP Service > DNS > General

Action: Add Name Server ▼

Name Server IP Address: 192.168.1.10

Apply Revert

To show the list name servers:

1. Click IP Service, DNS.
2. Select Show Name Servers from the Action list.

Figure 292: Showing the List of Name Servers for DNS

IP Service > DNS > General

Action: Show Name Servers ▼

Name Server IP Address List Total: 3

	Name Server IP Address
☐	192.168.1.10
☐	140.113.5.7
☐	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.

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 293: Configuring Static Entries in the DNS Table

The screenshot shows the 'IP Service > DNS > Static Host Table' web interface. The 'Action' dropdown is set to 'Add'. Below this, there are two input fields: 'Host Name' with the value 'yahoo.com' and 'IP Address' with the value '10.2.78.3'. At the bottom right, there are 'Apply' and 'Revert' buttons.

To show static entries in the DNS table:

1. Click IP Service, DNS, Static Host Table.
2. Select Show from the Action list.

Figure 294: Showing Static Entries in the DNS Table

The screenshot shows the 'IP Service > DNS > Static Host Table' web interface with the 'Action' dropdown set to 'Show'. Below the dropdown, it says 'IP Address List Total: 3'. A table displays the static entries:

	Host	IP Address
☐	yahoo.com	10.2.78.3
☐	hinet.net	124.29.31.155
☐	google.com	133.45.211.18

At the bottom right, there are 'Delete' and 'Revert' buttons.

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.

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:

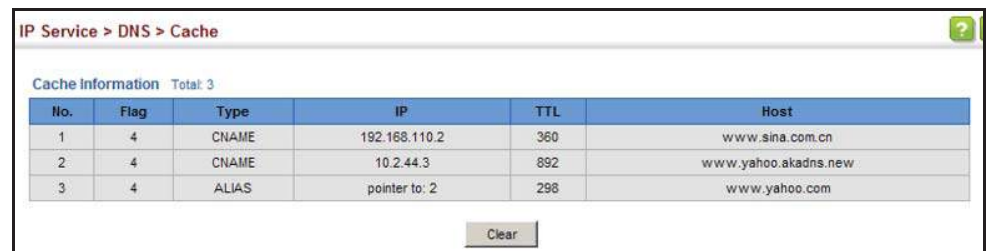
- ◆ **No.** – The entry number for each resource record.
- ◆ **Flag** – The flag is always “4” indicating a cache entry and therefore unreliable.
- ◆ **Type** – This field includes CNAME which specifies the host address for the owner, and ALIAS which specifies an alias.
- ◆ **IP** – The IP address associated 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 295: 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.new
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, or configure the DHCP server on this switch to support that subnet.

When configuring the DHCP server on this switch, you can configure an address pool for each unique IP interface, or manually assign a static IP address to clients based on their hardware address or client identifier. The DHCP server can provide the host's IP address, domain name, gateway router and DNS server, information about the host's boot image including the TFTP server to access for download and the name of the boot file, or boot information for NetBIOS Windows Internet Naming Service (WINS).

Specifying a DHCP Client Identifier

Use the IP Service > DHCP > Client page to specify the DHCP client identifier for a VLAN interface.

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 31: 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 32: 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:

- ◆ **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 the model number.
 - **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 296: Specifying a DHCP Client Identifier

IP Service > DHCP > Client

VLAN: 1 ▼

Vendor Class ID: ☒ Default ▼ SP6528

Apply Revert

Configuring DHCP Relay Service

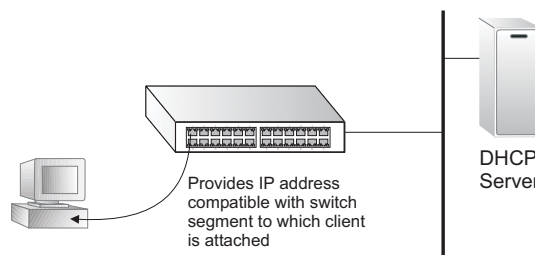
Use the IP Service > DHCP > Relay page to configure DHCP relay service for attached host devices, including DHCP option 82 information. DHCP provides an option for sending information about its DHCP clients to the DHCP server (specifically, the interface on the relay server through which the DHCP client request was received). Also known as DHCP Relay Option 82, it allows compatible DHCP servers to use this information when assigning IP addresses, or to set other services or policies for clients.

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 passes the DHCP response received from the server to the client.

Option 82 information contains information which can identify both the relay agent and the interface through which the DHCP request was received:

- ◆ The DHCP Relay Information Option Remote ID (RID) is the access node identifier – a string used to identify the switch to the DHCP server.
- ◆ The DHCP Relay Information Option Fields are the Option 82 circuit identification fields (CID – including VLAN ID, stack unit, and port). These fields identify the requesting device by indicating the interface through which the relay agent received the request.

Figure 297: Layer 3 DHCP Relay Service



Command Usage

- ◆ 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, specify the default router through which this switch can reach other IP subnetworks (see "[Configuring the IPv4 Default Gateway](#)" or "[Configuring the IPv6 Default Gateway](#)").
- ◆ DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.
- ◆ DHCP Snooping Information Option 82 (see [page 337](#)) and DHCP Relay Information Option 82 cannot both be enabled at the same time.
- ◆ DHCP request packets received by the switch are handled as follows:
 - If a DHCP relay server has been set on the switch, when the switch receives a DHCP request packet *without* option 82 information from the management VLAN or a non-management VLAN, it will add option 82 relay information and the relay agent's address to the DHCP request packet, and then unicast it to the DHCP server.
 - If a DHCP relay server has been set on the switch, when the switch receives a DHCP request packet *with* option 82 information from the management

VLAN or a non-management VLAN, it will process it according to the configured relay information option policy:

- If the policy is “replace,” the DHCP request packet’s option 82 content (the RID and CID sub-option) is replaced with information provided by the switch. The relay agent address is inserted into the DHCP request packet, and the switch then unicasts this packet to the DHCP server.
- If the policy is “keep,” the DHCP request packet’s option 82 content will be retained. The relay agent address is inserted into the DHCP request packet, and the switch then unicasts this packet to the DHCP server.
- If the policy is “drop,” the original DHCP request packet is flooded onto the VLAN which received the packet but is not relayed.

◆ DHCP reply packets received by the relay agent are handled as follows:

When the relay agent receives a DHCP reply packet with Option 82 information over the management VLAN, it first ensures that the packet is destined for it.

- If the RID in the DHCP reply packet is not identical with that configured on the switch, the option 82 information is retained, and the packet is flooded onto the VLAN through which it was received.
- If the RID in the DHCP reply packet matches that configured on the switch, it then removes the Option 82 information from the packet, and sends it on as follows:
 - If the DHCP packet’s broadcast flag is on, the switch uses the circuit-id information contained in the option 82 information fields to identify the VLAN connected to the requesting client and then broadcasts the DHCP reply packet to this VLAN.
 - If the DHCP packet’s broadcast flag is off, the switch uses the circuit-id information in option 82 fields to identify the interface connected to the requesting client and unicasts the reply packet to the client.

◆ DHCP packets are flooded onto the VLAN which received them if DHCP relay service is enabled on the switch and any of the following situations apply:

- There is no DHCP relay server set on the switch, when the switch receives a DHCP packet.
- A DHCP relay server has been set on the switch, when the switch receives a DHCP request packet with a non-zero relay agent address field (that is not the address of this switch).
- A DHCP relay server has been set on the switch, when the switch receives DHCP reply packet without option 82 information from the management VLAN.
- The reply packet contains a valid relay agent address field (that is not the address of this switch), or receives a reply packet with a zero relay agent address through the management VLAN.

- A DHCP relay server has been set on the switch, and the switch receives a reply packet on a non-management VLAN.

Parameters

These parameters are displayed:

- ◆ **Insertion of Relay Information** – Enable DHCP Option 82 information relay. (Default: Disabled)
- ◆ **DHCP Option Policy** – Specifies how to handle client requests which already contain DHCP Option 82 information:
 - **Drop** - Floods the original request packet onto the VLAN that received it instead of relaying it. (This is the default.)
 - **Keep** - Retains the Option 82 information in the client request, inserts the relay agent's address, and unicasts the packet to the DHCP server.
 - **Replace** - Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information provided by the relay agent itself, inserts the relay agent's address, and unicasts the packet to the DHCP server.
- ◆ **DHCP Sub-option Format** – Specifies whether or not to use the sub-type and sub-length fields in the circuit-ID (CID) and remote-ID (RID) in Option 82 information. (Default: Included)
- ◆ **Server IP Address** – Addresses of DHCP servers or relay 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. Enable or disable Option 82 relay information.
3. Set the Option 82 policy to specify how to handle Option 82 information already contained in DHCP client request packets.
4. Select whether or not to include the use of sub-type and sub-length fields for the circuit-ID (CID) and remote-ID (RID) in Option 82 information generated by the switch.
5. Enter up to five IP addresses for DHCP servers or relay servers in order of preference for any VLAN.
6. Click Apply.

Figure 298: Configuring DHCP Relay Service

IP Service > DHCP > Relay

Information

Insertion of Relay Information ☐ Enabled

DHCP Option Policy Drop ▼

DHCP Sub-option Format Extra Subtype Included ▼

Server

Server IP Address

Note: DHCP relay will not be active if an active DHCP server is detected on the same network segment.

Apply Revert

Enabling DHCP Dynamic Provision

Use the IP Service > DHCP > Dynamic Provision to enable dynamic provisioning via DHCP.

Command Usage

DHCPD is the daemon used by Linux to dynamically configure TCP/IP information for client systems. To support DHCP option 66/67, you have to add corresponding statements to the configuration file of DHCPD. Information on how to complete this process are described under [“Downloading a Configuration File and Other Parameters From a DHCP Server”](#).

Some alternative commands which can be added to the DHCPD to complete the dynamic provisioning process are also described under the [ip dhcp dynamic-provision](#) command.

By default, the parameters for DHCP option 66/67 are not carried by the reply sent from the DHCP server. To ask for a DHCP reply with option 66/67, the client can inform the server that it is interested in option 66/67 by sending a DHCP request that includes a 'parameter request list' option. Besides this, the client can also send a DHCP request that includes a 'vendor class identifier' option to the server so that the DHCP server can identify the device, and determine what information should be given to requesting device.

Parameters

These parameters are displayed:

- ◆ **Dynamic Provision via DHCP Status** – Enables dynamic provisioning via DHCP. (Default: Disabled)

Web Interface

To enable dynamic provisioning via DHCP:

1. Click IP Service, DHCP, Dynamic Provision.
2. Mark the Enable box if dynamic provisioning is configured on the DHCP daemon, and required for bootup.
3. Click Apply.

Figure 299: Enabling Dynamic Provisioning via DHCP

IP Service > DHCP > Dynamic Provision

Dynamic Provision via DHCP Status ☐ Enabled

Apply Revert

This chapter describes how to configure an 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 address can either be manually configured or 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)

This section describes how to configure an IPv4 interface for management access over the network. 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 IPv6 address, see [“Setting the Switch's IP Address \(IP Version 6\)” on page 487](#).

Configuring the IPv4 Default Gateway Use the System > IP (Configure Global) page to configure an IPv4 default gateway for the switch.

Parameters

These parameters are displayed:

- ◆ **Gateway IP Address** – IP address of the gateway router between the switch and management stations that exist on other network segments.
(Default: None)

An IP default gateway must be defined if the management station is located in a different IP segment.

An IP default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

Web Interface

To configure an IPv4 default gateway for the switch:

1. Click System, IP.
2. Select Configure Global from the Action list.
3. Enter the IPv4 default gateway.
4. Click Apply.

Figure 300: Configuring the IPv4 Default Gateway

The screenshot shows a web interface for configuring the switch's IP. At the top, it says "System > IP". Below that, there's a "Step:" dropdown menu with "1. Configure Global" selected. The main section is titled "Gateway IP Address" and contains a text input field with the value "192.168.0.1". At the bottom right, there are two buttons: "Apply" and "Revert".

Configuring IPv4 Interface Settings

Use the System > IP (Configure Interface – Add Address) page to configure an IPv4 address for the switch. The default IPv4 address for VLAN 1 is set to 192.168.2.10 using the subnet mask 255.255.255.0. To change the switch's default settings to values that are compatible with your network, you may need to establish a default gateway between the switch and management stations that exist on another network segment.

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.

Parameters

These parameters are displayed:

- ◆ **VLAN** – ID of the VLAN to be used for management access. 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: 1-4094; Default: VLAN 1)
- ◆ **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (User Specified), 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: User Specified)

- ◆ **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 or 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.

- ◆ **IP Address** – IP Address of the VLAN. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 192.168.2.10)
- ◆ **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)
- ◆ **Restart DHCP** – Requests a new IP address from the DHCP server.

Web Interface

To set a static IPv4 address for the switch:

1. Click System, IP.
2. Select Configure Interface from the Step list.
3. Select Add Address from the Action list.
4. Select any configured VLAN, set IP Address Mode to "User Specified," 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.
5. Select Primary or Secondary Address Type.
6. Click Apply.

Figure 301: Configuring a Static IPv4 Address

The screenshot shows the 'System > IP' configuration page. At the top, there are two dropdown menus: 'Step: 1. Configure Interface' and 'Action: Add Address'. Below these, the configuration fields are as follows:

VLAN	1
IP Address Mode	User Specified
IP Address Type	Primary
IP Address	192.168.0.2
Subnet Mask	255.255.255.0

At the bottom, there is a 'Restart DHCP' button with a tooltip that says 'Click this button to resend DHCP client request.' and two buttons: 'Apply' and 'Revert'.

To obtain an dynamic IPv4 address through DHCP/BOOTP for the switch:

1. Click System, IP.
2. Select Configure Interface from the Step list.
3. Select Add Address from the Action list.
4. Select any configured VLAN, and set IP Address Mode to "BOOTP" or "DHCP"
5. Click Apply to save your changes.
6. Then click Restart DHCP to immediately request a new address.

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 302: Configuring a Dynamic IPv4 Address

The screenshot shows the 'System > IP' configuration page. At the top, there are two dropdown menus: 'Step: 2. Configure Interface' and 'Action: Add Address'. Below these, the configuration fields are as follows:

VLAN	1
IP Address Mode	DHCP
IP Address Type	Primary
IP Address	
Subnet Mask	

At the bottom, there is a 'Restart DHCP' button with a tooltip that says 'Click this button to resend DHCP client request.' and two buttons: 'Apply' and '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 IPv4 address configured for an interface:

1. Click System, IP.
2. Select Configure Interface from the Step list.
3. Select Show Address from the Action list.
4. Select an entry from the VLAN list.

Figure 303: Showing the Configured IPv4 Address for an Interface

System > IP	
Step:	2. Configure Interface ▼
Action:	Show Address ▼
VLAN	1 ▼
IP Address Mode	DHCP
IP Address	192.168.2.12

Setting the Switch's IP Address (IP Version 6)

This section describes how to configure an IPv6 interface for management access over the network. 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 483](#).

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. Both link-local and global unicast address types can either be dynamically assigned (using the Configure Interface page) or manually configured (using the Add IPv6 Address page).

- ◆ 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 System > IPv6 Configuration (Configure Global) page to configure an IPv6 default gateway for the switch.

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.
 - 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 System, IPv6 Configuration.
2. Select Configure Global from the Action list.
3. Enter the IPv6 default gateway.
4. Click Apply.

Figure 304: Configuring the IPv6 Default Gateway

The screenshot shows a web interface titled "System > IPv6 Configuration". Below the title, there is a section labeled "Action:" with a dropdown menu currently set to "Configure Global". Underneath, there is a label "Default Gateway" followed by a text input field containing the IPv6 address "2001:1:1:1:1". At the bottom right of the form, there are two buttons: "Apply" and "Revert".

Configuring IPv6 Interface Settings

Use the System > IPv6 Configuration (Configure Interface) page to configure general IPv6 settings for the selected VLAN, including auto-configuration of a global unicast interface address, 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.

Command Usage

- ◆ The switch must be configured with a link-local address. The switch's address auto-configuration function will automatically create a link-local address, as well as an IPv6 global address if router advertisements are detected on the local interface.
- ◆ The option to explicitly enable IPv6 creates a link-local address, but will not generate a global IPv6 address if auto-configuration is not enabled. In this case, you can manually configure a global unicast address (see ["Configuring an IPv6 Address" on page 493](#)).
- ◆ 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** – ID of a configured VLAN that is to be used for management access. 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: 1-4094)
- ◆ **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 a link local address has not yet been assigned to this interface, this command will dynamically generate one. The link-local address is made with an address prefix in the range of FE80~FEBF and a host portion based the switch's MAC address in modified EUI-64 format. It will also generate a global unicast address if a global prefix is included in received router advertisements.
 - When DHCPv6 is started, the switch may attempt to acquire an IP address prefix through stateful address autoconfiguration. If 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 184](#)). 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. During the neighbor discover process, an IPv6 node will multicast neighbor solicitation messages to search for neighbor nodes. For a neighbor node to be considered reachable, it must respond to the neighbor soliciting node with a neighbor advertisement message to become a confirmed neighbor, after which the reachable timer will be considered in effect for subsequent unicast IPv6 layer communications.
- 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.

Web Interface

To configure general IPv6 settings for the switch:

1. Click System, IPv6 Configuration.
2. Select Configure Interface from the Action list.
3. Specify the VLAN to configure.
4. Enable address auto-configuration, or 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.
5. Click Apply.

Figure 305: Configuring General Settings for an IPv6 Interface

The screenshot shows the 'System > IPv6 Configuration' page. At the top, there is a breadcrumb trail 'System > IPv6 Configuration'. Below it is an 'Action:' dropdown menu set to 'Configure Interface'. The main configuration area includes several settings: 'VLAN' is set to '1'; 'Address Autoconfig' and 'Enable IPv6 Explicitly' are both checked and labeled 'Enabled'; 'MTU (1280-65535)' is set to '1500' bytes; 'ND DAD Attempts (0-600)' is set to '3'; 'ND NS Interval (1000-3600000)' is set to '1000' ms; and 'ND Reachable-Time (0-3600000)' is set to '30000' ms. At the bottom left, there is a 'Restart DHCPv6' button with a link 'Click this button to restart DHCPv6 service.' At the bottom right, there are 'Apply' and 'Revert' buttons.

Configuring an IPv6 Address Use the System > IPv6 Configuration (Add IPv6 Address) page to configure an IPv6 interface for management access over the network.

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 any configuration process that enables IPv6 functionality, or assigns a global unicast address to the switch, including address auto-configuration or explicitly enabling IPv6 (see [“Configuring IPv6 Interface Settings” on page 489](#)), 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:
 - The global unicast address can be automatically configured by taking the network prefix from router advertisements observed on the local interface, and using the modified EUI-64 form of the interface identifier to automatically create the host portion of the address (see [“Configuring IPv6 Interface Settings” on page 489](#)).
 - 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. 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: 1-4094)
- ◆ **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 00-12-24-56-78-9A, 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 00-12-24-FF-FE-56-78-9A.

- 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 System, 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 306: Configuring an IPv6 Address

The screenshot shows a web interface titled "System > IPv6 Configuration". Below the title bar, there is a form with the following fields and values:

- Action:** A dropdown menu with "Add IPv6 Address" selected.
- VLAN:** A dropdown menu with "1" selected.
- Address Type:** A dropdown menu with "Global" selected.
- IPv6 Address:** A text input field containing "2001:1::/64".

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

Showing IPv6 Addresses Use the System > IPv6 Configuration (Show IPv6 Address) page to display the IPv6 addresses assigned to an interface.

Parameters

These parameters are displayed:

- ◆ **VLAN** – ID of a configured VLAN. 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: 1-4094)
- ◆ **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 “[show ip interface](#)” command.

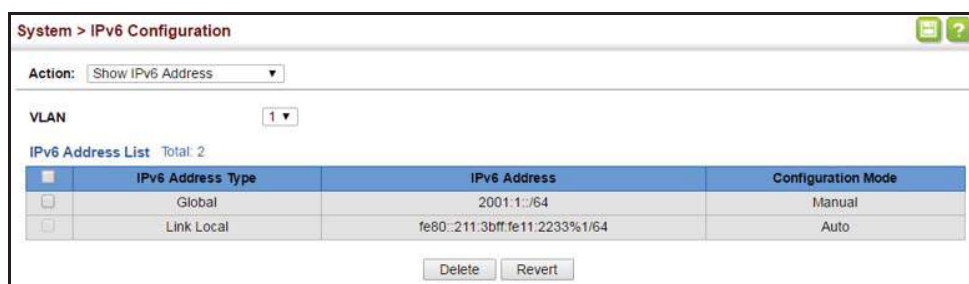
- ◆ **Configuration Mode** – Indicates if this address was automatically generated or manually configured.

Web Interface

To show the configured IPv6 addresses:

1. Click System, IPv6 Configuration.
2. Select Show IPv6 Address from the Action list.
3. Select a VLAN from the list.

Figure 307: Showing Configured IPv6 Addresses



Showing the IPv6 Neighbor Cache

Use the System > IPv6 Configuration (Show IPv6 Neighbor Cache) page to display the IPv6 addresses detected for neighbor devices.

Parameters

These parameters are displayed:

Table 33: 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 Address	Physical layer MAC address.
State	The following states are used for dynamic entries: ◆ 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.

Table 33: Show IPv6 Neighbors - display description (Continued)

Field	Description
	The following states are used for static entries: ◆ 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 System, IPv6 Configuration.
2. Select Show IPv6 Neighbors from the Action list.

Figure 308: Showing IPv6 Neighbors

System > IPv6 Configuration				
Action: Show IPv6 Neighbor Cache				
Current Neighbor Cache Table Total: 1				
IPv6 Address	Age	Link-layer Address	State	VLAN
fe80::ce37:abff:fe5b:77bc	26	CC-37-AB-5B-77-BC	Stale	1
Clear				

Showing IPv6 Statistics Use the System > IPv6 Configuration (Show Statistics) page to display statistics about IPv6 traffic passing through this switch.

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 34: 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.
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.

Table 34: Show IPv6 Statistics - display description (Continued)

Field	Description
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.
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.

Table 34: Show IPv6 Statistics - display description (Continued)

Field	Description
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.
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.

Table 34: Show IPv6 Statistics - display description (Continued)

Field	Description
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 System, IPv6 Configuration.
2. Select Show Statistics from the Action list.
3. Click IPv6, ICMPv6 or UDP.

Figure 309: Showing IPv6 Statistics (IPv6)

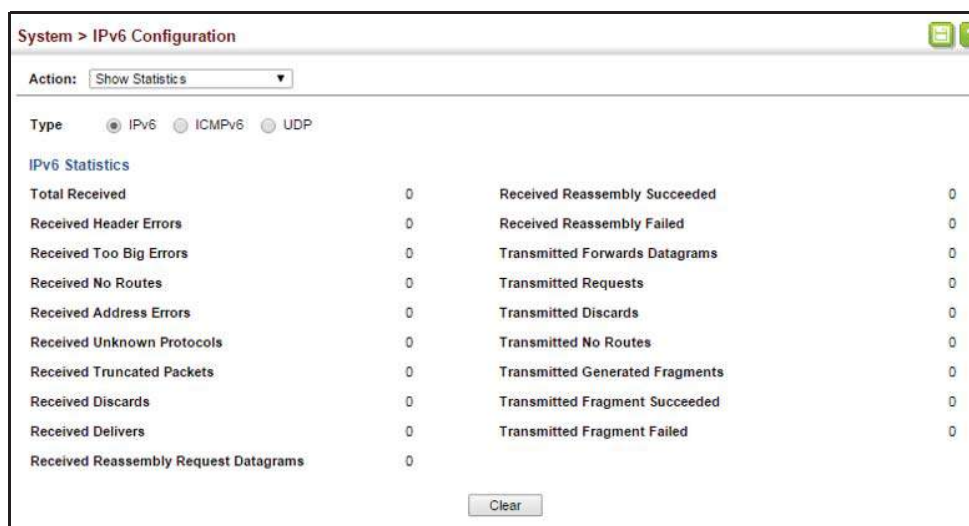


Figure 310: Showing IPv6 Statistics (ICMPv6)

System > 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		

Clear

Figure 311: Showing IPv6 Statistics (UDP)

System > IPv6 Configuration

Action: Show Statistics ▼

Type ☐ IPv6 ☐ ICMPv6 ☒ UDP

UDP Statistics

Input	0
No Port Errors	0
Other Errors	0
Output	0

Clear

Showing the MTU for Responding Destinations

Use the System > 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.

Parameters

These parameters are displayed:

Table 35: 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 System, IPv6 Configuration.
2. Select Show MTU from the Action list.

Figure 312: Showing Reported MTU Values



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 507](#)
- ◆ [“General Commands” on page 518](#)
- ◆ [“System Management Commands” on page 526](#)
- ◆ [“SNMP Commands” on page 591](#)
- ◆ [“Remote Monitoring Commands” on page 616](#)
- ◆ [“Authentication Commands” on page 623](#)
- ◆ [“General Security Measures” on page 684](#)
- ◆ [“Access Control Lists” on page 733](#)
- ◆ [“Interface Commands” on page 757](#)
- ◆ [“Link Aggregation Commands” on page 786](#)
- ◆ [“Port Mirroring Commands” on page 800](#)
- ◆ [“Congestion Control Commands” on page 810](#)
- ◆ [“Loopback Detection Commands” on page 814](#)
- ◆ [“Address Table Commands” on page 820](#)
- ◆ [“Spanning Tree Commands” on page 826](#)
- ◆ [“VLAN Commands” on page 856](#)

- ◆ “Class of Service Commands” on page 881
- ◆ “Quality of Service Commands” on page 893
- ◆ “Multicast Filtering Commands” on page 906
- ◆ “LLDP Commands” on page 962
- ◆ “Domain Name Service Commands” on page 985
- ◆ “DHCP Commands” on page 994
- ◆ “IP Interface Commands” on page 1003

Using the Command Line Interface

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



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

Accessing the CLI

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

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

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

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

```
User Access Verification

Username: admin
Password:
  CLI session with the SP6528 is opened.
  To end the CLI session, enter [Exit].

Console#
```

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



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

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

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

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

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

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

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

CLI session with the SP6528 is opened.
To end the CLI session, enter [Exit].

Vty-0#
```




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

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

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

You can enter commands as follows:

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

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

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

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

Minimum Abbreviation

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

Command Completion

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

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the "?" character to list keywords or parameters.

Showing Commands

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

```

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

```

snmp	Simple Network Management Protocol configuration and statistics
snmp-server	Displays SNMP server configuration
sntp	Simple Network Time Protocol configuration
spanning-tree	Spanning-tree configuration
ssh	Secure shell server connections
startup-config	Startup system configuration
subnet-vlan	IP subnet-based VLAN information
system	System information
tacacs-server	TACACS server information
tech-support	Technical information
time-range	Time range
traffic-segmentation	Traffic segmentation information
users	Information about users logged in
version	System hardware and software versions
vlan	Shows virtual LAN settings
voice	Shows the voice VLAN information
watchdog	Displays watchdog status

Console#show

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

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

Console#

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

Partial Keyword Lookup

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

Console#show s?				
snmp	snmp-server	sntp	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 36: General Command Modes

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

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

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

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

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

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

CLI session with the SP6528 is opened.
To end the CLI session, enter [Exit].

Console#
```

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

CLI session with the SP6528 is opened.
To end the CLI session, enter [Exit].

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

Configuration Commands

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

The configuration commands are organized into different modes:

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

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

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

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

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

Table 37: Configuration Command Modes

Mode	Command	Prompt	Page
Access Control List	access-list arp	Console(config-arp-acl)	752
	access-list ip standard	Console(config-std-acl)	734
	access-list ip extended	Console(config-ext-acl)	734
	access-list ipv6 standard	Console(config-std-ipv6-acl)	740
	access-list ipv6 extended	Console(config-ext-ipv6-acl)	740
	access-list mac	Console(config-mac-acl)	747
Class Map	class-map	Console(config-cmap)	894
Interface	interface {ethernet <i>port</i> port-channel <i>id</i> vlan <i>id</i> }	Console(config-if)	758
Line	line {console vty}	Console(config-line)	553
MSTP	spanning-tree mst-configuration	Console(config-mstp)	832
Policy Map	policy-map	Console(config-pmap)	897
Time Range	time-range	Console(config-time-range)	587
VLAN	vlan database	Console(config-vlan)	860

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 38: 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 39: Command Group Index

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	518
System Management	Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, and the system clock	526
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	591
Remote Monitoring	Supports statistics, history, alarm and event groups	616
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	623
General Security Measures	Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses	684
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)	733
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	757
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	786
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	800
Congestion Control	Sets the input/output rate limits, traffic storm thresholds, and thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.	810
Loopback Detection	Detects general loopback conditions caused by hardware problems or faulty protocol settings	814

Table 39: Command Group Index (Continued)

Command Group	Description	Page
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	820
Spanning Tree	Configures Spanning Tree settings for the switch	826
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling	856
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	881
Quality of Service	Configures Differentiated Services	893
Multicast Filtering	Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration, and IPv6 MLD snooping	906
Link Layer Discovery Protocol	Configures LLDP settings to enable information discovery about neighbor devices	962
Dynamic Host Configuration Protocol	Configures DHCP client, relay and server functions	994
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters	1003
Debug	Displays debugging information for all key functions	
	These commands are not described in this manual. Please refer to the prompt messages included in the CLI interface.	

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

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

General Commands

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

Table 40: General Commands

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

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

Syntax

prompt *string*

no prompt

string - Any alphanumeric string to use for the CLI prompt.
(Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Command Usage

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

Example

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

reload
 (Global Configuration)

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

Syntax

reload **at** *hour minute* [{*month day* | *day month*} [*year*]] |
in {**hour** *hours* | **minute** *minutes* | **hour** *hours* **minute** *minutes*} |
regularity *hour minute* [**period** {**daily** | **weekly** *day-of-week* |
monthly *day-of-month*}] | **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: 1970-2037)

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

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

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

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

reload cancel - Cancels the specified reload option.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ This command resets the entire system.
- ◆ Any combination of reload options may be specified. If the same option is re-specified, the previous setting will be overwritten.
- ◆ When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the [copy running-config startup-config](#) command (See [“copy” on page 542](#)).

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 2015 ---
***

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 512](#).

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 \(523\)](#)

[enable password \(624\)](#)

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 512](#).

Default Setting

None

Command Mode

Privileged Exec

Example

```

Console#configure
Console(config)#

```

Related Commands

[end \(524\)](#)

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 512](#).

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 \(520\)](#)

reload (Privileged Exec) This command restarts the system.



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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

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

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

Command Mode

Privileged Exec

Example

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

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

end This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

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

Example

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

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

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

Default Setting

None

Command Mode

Any

Example

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

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

Press ENTER to start session

User Access Verification

Username:
```

System Management Commands

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

Table 41: System Management Commands

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

Device Designation

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

Table 42: Device Designation Commands

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

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

Syntax

hostname *name*

no hostname

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

System Status

This section describes commands used to display system information.

Table 43: System Status Commands

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

Table 43: System Status Commands (Continued)

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

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

Command Mode

Privileged Exec

Command Usage

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

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

Example

```
Console#show access-list tcam-utilization
Pool capability code:
AM - MAC ACL, A4 - IPv4 ACL, A6S - IPv6 Standard ACL,
A6E - IPv6 extended ACL, DM - MAC diffServ, D4 - IPv4 diffServ,
D6S - IPv6 standard diffServ, D6E - IPv6 extended diffServ,
I - IP source guard, C - CPU interface, L - Link local,
Reserved - Reserved, ALL - All supported function,
```

Unit	Device	Pool	Total	Used	Free	Capability
1	0	0	64	0	64	A6S
1	0	1	64	0	64	A6E
1	0	2	128	0	128	A4
1	0	3	128	0	128	AM
1	0	4	128	128	0	MV PV VV
1	0	5	64	0	64	D6S D6E
1	0	6	128	0	128	D4
1	0	7	128	0	128	DM
1	0	8	64	64	0	I
1	0	9	64	64	0	C
1	0	10	64	64	0	Reserved
1	0	11	64	64	0	C L

Console#

Table 44: show access-list tcam-utilization - display description

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

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

Command Mode

Normal Exec, Privileged Exec

Command Usage

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

Example

```

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

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

Console#

```

Related Commands

[memory \(612\)](#)

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

Command Mode

Normal Exec, Privileged Exec

Example

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

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

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

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

Console#
```

Related Commands

[process cpu \(613\)](#)

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

Command Mode

Normal Exec, Privileged Exec

Example

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

Console#
```

Table 45: show process cpu guard - display description

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

Related Commands

[process cpu guard \(614\)](#)

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

Command Mode

Privileged Exec

Example

```

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

```

FS	0.00	0.00	0.00
HTTP_TD	0.00	0.00	5.00
HW_WTDOG_TD	0.00	0.00	0.00
IML_TX	0.00	0.00	0.00
IP_SERVICE_GROU	0.00	0.00	0.00
KEYGEN_TD	0.00	0.00	0.00
L2_L4_PROCESS	0.00	0.00	4.00
L2MCAST_GROUP	0.00	0.00	0.00
L2MUX_GROUP	0.00	0.00	0.00
L4_GROUP	0.00	0.00	0.00
LACP_GROUP	0.00	0.00	0.00
MSL_TD	0.00	0.00	0.00
NETACCESS_GROUP	0.00	0.00	0.00
NETACCESS_NMTR	0.00	0.25	2.00
NETCFG_GROUP	0.00	0.00	0.00
NETCFG_PROC	0.00	0.08	1.00
NIC	0.00	0.00	0.00
NMTRDRV	1.00	1.66	4.00
NSM_GROUP	0.00	0.00	0.00
NSM_PROC	0.00	0.00	0.00
NSM_TD	0.00	0.00	0.00
OSPF6_TD	0.00	0.00	0.00
OSPF_TD	0.00	0.00	0.00
PIM_GROUP	0.00	0.00	0.00
PIM_PROC	0.00	0.00	0.00
PIM_SM_TD	0.00	0.00	0.00
POE_PROC	0.00	0.00	0.00
RIP_TD	0.00	0.00	0.00
SNMP_GROUP	0.00	0.00	0.00
SNMP_TD	0.00	0.00	0.00
SSH_GROUP	0.00	0.00	0.00
SSH_TD	0.00	0.00	0.00
STA_GROUP	0.00	0.00	0.00
STKCTRL_GROUP	0.00	0.00	0.00
STKTPLG_GROUP	0.00	0.00	0.00
SWCTRL_GROUP	0.00	0.00	0.00
SWCTRL_TD	0.00	0.00	0.00
SWDRV_MONITOR	21.00	19.25	21.00
SYS_MGMT_PROC	0.00	0.00	0.00
SYSDRV	0.00	0.00	0.00
SYSLOG_TD	0.00	0.00	0.00
SYSMGMT_GROUP	0.00	0.00	0.00
SYSTEM	0.00	0.00	0.00
UDLD_GROUP	0.00	0.00	0.00
WTDG_PROC	0.00	0.00	0.00
XFER_GROUP	0.00	0.00	0.00
XFER_TD	0.00	0.00	0.00

Console#

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

Syntax

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

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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

Command Mode

Privileged Exec

Command Usage

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

Example

```
Console#show running-config
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-e0-0c-00-00-fd_03</stackingMac>
!
snmp-server community public ro
snmp-server community private rw
!
```

```
enable password 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
  VLAN 1 name DefaultVlan media ethernet
!
spanning-tree mst configuration
!
interface ethernet 1/1
  no negotiation
...
interface ethernet 1/28
  no negotiation
!
interface vlan 1
  ip address dhcp
!
interface vlan 1
!
line console
!
line vty
!
end
!
Console#
```

Related Commands

[show startup-config \(534\)](#)

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

Command Mode

Privileged Exec

Command Usage

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

Example

Refer to the example for the running configuration file.

Related Commands

[show running-config \(533\)](#)

show system This command displays system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show system
System Description : SP6528
System OID String : 1.3.6.1.4.1.16813.26.104
System Information
  System Up Time      : 0 days, 2 hours, 25 minutes, and 27.66 seconds
  System Name         :
  System Location     :
  System Contact      :
  MAC Address (Unit 1) : 00-E0-0C-00-00-FD
  Web Server          : Enabled
  Web Server Port     : 80
  Web Secure Server   : Enabled
  Web Secure Server Port : 443
  Telnet Server       : Enabled
  Telnet Server Port  : 23
  Jumbo Frame         : Disabled
Console#
```

Table 46: show system – display description

Parameter	Description
System Description	Brief description of device type.
System OID String	MIB II object ID for switch's network management subsystem.
System Up Time	Length of time the management agent has been up.
System Name	Name assigned to the switch system.
System Location	Specifies the system location.
System Contact	Administrator responsible for the system.
MAC Address	MAC address assigned to this switch.
Web Server/Port	Shows administrative status of web server and UDP port number.
Web Secure Server/Port	Shows administrative status of secure web server and UDP port number.

Table 46: show system – display description (Continued)

Parameter	Description
Telnet Server/Port	Shows administrative status of Telnet server and TCP port number.
Jumbo Frame	Shows if jumbo frames are enabled or disabled.

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

Command Mode

Normal Exec, Privileged Exec

Command Usage

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

Example

```

User Access Verification

Username: admin
Password:

      CLI session with the SFP6528 is opened.
      To end the CLI session, enter [Exit].

Vty-2#show tech-support

dir:
File Name                               Type      Startup Modified Time          Size (bytes)
-----
Unit 1:
SP6528_V1.1.2.0.bix                     OpCode   Y        2016-11-24 04:26:03      8057096
Factory_Default_Config.cfg              Config   N        2015-07-01 07:24:11        455
startup1.cfg                            Config   Y        2015-07-01 07:24:22      1343
-----
Free space for compressed user config files:  24018944

show arp:
ARP Cache Timeout: 1200 (seconds)

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

Total entry : 1

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

```

```
Eth 1/ 5          Down      1    0    Auto-100full    1000BASE-T    None
...
```

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

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

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

Example

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

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

Web Online Users:
Line      User Name          Idle Time (h:m:s) Remote IP Addr
-----
HTTP      admin              0:00:02 192.168.2.99

Console#
```

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

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show version
Unit 1
Serial Number      : S123456
Hardware Version   : R01
Number of Ports    : 28
Main Power Status  : Up
Role               : Master
Loader Version     : 0.1.1.7
Linux Kernel Version : 2.6.19
```

```
Operation Code Version : 1.1.2.0
```

```
Console#
```

Table 47: show version – display description

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

show watchdog This command shows if watchdog debugging is enabled.

Command Mode

Privileged Exec

Example

```
Console#show watchdog

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

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

Syntax

watchdog software {disable | enable}

Default Setting

Disabled

Command Mode

Privileged Exec

Example

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

Frame Size

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

Table 48: Frame Size Commands

Command	Function	Mode
<code>jumbo frame</code>	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 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 \(535\)](#)
[show ipv6 mtu \(1026\)](#)

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 49: 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

Table 49: Flash/File Commands (Continued)

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

General Commands

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

Syntax

boot system {**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 \(546\)](#)

[whichboot \(547\)](#)

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

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

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

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

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

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

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

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

public-key - Keyword that allows you to copy a SSH key from a TFTP server. (See "Secure Shell" on page 657.)

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 127 characters for files on the server. (Valid characters: A-Z, a-z, 0-9, "", "-", "_")
- ◆ The switch supports only two operation code files, but the maximum number of user-defined configuration files is 16.
- ◆ You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- ◆ To replace the startup configuration, you must use **startup-config** as the destination.
- ◆ The Boot ROM and Loader cannot be uploaded or downloaded from the 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."](#) For information on configuring the switch to use HTTPS for a secure connection, see the [ip http secure-server](#) command.
- ◆ The reload command will not be accepted during copy operations to flash memory.
- ◆ When logging into an FTP server, the interface prompts for a user name and password configured on the remote server. Note that "anonymous" is set as the default user name.

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 {**file name** *filename* | **public-key** *username* [**dsa** | **rsa**]}

file - Keyword that allows you to delete a file.

name - Keyword indicating a file.

filename - Name of configuration file or code image.

public-key - Keyword that allows you to delete a SSH key on the switch.
(See [“Secure Shell” on page 657.](#))

username - Name of an SSH user. (Range: 1-8 characters)

dsa - DSA public key type.

rsa - RSA public key type.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ If the file type is used for system startup, then this file cannot be deleted.
- ◆ “Factory_Default_Config.cfg” cannot be deleted.

- ◆ If the public key type is not specified, then both DSA and RSA keys will be deleted.

Example

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

```
Console#delete test2.cfg
Console#
```

Related Commands

[dir \(546\)](#)

[delete public-key \(662\)](#)

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

Syntax

dir {**config** | **opcode**}: [*filename*]

config - Switch configuration file.

opcode - Run-time operation code image file.

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

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

File information is shown below:

Table 50: File Directory Information

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

Example

The following example shows how to display all file information:

```

Console#dir
File Name                               Type      Startup Modified Time          Size (bytes)
-----
Unit 1:
SFP6528_V1.1.2.0.bix                   OpCode    Y         2015-07-01 07:26:54        7733512
Factory_Default_Config.cfg             Config    N         2015-07-01 07:24:11          455
startup1.cfg                           Config    Y         2015-07-01 07:24:22         1343
-----
Free space for compressed user config files: 24018944
Console#

```

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

Syntax

whichboot

Default Setting

None

Command Mode

Privileged Exec

Example

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

```

Console#whichboot
File Name                               Type      Startup Modified Time          Size (bytes)
-----
Unit 1:
SP6528_V1.1.2.0.bix                   OpCode    Y         2016-11-24 04:26:03        8057096
startup1.cfg                           Config    Y         2017-01-18 07:20:55         1401
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 SFP6528.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 SFP6528.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   : SP6528.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 51: 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 commands	Applies an authorization method to commands entered at specific CLI privilege levels	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

Table 51: Line Commands (Continued)

Command	Function	Mode
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 \(562\)](#)

[show users \(537\)](#)

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

Syntax

databits {7 | 8}

no databits

7 - Seven data bits per character.

8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

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

Example

To specify 7 data bits, enter this command:

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

Related Commands

[parity \(556\)](#)

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

Syntax

exec-timeout [*seconds*]

no exec-timeout

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

Default Setting

10 minutes

Command Mode

Line Configuration

Command Usage

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

Example

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

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

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

Syntax

login [local]

no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- ◆ There are three authentication modes provided by the switch itself at login:
 - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
 - **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
 - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

- ◆ This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

Example

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

Related Commands

[username \(625\)](#)

[password \(557\)](#)

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

Syntax

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

no parity

none - No parity

even - Even parity

odd - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

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

Example

To specify no parity, enter this command:

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


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

Syntax

password {0 | 7} *password*

no password

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

password - Character string that specifies the line password.

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

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

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

Example

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

Related Commands

[login \(555\)](#)

[password-thresh \(557\)](#)

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

Syntax

password-thresh [*threshold*]

no password-thresh

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

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

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

Example

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

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

Related Commands

[silent-time](#) (558)

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

Syntax

silent-time [*seconds*]

no silent-time

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

Default Setting

Disabled

Command Mode

Line Configuration

Example

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

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

Related Commands

[password-thresh \(557\)](#)

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

Syntax

speed *bps*

no speed

bps - Baud rate in bits per second.

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

Default Setting

115200 bps

Command Mode

Line Configuration

Command Usage

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

Example

To specify 57600 bps, enter this command:

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

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

Syntax

stopbits {1 | 2}

no stopbits

1 - One stop bit

2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

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

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

Syntax

timeout login response [*seconds*]

no timeout login response

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

Default Setting

300 seconds

Command Mode

Line Configuration

Command Usage

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

Example

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

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

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

Syntax

disconnect *session-id*

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

Command Mode

Privileged Exec

Command Usage

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

Example

```
Console#disconnect 1
Console#
```

Related Commands

[show ssh \(666\)](#)

[show users \(537\)](#)

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

Syntax

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

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

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

character - Any valid keyboard character.

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

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

terminal-type - The type of terminal emulation used.

ansi-bbs - ANSI-BBS

vt-100 - VT-100

vt-102 - VT-102

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

Default Setting

Escape Character: 27 (ASCII-number)
History: 10
Length: 24
Terminal Type: VT100
Width: 80

Command Mode

Privileged Exec

Example

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

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

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

Syntax

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

console - Console terminal line.

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

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
Terminal Configuration for this session:
Length                : 24
Width                 : 80
History Size          : 10
Escape Character(ASCII-number) : 27
Terminal Type         : VT100

Console Configuration:
Password Threshold    : 3 times
EXEC Timeout          : 600 seconds
Login Timeout         : 300 seconds
```

```
Silent Time      : Disabled
Baud Rate       : 115200
Data Bits      : 8
Parity         : None
Stop Bits      : 1

VTY Configuration:
Password Threshold : 3 times
EXEC Timeout      : 600 seconds
Login Timeout     : 300 sec.
Silent Time       : Disabled
Console#
```

Event Logging

This section describes commands used to configure event logging on the switch.

Table 52: Event Logging Commands

Command	Function	Mode
<code>logging command</code>	Stores CLI command execution records in syslog RAM and flash	GC
<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 command This command stores CLI command execution records in syslog RAM and flash. Use the **no** form to disable this feature.

Syntax

[no] logging command

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The records stored include the commands executed from the CLI, command execution time and information about the CLI user including user name, user interface (console, Telnet, SSH) and user IP address. The severity level for this record type is 6 (see the [logging facility](#) command).

Example

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

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

Syntax

logging facility *type*

no logging facility

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

Default Setting

23

Command Mode

Global Configuration

Command Usage

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

Example

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

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

Syntax

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

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

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

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

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

Table 53: Logging Levels

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

Default Setting

Flash: errors (level 3 - 0)

RAM: debugging (level 7 - 0)

Command Mode

Global Configuration

Command Usage

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

Example

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

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

Syntax

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

no logging host *host-ip-address*

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

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

Default Setting

UPD Port: 514

Command Mode

Global Configuration

Command Usage

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

Example

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

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

Syntax

[no] **logging on**

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

Related Commands

[logging history \(564\)](#)

[logging trap \(567\)](#)

[clear log \(567\)](#)

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 564](#).
Messages sent include the selected level through level 0.

Default Setting

Disabled

Level 7

Command Mode

Global Configuration

Command Usage

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

Example

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

clear log This command clears messages from the log buffer.

Syntax

clear log [*flash* | *ram*]

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

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

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

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

Related Commands

[show log \(568\)](#)

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

Syntax

show log {flash | ram}

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

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

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

Example

The following example shows the event message stored in RAM.

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

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

Syntax

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

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

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

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

sendmail - Displays settings for the SMTP event handler ([page 574](#)).

trap - Displays settings for the trap function.

Default Setting

None

Command Mode

Privileged Exec

Example

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

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

Table 54: show logging flash/ram - display description

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

The following example displays settings for the trap function.

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

Table 55: show logging trap - display description

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

Related Commands

[show logging sendmail \(574\)](#)

SMTP Alerts

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

Table 56: Event Logging Commands

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

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

Syntax

[no] logging sendmail

Default Setting

Enabled

Command Mode

Global Configuration

Example

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

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

Syntax

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

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

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

Syntax

[no] logging sendmail host *ip-address*

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

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

Syntax

logging sendmail level *level*

no logging sendmail level

level - One of the system message levels ([page 564](#)). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

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

Example

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

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

logging sendmail source-email

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

Syntax

logging sendmail source-email *email-address*

no logging sendmail source-email

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

show logging sendmail This command displays the settings for the SMTP event handler.

Command Mode

Privileged Exec

Example

```
Console#show logging sendmail
SMTP Servers
-----
192.168.1.19

SMTP Minimum Severity Level: 7

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

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

SMTP Status: Enabled
Console#
```

Time

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

Table 57: Time Commands

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

Table 57: Time Commands (Continued)

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

* Daylight savings time.

SNTP Commands

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

Syntax

[no] sntp client

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

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

Example

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

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

Related Commands

[sntp server \(576\)](#)

[sntp poll \(576\)](#)

[show sntp \(577\)](#)

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 \(575\)](#)

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

Syntax

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

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

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

Related Commands[sntp client \(575\)](#)[sntp poll \(576\)](#)[show sntp \(577\)](#)

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

Command Mode

Normal Exec, Privileged Exec

Command Usage

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

Example

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

NTP Commands

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

Syntax

[no] ntp authenticate

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

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

Example

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

Related Commands

[ntp authentication-key \(578\)](#)

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 \(578\)](#)

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

Syntax

[no] **ntp client**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

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

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

Example

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

Related Commands

[sntp client \(575\)](#)

[ntp server \(580\)](#)

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 \(579\)](#)[show ntp \(581\)](#)

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           : Jan 19 18:39:35 2017
Polling                : 1024 seconds
Current Mode           : unicast
NTP Status              : Enabled
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 118.163.81.61 version 3
Console#

```

Manual Configuration Commands

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

Syntax

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

no clock summer-time

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

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

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

b-year - The year summer time will begin.

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

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

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

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

e-year - The year summer time will end.

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

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

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

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

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

Example

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

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

Related Commands

[show sntp \(577\)](#)

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

Syntax

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

no clock summer-time

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

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

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

Table 58: Predefined Summer-Time Parameters

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

Example

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

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

Related Commands

[show sntp \(577\)](#)

**clock summer-time
(recurring)**

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

Syntax

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

no clock summer-time

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

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

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

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

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

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

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

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

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

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

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

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

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

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

Example

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

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

Related Commands

[show sntp \(577\)](#)

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

Syntax

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

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

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

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

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

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

Related Commands

[show sntp \(577\)](#)

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

Syntax

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

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

min - Minute. (Range: 0 - 59)

sec - Second. (Range: 0 - 59)

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

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

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

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

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2015.

```
Console#calendar set 15:12:34 1 February 2015
Console#
```

show calendar This command displays the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

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

Time Range

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

Table 59: Time Range Commands

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

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

Syntax

[no] time-range *name*

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

Related Commands

[Access Control Lists \(733\)](#)

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

Syntax

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

absolute end *hour minutes day month year*

no absolute

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

minute - Minute. (Range: 0-59)

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

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

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

Default Setting

None

Command Mode

Time Range Configuration

Command Usage

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

Example

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

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

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

Syntax

[no] **periodic** {**daily** | **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** | **weekdays** | **weekend**} *hour minute* to {**daily** | **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** | **weekdays** | **weekend**} [*hour minute*]

daily - Daily

friday - Friday

monday - Monday

saturday - Saturday

sunday - Sunday

thursday - Thursday

tuesday - Tuesday

wednesday - Wednesday

weekdays - Weekdays

weekend - Weekends

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

minute - Minute. (Range: 0-59)

Default Setting

None

Command Mode

Time Range Configuration

Command Usage

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

Example

This example configures a time range for the periodic occurrence of an event.

```
Console(config)#time-range sales
Console(config-time-range)#periodic daily 1 1 to 2 1
Console(config-time-range)#
```

show time-range This command shows configured time ranges.

Syntax

show time-range [*name*]

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

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show time-range r&d
Time-range r&d:
  status: inactive
  absolute start 01:01 01 April 2015
  periodic    Daily 01:01 to    Daily 02:01
  periodic    Daily 02:01 to    Daily 03:01
Console#
```

SNMP Commands

SNMP commands control access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 60: SNMP Commands

Command	Function	Mode
<i>General SNMP Commands</i>		
<code>snmp-server</code>	Enables the SNMP agent	GC
<code>snmp-server community</code>	Sets up the community access string to permit access to SNMP commands	GC
<code>snmp-server contact</code>	Sets the system contact string	GC
<code>snmp-server location</code>	Sets the system location string	GC
<code>show snmp</code>	Displays the status of SNMP communications	NE, PE
<i>SNMP Target Host Commands</i>		
<code>snmp-server enable traps</code>	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC
<code>snmp-server host</code>	Specifies the recipient of an SNMP notification operation	GC
<code>snmp-server enable port-traps link-up-down</code>	Enables the device to send SNMP traps (i.e., SNMP notifications) when a link-up or link-down state change occurs	IC
<code>snmp-server enable port-traps mac-notification</code>	Enables the device to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed	IC
<code>show snmp-server enable port-traps</code>	Shows if SNMP traps are enabled or disabled for the specified interfaces	PE
<i>SNMPv3 Engine Commands</i>		
<code>snmp-server engine-id</code>	Sets the SNMP engine ID	GC
<code>snmp-server group</code>	Adds an SNMP group, mapping users to views	GC
<code>snmp-server user</code>	Adds a user to an SNMP group	GC
<code>snmp-server view</code>	Adds an SNMP view	GC

Table 60: SNMP Commands (Continued)

Command	Function	Mode
<code>show snmp engine-id</code>	Shows the SNMP engine ID	PE
<code>show snmp group</code>	Shows the SNMP groups	PE
<code>show snmp user</code>	Shows the SNMP users	PE
<code>show snmp view</code>	Shows the SNMP views	PE
<i>Notification Log Commands</i>		
<code>nlm</code>	Enables the specified notification log	GC
<code>snmp-server notify-filter</code>	Creates a notification log and specifies the target host	GC
<code>show nlm oper-status</code>	Shows operation status of configured notification logs	PE
<code>show snmp notify-filter</code>	Displays the configured notification logs	PE
<i>ATC Trap Commands</i>		
<code>snmp-server enable port-traps atc broadcast-alarm-clear</code>	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
<code>snmp-server enable port-traps atc broadcast-alarm-fire</code>	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control	IC (Port)
<code>snmp-server enable port-traps atc broadcast-control-apply</code>	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
<code>snmp-server enable port-traps atc broadcast-control-release</code>	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
<code>snmp-server enable port-traps atc multicast-alarm-clear</code>	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
<code>snmp-server enable port-traps atc multicast-alarm-fire</code>	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control	IC (Port)
<code>snmp-server enable port-traps atc multicast-control-apply</code>	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
<code>snmp-server enable port-traps atc multicast-control-release</code>	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
<i>Transceiver Power Threshold Trap Commands</i>		
<code>transceiver-threshold current</code>	Sends a trap when the transceiver current falls outside the specified thresholds	IC (Port)
<code>transceiver-threshold rx-power</code>	Sends a trap when the power level of the received signal falls outside the specified thresholds	IC (Port)
<code>transceiver-threshold temperature</code>	Sends a trap when the transceiver temperature falls outside the specified thresholds	IC (Port)
<code>transceiver-threshold tx-power</code>	Sends a trap when the power level of the transmitted signal power outside the specified thresholds	IC (Port)
<code>transceiver-threshold voltage</code>	Sends a trap when the transceiver voltage falls outside the specified thresholds	IC (Port)

Table 60: SNMP Commands (Continued)

Command	Function	Mode
<i>Additional Trap Commands</i>		
<code>memory</code>	Sets the rising and falling threshold for the memory utilization alarm	GC
<code>process cpu</code>	Sets the rising and falling threshold for the CPU utilization alarm	GC
<code>process cpu guard</code>	Sets the CPU utilization watermark and threshold	GC
<code>show memory</code>	Shows memory utilization parameters	PE
<code>show process cpu</code>	Shows CPU utilization parameters	NE, PE
<code>show process cpu guard</code>	Shows the CPU utilization watermark and threshold	PE
<code>show process cpu task</code>	Shows CPU utilization per process	NE, PE

General SNMP Commands

snmp-server This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

Syntax

[no] snmp-server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server
Console(config)#
```

snmp-server community This command defines community access strings used to authorize management access by clients using SNMP v1 or v2c. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro** | **rw**]

no snmp-server community *string*

string - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)

ro - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

rw - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

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

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*

no snmp-server contact

string - String that describes the system contact information.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

[snmp-server location \(595\)](#)

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 \(594\)](#)

show snmp This command can be used to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counters for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
Console#show snmp

SNMP Agent : Enabled

SNMP Traps :
  Authentication : Enabled
  MAC-notification : Disabled
  MAC-notification interval : 1 second(s)

SNMP Communities :
  1. public, and the access level is read-only
```

```
2. private, and the access level is read/write

0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs

SNMP Logging: Disabled
Console#
```

SNMP Target Host Commands

snmp-server enable traps This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

[no] snmp-server enable traps [authentication | mac-notification [interval seconds]]

authentication - Keyword to issue authentication failure notifications.

mac-notification - Keyword to issue trap when a dynamic MAC address is added or removed.

interval - Specifies the interval between issuing two consecutive traps. (Range: 1-3600 seconds; Default: 1 second)

Default Setting

Issue authentication traps
Other traps are disabled

Command Mode

Global Configuration

Command Usage

- ◆ If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication

notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

- ◆ The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.
- ◆ The authentication traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the **snmp-server group** command.

Example

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

Related Commands

[snmp-server host \(597\)](#)

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](#)” 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 593](#)).
2. Create a view with the required notification messages ([page 605](#)).
3. Create a group that includes the required notify view ([page 602](#)).
4. Allow the switch to send SNMP traps; i.e., notifications ([page 596](#)).

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 593](#)).
 2. Create a remote SNMPv3 user to use in the message exchange process ([page 603](#)).
 3. Create a view with the required notification messages ([page 605](#)).
 4. Create a group that includes the required notify view ([page 602](#)).
 5. Allow the switch to send SNMP traps; i.e., notifications ([page 596](#)).
 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 ([596](#))

snmp-server enable port-traps link-up-down	This command enables the device to send SNMP traps (i.e., SNMP notifications) when a link-up or link-down state change occurs. Use the no form to restore the default setting.

Syntax

[no] snmp-server enable port-traps link-up-down

link-up-down - Keyword to issue trap when a link-up or link-down state change occurs.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps mac-notification
Console(config)#
```

snmp-server enable port-traps mac-notification This command enables the device to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed. Use the **no** form to restore the default setting.

Syntax

[no] snmp-server enable port-traps mac-notification

mac-notification - Keyword to issue trap when a dynamic MAC address is added or removed.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command can enable MAC authentication traps on the current interface only if they are also enabled at the global level with the **snmp-server enable traps mac-authentication** command.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps mac-notification
Console(config)#
```

show snmp-server enable port-traps This command shows if SNMP traps are enabled or disabled for the specified interfaces.

Syntax

show snmp-server enable port-traps interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Command Mode

Privileged Exec

Example

```
Console#show snmp-server enable port-traps interface
Interface MAC Notification Trap
-----
Eth 1/1                               No
Eth 1/2                               No
Eth 1/3                               No
:
```

SNMPv3 Commands

snmp-server engine-id This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

Syntax

snmp-server engine-id {**local** | **remote** {*ip-address*}} *engineid-string*

no snmp-server engine-id {**local** | **remote** {*ip-address*}}

local - Specifies the SNMP engine on this switch.

remote - Specifies an SNMP engine on a remote device.

ip-address - IPv4 or IPv6 address of the remote device.

engineid-string - String identifying the engine ID. (Range: 9-64 hexadecimal characters)

Default Setting

A unique engine ID is automatically generated by the switch based on its MAC address.

Command Mode

Global Configuration

Command Usage

- ◆ An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
- ◆ A remote engine ID is required when using SNMPv3 informs. (See the [snmp-server host](#) command.) The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the

remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

- ◆ Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value "0123456789" is equivalent to "0123456789" followed by 16 zeroes for a local engine ID.
- ◆ A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users (page 603).

Example

```
Console(config)#snmp-server engine-id local 1234567890
Console(config)#snmp-server engine-id remote 192.168.1.19 9876543210
Console(config)#
```

Related Commands

[snmp-server host \(597\)](#)

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](#)" 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: public¹⁰ (read only), private¹¹ (read/write)

readview - Every object belonging to the Internet OID space (1).

writeview - Nothing is defined.

notifyview - Nothing is defined.

¹⁰. No view is defined.

Command Mode

Global Configuration

Command Usage

- ◆ A group sets the access policy for the assigned users.
- ◆ When authentication is selected, the MD5 or SHA algorithm is used as specified in the `snmp-server user` command.
- ◆ When privacy is selected, the DES 56-bit algorithm is used for data encryption.
- ◆ For additional information on the notification messages supported by this switch, see “Supported Notification Messages”. Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the `snmp-server enable traps` command.

Example

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

snmp-server user This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the **no** form to remove a user from an SNMP group.

Syntax

snmp-server user *username* *groupname*
{**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv** {**3des** | **aes128** | **aes192** | **aes256** | **des56**} *priv-password*]]

snmp-server user *username* *groupname* **remote** *ip-address*
{**v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv** {**3des** | **aes128** | **aes192** | **aes256** | **des56**} *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote** *ip-address* **v3**}

username - Name of user connecting to the SNMP agent.
(Range: 1-32 characters)

groupname - Name of an SNMP group to which the user is assigned.
(Range: 1-32 characters)

remote - Specifies an SNMP engine on a remote device.

ip-address - IPv4 address of the remote device.

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

encrypted - Accepts the password as encrypted input.

auth - Uses SNMPv3 with authentication.

11. Maps to the defaultview.

md5 | sha - Uses MD5 or SHA authentication.

auth-password - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (Range: 8-32 characters for unencrypted password.)

If the **encrypted** option is selected, enter an encrypted password. (Range: 32 characters for MD5 encrypted password, 40 characters for SHA encrypted password)

3des - Uses SNMPv3 with privacy with 3DES (168-bit) encryption.

aes128 - Uses SNMPv3 with privacy with AES128 encryption.

aes192 - Uses SNMPv3 with privacy with AES192 encryption.

aes256 - Uses SNMPv3 with privacy with AES256 encryption.

des56 - Uses SNMPv3 with privacy with DES56 encryption.

priv-password - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (Range: 8-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Local users (i.e., the command does not specify a remote engine identifier) must be configured to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch.
- ◆ Remote users (i.e., the command specifies a remote engine identifier) must be configured to identify the source of SNMPv3 inform messages sent from the local switch.
- ◆ The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the [snmp-server engine-id](#) command before using this configuration command.
- ◆ Before you configure a remote user, use the [snmp-server engine-id](#) command to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.
- ◆ SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore

need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

Example

```
Console(config)#snmp-server user steve r&d v3 auth md5 greenpeace priv des56
einstien
Console(config)#snmp-server engine-id remote 192.168.1.19 9876543210
Console(config)#snmp-server user mark r&d remote 192.168.1.19 v3 auth md5
greenpeace priv des56 einstien
Console(config)#
```

snmp-server view This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

Syntax

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name*

view-name - Name of an SNMP view. (Range: 1-32 characters)

oid-tree - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)

included - Defines an included view.

excluded - Defines an excluded view.

Default Setting

defaultview (includes access to the entire MIB tree)

Command Mode

Global Configuration

Command Usage

- ◆ Views are used in the [snmp-server group](#) command to restrict user access to specified portions of the MIB tree.
- ◆ The predefined view "defaultview" includes access to the entire MIB tree.

Examples

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in the following table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included
Console(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included
Console(config)#
```

show snmp engine-id This command shows the SNMP engine ID.

Command Mode

Privileged Exec

Example

This example shows the default engine ID.

```
Console#show snmp user
No user exist.

SNMP remote user
No user exist.
Console#show snmp engine-id
Local SNMP Engine ID      : 800041AD03CC37ABD7A6840000
Local SNMP Engine Boots   : 13

Remote SNMP Engine ID      IP address
800000000030001234567854321 192.168.16.26
Console#
```

Table 61: show snmp engine-id - display description

Field	Description
Local SNMP engineID	String identifying the engine ID.
Local SNMP engineBoots	The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.
Remote SNMP engineID	String identifying an engine ID on a remote device.
IP address	IP address of the device containing the corresponding remote SNMP engine.

show snmp group Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

Command Mode

Privileged Exec

Example

```

Console#show snmp group
Group Name       : r&d
Security Model   : v3
Security Level   : Authentication and privacy
Read View        : No readview specified
Write View       : No writeview specified
Notify View      : No notifyview specified
Storage Type     : Nonvolatile
Row Status       : Active

Group Name       : public
Security Model   : v1
Read View        : defaultview
Write View       : No writeview specified
Notify View      : No notifyview specified
Storage Type     : Volatile
Row Status       : Active

Group Name       : public
Security Model   : v2c
Read View        : defaultview
Write View       : No writeview specified
Notify View      : No notifyview specified
Storage Type     : Volatile
Row Status       : Active

Group Name       : private
Security Model   : v1
Read View        : defaultview
Write View       : defaultview
Notify View      : No notifyview specified
Storage Type     : Volatile
Row Status       : Active

Group Name       : private
Security Model   : v2c
Read View        : defaultview
Write View       : defaultview
Notify View      : No notifyview specified
Storage Type     : Volatile
Row Status       : Active
Console#

```

Table 62: show snmp group - display description

Field	Description
Group Name	Name of an SNMP group.
Security Model	The SNMP version.
Security Level	This associated security level can use SNMPv3 with authentication, no authentication, or with authentication and privacy.

Table 62: show snmp group - display description (Continued)

Field	Description
Read View	The associated read view.
Write View	The associated write view.
Notify View	The associated notify view.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.

show snmp user This command shows information on SNMP users.

Command Mode

Privileged Exec

Example

```
Console#show snmp user
Engine ID           : 800041ad03cc37abd7a6840000
User Name           : Steve
Group Name          : public
Security Model       : v1
Authentication Protocol : None
Privacy Protocol     : None
Storage Type        : Nonvolatile
Row Status          : Active

SNMP remote user
Engine ID           : 80000000030001234567854321
User Name           : Mark
Group Name          : public
Security Model       : v3
Security Level       : No authentication and no privacy
Authentication Protocol : None
Privacy Protocol     : None
Storage Type        : Nonvolatile
Row Status          : Active
Console#
```

Table 63: show snmp user - display description

Field	Description
Engine ID	String identifying the engine ID.
User Name	Name of user connecting to the SNMP agent.
Group Name	Name of an SNMP group.
Security Model	The user security model: SNMP v1, v2c or v3.
Security Level	Indicates if authentication or encryption are used.
Authentication Protocol	The authentication protocol used with SNMPv3.
Privacy Protocol	The privacy protocol used with SNMPv3.

Table 63: show snmp user - display description (Continued)

Field	Description
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.
SNMP remote user	A user associated with an SNMP engine on a remote device.

show snmp view This command shows information on the SNMP views.

Command Mode

Privileged Exec

Example

```

Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active

View Name      : defaultview
Subtree OID    : 1
View Type      : included
Storage Type   : volatile
Row Status     : active
Console#

```

Table 64: show snmp view - display description

Field	Description
View Name	Name of an SNMP view.
Subtree OID	A branch in the MIB tree.
View Type	Indicates if the view is included or excluded.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.

Notification Log Commands

nlm This command enables or disables the specified notification log.

Syntax

[no] nlm *filter-name*

filter-name - Notification log name. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Notification logging is enabled by default, but will not start recording information until a logging profile specified by the [snmp-server notify-filter](#) command is enabled by the **nlm** command.
- ◆ Disabling logging with this command does not delete the entries stored in the notification log.

Example

This example enables the notification log A1.

```
Console(config)#nlm A1
Console(config)#
```

snmp-server notify-filter This command creates an SNMP notification log. Use the **no** form to remove this log.

Syntax

[no] snmp-server notify-filter *profile-name* **remote** *ip-address*

profile-name - Notification log profile name. (Range: 1-32 characters)

ip-address - IPv4 or IPv6 address of a remote device. The specified target host must already have been configured using the [snmp-server host](#) command.



Note: The notification log is stored locally. It is not sent to a remote device. This remote host parameter is only required to complete mandatory fields in the SNMP Notification MIB.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Systems that support SNMP often need a mechanism for recording Notification information as a hedge against lost notifications, whether there are Traps or Informs that may exceed retransmission limits. The Notification Log MIB (NLM,

RFC 3014) provides an infrastructure in which information from other MIBs may be logged.

- ◆ Given the service provided by the NLM, individual MIBs can now bear less responsibility to record transient information associated with an event against the possibility that the Notification message is lost, and applications can poll the log to verify that they have not missed any important Notifications.
- ◆ If notification logging is not configured and enabled, when the switch reboots, some SNMP traps (such as warm start) cannot be logged.
- ◆ To avoid this problem, notification logging should be configured and enabled using the **snmp-server notify-filter** command and **nlm** command, and these commands stored in the startup configuration file. Then when the switch reboots, SNMP traps (such as warm start) can now be logged.
- ◆ When this command is executed, a notification log is created (with the default parameters defined in RFC 3014). Notification logging is enabled by default (see the **nlm** command), but will not start recording information until a logging profile specified with this command is enabled with the **nlm** command.
- ◆ Based on the default settings used in RFC 3014, a notification log can contain up to 256 entries, and the entry aging time is 1440 minutes. Information recorded in a notification log, and the entry aging time can only be configured using SNMP from a network management station.
- ◆ When a trap host is created with the **snmp-server host** command, a default notify filter will be created as shown in the example under the **show snmp notify-filter** command.

Example

This example first creates an entry for a remote host, and then instructs the switch to record this device as the remote host for the specified notification log.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server notify-filter A1 remote 10.1.19.23
Console#
```

show nlm oper-status This command shows the operational status of configured notification logs.

Command Mode

Privileged Exec

Example

```
Console#show nlm oper-status
Filter Name: A1
Oper-Status: Operational
Console#
```

show snmp notify-filter This command displays the configured notification logs.

Command Mode

Privileged Exec

Example

This example displays the configured notification logs and associated target hosts.

```
Console#show snmp notify-filter
Filter profile name      IP address
-----
A1                      10.1.19.23
Console#
```

Additional Trap Commands

memory This command sets an SNMP trap based on configured thresholds for memory utilization. Use the **no** form to restore the default setting.

Syntax

memory {**rising** *rising-threshold* | **falling** *falling-threshold*}

no memory {**rising** | **falling**}

rising-threshold - Rising threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

falling-threshold - Falling threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

Default Setting

Rising Threshold: 90%

Falling Threshold: 70%

Command Mode

Global Configuration

Command Usage

Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

Example

```
Console(config)#memory rising 80
Console(config)#memory falling 60
Console#
```

Related Commands

[show memory \(529\)](#)

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 \(530\)](#)

process cpu guard This command sets the CPU utilization high and low watermarks in percentage of CPU time utilized and the CPU high and low thresholds in the number of packets being processed per second. Use the **no** form of this command without any parameters to restore all of the default settings, or with a specific parameter to restore the default setting for that item.

Syntax

process cpu guard [**high-watermark** *high-watermark* |
low-watermark *low-watermark* | **max-threshold** *max-threshold* |
min-threshold *min-threshold* | **trap**]

high-watermark - If the percentage of CPU usage time is higher than the high-watermark, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until usage time falls below the low watermark. (Range: 40-100%)

low-watermark - If packet flow has been stopped after exceeding the high watermark, normal flow will be restored after usage falls beneath the low watermark. (Range: 40-100%)

max-threshold - If the number of packets being processed per second by the CPU is higher than the maximum threshold, the switch stops packet flow to the CPU (allowing it to catch up with packets already in the buffer) until the number of packets being processed falls below the minimum threshold. (Range: 50-500 pps)

min-threshold - If packet flow has been stopped after exceeding the maximum threshold, normal flow will be restored after usage falls beneath the minimum threshold. (Range: 50-500 pps)

trap - If traps are enabled, the switch will send an alarm message if CPU utilization exceeds the high watermark in percentage of CPU usage time or exceeds the maximum threshold in the number of packets being processed by the CPU.

Default Setting

Guard Status: Disabled

High Watermark: 90%

Low Watermark: 70%

Maximum Threshold: 500 packets per second

Minimum Threshold: 50 packets per second

Trap Status: Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Once the high watermark is exceeded, utilization must drop beneath the low watermark before the alarm is terminated, and then exceed the high watermark again before another alarm is triggered.

- ◆ Once the maximum threshold is exceeded, utilization must drop beneath the minimum threshold before the alarm is terminated, and then exceed the maximum threshold again before another alarm is triggered.

Example

```
Console(config)#process cpu guard high-watermark 80
Console(config)#process cpu guard low-watermark 60
Console(config)#
```

Related Commands

[show process cpu guard \(530\)](#)

Remote Monitoring Commands

Remote Monitoring allows a remote device to collect information or respond to specified events on an independent basis. This switch is an RMON-capable device which can independently perform a wide range of tasks, significantly reducing network management traffic. It can continuously run diagnostics and log information on network performance. If an event is triggered, it can automatically notify the network administrator of a failure and provide historical information about the event. If it cannot connect to the management agent, it will continue to perform any specified tasks and pass data back to the management station the next time it is contacted.

This switch supports mini-RMON, which consists of the Statistics, History, Event and Alarm groups. When RMON is enabled, the system gradually builds up information about its physical interfaces, storing this information in the relevant RMON database group. A management agent then periodically communicates with the switch using the SNMP protocol. However, if the switch encounters a critical event, it can automatically send a trap message to the management agent which can then respond to the event if so configured.

Table 65: RMON Commands

Command	Function	Mode
<code>rmon alarm</code>	Sets threshold bounds for a monitored variable	GC
<code>rmon event</code>	Creates a response event for an alarm	GC
<code>rmon collection history</code>	Periodically samples statistics	IC
<code>rmon collection rmon1</code>	Enables statistics collection	IC
<code>show rmon alarms</code>	Shows the settings for all configured alarms	PE
<code>show rmon events</code>	Shows the settings for all configured events	PE
<code>show rmon history</code>	Shows the sampling parameters for each entry	PE
<code>show rmon statistics</code>	Shows the collected statistics	PE

rmon alarm This command sets threshold bounds for a monitored variable. Use the **no** form to remove an alarm.

Syntax

rmon alarm *index variable interval {absolute | delta}*
rising-threshold *threshold [event-index]* **falling-threshold** *threshold*
[event-index] [owner name]

no rmon alarm *index*

index – Index to this entry. (Range: 1-65535)

variable – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled. Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.

interval – The polling interval. (Range: 1-31622400 seconds)

absolute – The variable is compared directly to the thresholds at the end of the sampling period.

delta – The last sample is subtracted from the current value and the difference is then compared to the thresholds.

threshold – An alarm threshold for the sampled variable.
 (Range: 0-2147483647)

event-index – The index of the event to use if an alarm is triggered. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 1-65535)

name – Name of the person who created this entry. (Range: 1-127 characters)

Default Setting

1.3.6.1.4.1.16813.26.104.1 - 1.3.6.1.4.1.16813.26.104.28

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 563).

trap – Sends a trap message to all configured trap managers (see the [snmp-server host](#) command).

community – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts. Although this string can be set using the **rmon event** command by itself, it is recommended that the string be defined using the [snmp-server community](#) command prior to using the **rmon event** command. (Range: 1-32 characters)

string – A comment that describes this event. (Range: 1-127 characters)

name – Name of the person who created this entry.
(Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.
- ◆ The specified events determine the action to take when an alarm triggers this event. The response to an alarm can include logging the alarm or sending a message to a trap manager.

Example

```
Console(config)#rmon event 2 log description urgent owner mike
Console(config)#
```

rmon collection history This command periodically samples statistics on a physical interface. Use the no form to disable periodic sampling.

Syntax

rmon collection history controlEntry *index*

[**buckets** *number* [**interval** *seconds*]] |

[**interval** *seconds*] |

[**owner** *name* [**buckets** *number* [**interval** *seconds*]]]

no rmon collection history controlEntry *index*

index – Index to this entry. (Range: 1-65535)

number – The number of buckets requested for this entry. (Range: 1-65536)

seconds – The polling interval. (Range: 1-3600 seconds)

name – Name of the person who created this entry.
(Range: 1-32 characters)

Default Setting

1.3.6.1.4.1.16813.26.104.1 - 1.3.6.1.4.1.16813.26.104.28

Buckets: 8

Interval: 30 seconds for even numbered entries,
1800 seconds for odd numbered entries

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.
- ◆ If periodic sampling is already enabled on an interface, the entry must be deleted before any changes can be made with this command.

- ◆ The information collected for each sample includes:
input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and network utilization.
- ◆ The switch reserves two controlEntry index entries for each port. If a default index entry is re-assigned to another port by this command, the **show running-config** command will display a message indicating that this index is not available for the port to which is normally assigned.

For example, if control entry 15 is assigned to port 5 as shown below, the **show running-config** command will indicate that this entry is not available for port 8.

```
Console(config)#interface ethernet 1/5
Console(config-if)#rmon collection history controlEntry 15
Console(config-if)#end
Console#show running-config
!
interface ethernet 1/5
  rmon collection history controlEntry 15 buckets 50 interval 1800
...
interface ethernet 1/8
  no rmon collection history controlEntry 15
```

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection history controlentry 21 owner mike buckets
  24 interval 60
Console(config-if)#
```

rmon collection rmon1 This command enables the collection of statistics on a physical interface. Use the **no** form to disable statistics collection.

Syntax

rmon collection rmon1 controlEntry *index* [**owner** *name*]

no rmon collection rmon1 controlEntry *index*

index – Index to this entry. (Range: 1-65535)

name – Name of the person who created this entry.
(Range: 1-32 characters)

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.
- ◆ If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made with this command.
- ◆ The information collected for each entry includes:
input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and packets of specified lengths

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection rmon1 controentry 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
:
```

Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access¹² to the data ports.

Table 66: 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

¹². For other methods of controlling client access, see [“General Security Measures”](#) on page 684.

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 552](#)), user authentication via a remote authentication server ([page 623](#)), and host access authentication for specific ports ([page 666](#)).

Table 67: User Access Commands

Command	Function	Mode
enable password	Sets a password to control access to the Privileged Exec level	GC
username	Establishes a user name-based authentication system at login	GC
privilege	Assigns a privilege level to specified command groups or individual commands	GC
show privilege	Shows the privilege level for the current user, or the privilege level for commands modified by the privilege command	PE

enable password After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*

no enable password [**level** *level*]

level *level* - Sets the command access privileges. (Range: 0-15)

Level 0, 8 and 15 are designed for users (guest), managers (network maintenance), and administrators (top-level access). The other levels can be used to configured specialized access profiles.

Level 0-7 provide the same default access privileges, all within Normal Exec mode under the "Console>" command prompt.

Level 8-14 provide the same default access privileges, including additional commands in Normal Exec mode, and a subset of commands in Privileged Exec mode under the "Console#" command prompt.

Level 15 provides full access to all commands.

The privilege level associated with any command can be changed using the [privilege](#) command.

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

password - Password for this privilege level.

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

Default Setting

The default is level 15.

The default password is “super”

Command Mode

Global Configuration

Command Usage

- ◆ You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the [enable](#) command.
- ◆ The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

[enable](#) (520)

[authentication enable](#) (628)

username This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}

no username *name*

name - The name of the user. (Maximum length: 32 characters, case sensitive. Maximum users: 16)

The device has two predefined users, **guest** which is assigned privilege level **0** (Normal Exec) and has access to a limited number of commands, and **admin** which is assigned privilege level 15 and has full access to all commands.

access-level *level* - Specifies command access privileges. (Range: 0-15)

Level 0, 8 and 15 are designed for users (guest), managers (network maintenance), and administrators (top-level access). The other levels can be used to configured specialized access profiles.

Level 0-7 provide the same default access privileges, all within Normal Exec mode under the “Console>” command prompt.

Level 8-14 provide the same default access privileges, including additional commands in Normal Exec mode, and a subset of commands in Privileged Exec mode under the "Console#" command prompt.

Level 15 provides full access to all commands.

The privilege level associated with any command can be changed using the `privilege` command.

Any privilege level can access all of the commands assigned to lower privilege levels. For example, privilege level 8 can access all commands assigned to privilege levels 7-0 according to default settings, and to any other commands assigned to levels 7-0 using the `privilege` command.

nopassword - No password is required for this user to log in.

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

password *password* - The authentication password for the user. (Maximum length: 32 characters plain text or encrypted, case sensitive)

Default Setting

The default access level is 0 (Normal Exec).

The factory defaults for the user names and passwords are:

Table 68: Default Login Settings

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup. There is no need for you to manually configure encrypted passwords.

Example

This example shows how to set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

privilege This command assigns a privilege level to specified command groups or individual commands. Use the **no** form to restore the default setting.

Syntax

privilege *mode* [**all**] **level** *level command*

no privilege *mode* [**all**] *command*

mode - The configuration mode containing the specified *command*.
(See “[Understanding Command Modes](#)” on page 512 and “[Configuration Commands](#)” on page 513.)

all - Modifies the privilege level for all subcommands under the specified *command*.

level *level* - Specifies the privilege level for the specified *command*. Refer to the default settings described for the access level parameter under the [username](#) command. (Range: 0-15)

command - Specifies any command contained within the specified *mode*.

Default Setting

Privilege level 0 provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Level 8 provides access to all display status and configuration commands, except for those controlling various authentication and security features. Level 15 provides full access to all commands.

Command Mode

Global Configuration

Example

This example sets the privilege level for the ping command to Privileged Exec.

```
Console(config)#privilege exec level 15 ping
Console(config)#
```

show privilege This command shows the privilege level for the current user, or the privilege level for commands modified by the [privilege](#) command.

Syntax

show privilege [**command**]

command - Displays the privilege level for all commands modified by the [privilege](#) command.

Command Mode

Privileged Exec

Example

This example shows the privilege level for any command modified by the [privilege](#) command.

```
Console#show privilege command
privilege line all level 0 accounting
privilege exec level 15 ping
Console(config)#
```

Authentication Sequence

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

Table 69: 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 (624)

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 (625)

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 70: RADIUS Client Commands

Command	Function	Mode
radius-server acct-port	Sets the RADIUS server network port	GC
radius-server auth-port	Sets the RADIUS server network port	GC
radius-server host	Specifies the RADIUS server	GC
radius-server key	Sets the RADIUS encryption key	GC
radius-server retransmit	Sets the number of retries	GC
radius-server timeout	Sets the interval between sending authentication requests	GC
show radius-server	Shows the current RADIUS settings	PE

radius-server acct-port This command sets the RADIUS server network port for accounting messages. Use the **no** form to restore the default.

Syntax

radius-server acct-port *port-number*

no radius-server acct-port

port-number - RADIUS server UDP port used for accounting messages.
(Range: 1-65535)

Default Setting

1813

Command Mode

Global Configuration

Example

```
Console(config)#radius-server acct-port 181
Console(config)#
```

radius-server auth-port This command sets the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server auth-port *port-number*

no radius-server auth-port

port-number - RADIUS server UDP port used for authentication messages.
(Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server auth-port 181
Console(config)#
```

radius-server host This command specifies primary and backup RADIUS servers, and authentication and accounting parameters that apply to each server. Use the **no** form to remove a specified server, or to restore the default values.

Syntax

[no] radius-server *index* **host** *host-ip-address* [**acct-port** *acct-port*] [**auth-port** *auth-port*] [**key** *key*] [**retransmit** *retransmit*] [**timeout** *timeout*]

index - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.

host-ip-address - IP address of server.

acct-port - RADIUS server UDP port used for accounting messages.
(Range: 1-65535)

auth-port - RADIUS server UDP port used for authentication messages.
(Range: 1-65535)

key - Encryption key used to authenticate logon access for client. Enclose any string containing blank spaces in double quotes.
(Maximum length: 48 characters)

retransmit - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

auth-port - 1812
acct-port - 1813
timeout - 5 seconds
retransmit - 2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10  
retransmit 5 key green  
Console(config)#
```

radius-server key This command sets the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key-string*

no radius-server key

key-string - Encryption key used to authenticate logon access for client.
Enclose any string containing blank spaces in double quotes.
(Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green  
Console(config)#
```

radius-server retransmit This command sets the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number-of-retries*

no radius-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5  
Console(config)#
```

radius-server timeout This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number-of-seconds*

no radius-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10  
Console(config)#
```

show radius-server This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```

Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
  Authentication Port Number : 1812
  Accounting Port Number    : 1813
  Retransmit Times          : 2
  Request Timeout           : 5

Server 1:
  Server IP Address          : 192.168.1.1
  Authentication Port Number : 1812
  Accounting Port Number     : 1813
  Retransmit Times           : 2
  Request Timeout            : 5

RADIUS Server Group:
Group Name      Member Index
-----
radius          1
Console#

```

TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 71: TACACS+ Client Commands

Command	Function	Mode
tacacs-server host	Specifies the TACACS+ server and optional parameters	GC
tacacs-server key	Sets the TACACS+ encryption key	GC
tacacs-server port	Specifies the TACACS+ server network port	GC
tacacs-server retransmit	Sets the number of retries	GC
tacacs-server timeout	Sets the interval between sending authentication requests	GC
show tacacs-server	Shows the current TACACS+ settings	GC

tacacs-server host This command specifies the TACACS+ server and other optional parameters. Use the **no** form to remove the server, or to restore the default values.

Syntax

tacacs-server *index* **host** *host-ip-address* [**key** *key*] [**port** *port-number*]
[**retransmit** *retransmit*] [**timeout** *timeout*]

no tacacs-server *index*

index - The index for this server. (Range: 1)

host-ip-address - IP address of a TACACS+ server.

key - Encryption key used to authenticate logon access for the client.
Enclose any string containing blank spaces in double quotes.
(Maximum length: 48 characters)

port-number - TACACS+ server TCP port used for authentication messages.
(Range: 1-65535)

retransmit - Number of times the switch will try to authenticate logon
access via the TACACS+ server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending
a request. (Range: 1-540)

Default Setting

authentication port - 49

timeout - 5 seconds

retransmit - 2

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server 1 host 192.168.1.25 port 181 timeout 10  
retransmit 5 key green  
Console(config)#
```

tacacs-server key This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server key *key-string*

no tacacs-server key

key-string - Encryption key used to authenticate logon access for the client.
Enclose any string containing blank spaces in double quotes.
(Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

tacacs-server port This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port-number*

no tacacs-server port

port-number - TACACS+ server TCP port used for authentication messages.
(Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server retransmit This command sets the number of retries. Use the **no** form to restore the default.

Syntax

tacacs-server retransmit *number-of-retries*

no tacacs-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server retransmit 5
Console(config)#
```

tacacs-server timeout This command sets the interval between transmitting authentication requests to the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server timeout *number-of-seconds*

no tacacs-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server timeout 10
Console(config)#
```

show tacacs-server This command displays the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server

Remote TACACS+ Server Configuration:

Global Settings:
  Server Port Number : 49
  Retransmit Times   : 2
  Timeout            : 5

Server 1:
  Server IP Address  : 10.11.12.13
  Server Port Number : 49
  Retransmit Times   : 2
  Timeout            : 4
```

```
TACACS+ Server Group:
Group Name          Member Index
-----
tacacs+             1
Console#
```

AAA

The Authentication, Authorization, and Accounting (AAA) feature provides the main framework for configuring access control on the switch. The AAA functions require the use of configured RADIUS or TACACS+ servers in the network.

Table 72: AAA Commands

Command	Function	Mode
aaa accounting commands	Enables accounting of Exec mode commands	GC
aaa accounting dot1x	Enables accounting of 802.1X services	GC
aaa accounting exec	Enables accounting of Exec services	GC
aaa accounting update	Enables periodic updates to be sent to the accounting server	GC
aaa authorization commands	Enables accounting of Exec mode commands	GC
aaa authorization exec	Enables authorization of Exec sessions	GC
aaa group server	Groups security servers in to defined lists	GC
server	Configures the IP address of a server in a group list	SG
accounting dot1x	Applies an accounting method to an interface for 802.1X service requests	IC
accounting commands	Applies an accounting method to CLI commands entered by a user	Line
accounting exec	Applies an accounting method to local console, Telnet or SSH connections	Line
authorization commands	Applies an authorization method to CLI commands entered by a user	Line
authorization exec	Applies an authorization method to local console, Telnet or SSH connections	Line
show accounting	Displays all accounting information	PE
show authorization	Displays all authorization information	PE

aaa accounting commands This command enables the accounting of Exec mode commands. Use the **no** form to disable the accounting service.

Syntax

aaa accounting commands *level* {**default** | *method-name*} **start-stop** **group** {**tacacs+** | *server-group*}

no aaa accounting commands *level* {**default** | *method-name*}

level - The privilege level for executing commands. (Range: 0-15)

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests.
(Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Accounting is not enabled
No servers are specified

Command Mode

Global Configuration

Command Usage

- ◆ The accounting of Exec mode commands is only supported by TACACS+ servers.
- ◆ Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified TACACS+ server, and do not actually send any information to the server about the methods to use.

Example

```
Console(config)#aaa accounting commands 15 default start-stop group tacacs+
Console(config)#
```

aaa accounting dot1x This command enables the accounting of requested 802.1X services for network access. Use the **no** form to disable the accounting service.

Syntax

```
aaa accounting dot1x {default | method-name}  
start-stop group {radius | tacacs+ | server-group}  
no aaa accounting dot1x {default | method-name}
```

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests.
(Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the [radius-server host](#) command.

tacacs+ - Specifies all TACACS+ hosts configure with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Accounting is not enabled
No servers are specified

Command Mode

Global Configuration

Command Usage

Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

Example

```
Console(config)#aaa accounting dot1x default start-stop group radius  
Console(config)#
```

aaa accounting exec This command enables the accounting of requested Exec services for network access. Use the **no** form to disable the accounting service.

Syntax

```
aaa accounting exec {default | method-name}
start-stop group {radius | tacacs+ | server-group}
no aaa accounting exec {default | method-name}
```

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests.
(Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the [radius-server host](#) command.

tacacs+ - Specifies all TACACS+ hosts configure with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the [aaa group server](#) command. (Range: 1-64 characters)

Default Setting

Accounting is not enabled
No servers are specified

Command Mode

Global Configuration

Command Usage

- ◆ This command runs accounting for Exec service requests for the local console and Telnet connections.
- ◆ Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

Example

```
Console(config)#aaa accounting exec default start-stop group tacacs+
Console(config)#
```

aaa accounting update This command enables the sending of periodic updates to the accounting server. Use the **no** form to disable accounting updates.

Syntax

aaa accounting update [**periodic** *interval*]

no aaa accounting update

interval - Sends an interim accounting record to the server at this interval.
(Range: 1-2147483647 minutes)

Default Setting

1 minute

Command Mode

Global Configuration

Command Usage

- ◆ When accounting updates are enabled, the switch issues periodic interim accounting records for all users on the system.
- ◆ Using the command without specifying an interim interval enables updates, but does not change the current interval setting.

Example

```
Console(config)#aaa accounting update periodic 30
Console(config)#
```

aaa authorization commands This command enables the authorization of Exec mode commands. Use the **no** form to disable the authorization service.

Syntax

aaa authorization commands *level* {**default** | *method-name*} **start-stop** **group** {**tacacs+** | *server-group*}

no aaa authorization commands *level* {**default** | *method-name*}

level - The privilege level for executing commands. (Range: 0-15)

default - Specifies the default authorization method for service requests.

method-name - Specifies an authorization method for service requests.
(Range: 1-64 characters)

start-stop - Records authorization from starting point and stopping point.

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the [tacacs-server host](#) command.

server-group - Specifies the name of a server group configured with the `aaa group server` command. (Range: 1-64 characters)

Default Setting

Authorization is not enabled
No servers are specified

Command Mode

Global Configuration

Command Usage

- ◆ The authorization of Exec mode commands is only supported by TACACS+ servers.
- ◆ Note that the **default** and *method-name* fields are only used to describe the authorization method(s) configured on the specified TACACS+ server, and do not actually send any information to the server about the methods to use.

Example

```
Console(config)#aaa authorization commands 15 default start-stop group
tacacs+
Console(config)#
```

aaa authorization exec This command enables the authorization for Exec access. Use the **no** form to disable the authorization service.

Syntax

aaa authorization exec {**default** | *method-name*}
group {**tacacs+** | *server-group*}

no aaa authorization exec {**default** | *method-name*}

default - Specifies the default authorization method for Exec access.

method-name - Specifies an authorization method for Exec access.
(Range: 1-64 characters)

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the `tacacs-server host` command.

server-group - Specifies the name of a server group configured with the `aaa group server` command. (Range: 1-64 characters)

Default Setting

Authorization is not enabled
No servers are specified

Command Mode

Global Configuration

Command Usage

- ◆ This command performs authorization to determine if a user is allowed to run an Exec shell for local console, Telnet, or SSH connections.
- ◆ AAA authentication must be enabled before authorization is enabled.
- ◆ If this command is issued without a specified named method, the default method list is applied to all interfaces or lines (where this authorization type applies), except those that have a named method explicitly defined.

Example

```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

aaa group server Use this command to name a group of security server hosts. To remove a server group from the configuration list, enter the **no** form of this command.

Syntax

[no] **aaa group server** {**radius** | **tacacs+**} *group-name*

radius - Defines a RADIUS server group.

tacacs+ - Defines a TACACS+ server group.

group-name - A text string that names a security server group.
(Range: 1-64 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```


server This command adds a security server to an AAA server group. Use the **no** form to remove the associated server from the group.

Syntax

[no] server {*index* | *ip-address*}

index - Specifies the server index. (Range: RADIUS 1-5, TACACS+ 1)

ip-address - Specifies the host IP address of a server.

Default Setting

None

Command Mode

Server Group Configuration

Command Usage

- ◆ When specifying the index for a RADIUS server, that server index must already be defined by the [radius-server host](#) command.
- ◆ When specifying the index for a TACACS+ server, that server index must already be defined by the [tacacs-server host](#) command.

Example

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

accounting dot1x This command applies an accounting method for 802.1X service requests on an interface. Use the **no** form to disable accounting on the interface.

Syntax

accounting dot1x {**default** | *list-name*}

no accounting dot1x

default - Specifies the default method list created with the [aaa accounting dot1x](#) command.

list-name - Specifies a method list created with the [aaa accounting dot1x](#) command.

Default Setting

None

Command Mode

Interface Configuration

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#accounting dot1x tps
Console(config-if)#
```

accounting commands This command applies an accounting method to entered CLI commands. Use the **no** form to disable accounting for entered CLI commands.

Syntax

accounting commands *level* {**default** | *list-name*}

no accounting commands *level*

level - The privilege level for executing commands. (Range: 0-15)

default - Specifies the default method list created with the [aaa accounting commands](#) command.

list-name - Specifies a method list created with the [aaa accounting commands](#) command.

Default Setting

None

Command Mode

Line Configuration

Example

```
Console(config)#line console
Console(config-line)#accounting commands 15 default
Console(config-line)#
```

accounting exec This command applies an accounting method to local console, Telnet or SSH connections. Use the **no** form to disable accounting on the line.

Syntax

accounting exec {**default** | *list-name*}

no accounting exec

default - Specifies the default method list created with the [aaa accounting exec](#) command.

list-name - Specifies a method list created with the [aaa accounting exec](#) command.

Default Setting

None

Command Mode

Line Configuration

Example

```
Console(config)#line console
Console(config-line)#accounting exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#accounting exec default
Console(config-line)#
```

authorization commands This command applies an authorization method to entered CLI commands. Use the **no** form to disable authorization for entered CLI commands.

Syntax

authorization commands *level* {**default** | *list-name*}

no authorization commands *level*

level - The privilege level for executing commands. (Range: 0-15)

default - Specifies the default method list created with the [aaa authorization commands](#) command.

list-name - Specifies a method list created with the [aaa authorization commands](#) command.

Default Setting

None

Command Mode

Line Configuration

Example

```
Console(config)#line console
Console(config-line)#authorization commands 15 default
Console(config-line)#
```

authorization exec This command applies an authorization method to local console, Telnet or SSH connections. Use the **no** form to disable authorization on the line.

Syntax

authorization exec {**default** | *list-name*}

no authorization exec

default - Specifies the default method list created with the **aaa authorization exec** command.

list-name - Specifies a method list created with the **aaa authorization exec** command.

Default Setting

None

Command Mode

Line Configuration

Example

```
Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization exec default
Console(config-line)#
```

show accounting This command displays the current accounting settings per function and per port.

Syntax

show accounting [**commands** [*level*]] |
[[**dot1x** [**statistics** [**username** *user-name* | **interface** *interface*]] |
exec [**statistics**] | **statistics**]

commands - Displays command accounting information.

level - Displays command accounting information for a specifiable command level.

dot1x - Displays dot1x accounting information.

exec - Displays Exec accounting records.

statistics - Displays accounting records.

user-name - Displays accounting records for a specifiable username.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

Default Setting

None

Command Mode

Privileged Exec

Example

```

Console#show accounting
Accounting Type : dot1x
  Method List   : default
  Group List    : radius
  Interface     : Eth 1/1

  Method List   : tps
  Group List    : radius
  Interface     : Eth 1/2

Accounting Type : EXEC
  Method List   : default
  Group List    : tacacs+
  Interface     : vty

Accounting Type : Commands 0
  Method List   : default
  Group List    : tacacs+
  Interface     :
  :
Accounting Type : Commands 15
  Method List   : default
  Group List    : tacacs+
  Interface     :

Console#

```

show authorization This command displays the current authorization settings per function and per port.

Syntax

show authorization [**commands** [*level*] | **exec**]

commands - Displays command authorization information.

level - Displays command authorization information for a specifiable command level.

exec - Displays Exec authorization records.

Default Setting

None

Command Mode

Privileged Exec

Example

```

Console#show authorization
Authorization Type : EXEC
  Method List      : default
  Group List       : tacacs+
  Interface        : vty

Authorization Type : Commands 0
  Method List      : default
  Group List       : tacacs+
  Interface        :
  :
Authorization Type : Commands 15
  Method List      : default
  Group List       : tacacs+
  Interface        :

Console#

```

Web Server

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

Table 73: Web Server Commands

Command	Function	Mode
ip http authentication	Sets the method list for EXEC authorization of an EXEC session	GC
ip http port	Specifies the port to be used by the web browser interface	GC
ip http server	Allows the switch to be monitored or configured from a browser	GC
ip http secure-port	Specifies the TCP port number for HTTPS	GC
ip http secure-server	Enables HTTPS (HTTP/SSL) for encrypted communications	GC
show authorization	Displays all authorization information	PE
show system	Displays system information	NE, PE



Note: Users are automatically logged off of the HTTP server or HTTPS server if no input is detected for 300 seconds.

ip http authentication This command specifies the method list for EXEC authorization for starting an EXEC session used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http authentication aaa exec-authorization {default | *list-name*}

no ip http authentication aaa exec-authorization

default - Specifies the default method list used for authorization requests.

list-name - Specifies a method list created with the [aaa authorization commands](#) command.

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#ip http authentication aaa exec-authorization default
Console(config)#
```

Related Commands

[aaa authorization commands \(642\)](#)

[ip http server \(652\)](#)

[show system \(535\)](#)

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 \(652\)](#)

[show system \(535\)](#)

ip http server This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

[no] ip http server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server  
Console(config)#
```

Related Commands

[ip http authentication \(651\)](#)

[show system \(535\)](#)

ip http secure-port This command specifies the TCP port number used for HTTPS connection to the switch's web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*

no ip http secure-port

port_number – The TCP port used for HTTPS. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- ◆ You cannot configure the HTTP and HTTPS servers to use the same port.
- ◆ If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://device:port_number**

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

[ip http secure-server \(653\)](#)

[show system \(535\)](#)

ip http secure-server This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

Syntax

[no] ip http secure-server

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- ◆ Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.
- ◆ If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https://device[:port_number]**
- ◆ When you start HTTPS, the connection is established in this way:
 - The client authenticates the server using the server's digital certificate.
 - The client and server negotiate a set of security protocols to use for the connection.
 - The client and server generate session keys for encrypting and decrypting data.

- ◆ The client and server establish a secure encrypted connection.

A padlock icon should appear in the status bar for Internet Explorer 11, Mozilla Firefox 40, or Google Chrome 45, or more recent versions.

The following web browsers and operating systems currently support HTTPS:

Table 74: HTTPS System Support

Web Browser	Operating System
Internet Explorer 11 or later	Windows 7, 8, 10
Mozilla Firefox 40 or later	Windows 7, 8, 10, Linux
Google Chrome 45 or later	Windows 7, 8, 10

- ◆ To specify a secure-site certificate, see [“Replacing the Default Secure-site Certificate.”](#) Also refer to the [copy tftp https-certificate](#) command.
- ◆ Connection to the web interface is not supported for HTTPS using an IPv6 link local address.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

[ip http secure-port \(652\)](#)
[copy tftp https-certificate \(542\)](#)
[show system \(535\)](#)

Telnet Server

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

Table 75: Telnet Server Commands

Command	Function	Mode
ip telnet max-sessions	Specifies the maximum number of Telnet sessions that can simultaneously connect to this system	GC
ip telnet port	Specifies the port to be used by the Telnet interface	GC
ip telnet server	Allows the switch to be monitored or configured from Telnet	GC
telnet (client)	Accesses a remote device using a Telnet connection	PE
show ip telnet	Displays configuration settings for the Telnet server	PE



Note: This switch also supports a Telnet client function. A Telnet connection can be made from this switch to another device by entering the **telnet** command at the Privileged Exec configuration level.

ip telnet max-sessions This command specifies the maximum number of Telnet sessions that can simultaneously connect to this system. Use the **no** form to restore the default setting.

Syntax

ip telnet max-sessions *session-count*

no ip telnet max-sessions

session-count - The maximum number of allowed Telnet session.
(Range: 0-8)

Default Setting

8 sessions

Command Mode

Global Configuration

Command Usage

A maximum of eight sessions can be concurrently opened for Telnet and Secure Shell (i.e., both Telnet and SSH share a maximum number of eight sessions).

Example

```
Console(config)#ip telnet max-sessions 1
Console(config)#
```

ip telnet port This command specifies the TCP port number used by the Telnet interface. Use the **no** form to use the default port.

Syntax

ip telnet port *port-number*

no telnet port

port-number - The TCP port number to be used by the browser interface.
(Range: 1-65535)

Default Setting

23

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet port 123
Console(config)#
```

ip telnet server This command allows this device to be monitored or configured from Telnet. Use the **no** form to disable this function.

Syntax

[no] ip telnet server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet server
Console(config)#
```

telnet (client) This command accesses a remote device using a Telnet connection.

Syntax

telnet *host*

host - IP address or alias of a remote device.

Command Mode

Privileged Exec

Example

```
Console#telnet 192.168.2.254
Connect To 192.168.2.254...

*****

WARNING - MONITORED ACTIONS AND ACCESSES

User Access Verification

Username:

Console(config)#
```

show ip telnet This command displays the configuration settings for the Telnet server.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip telnet
IP Telnet Configuration:

Telnet Status: Enabled
Telnet Service Port: 23
Telnet Max Session: 8
Console#
```

Secure Shell

This section describes the commands used to configure the SSH server. Note that you also need to install a SSH client on the management station when using this protocol to configure the switch.



Note: The switch supports both SSH Version 1.5 and 2.0 clients.

Table 76: 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
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC
copy tftp public-key	Copies the user's public key from a TFTP server to the switch	PE
delete public-key	Deletes the public key for the specified user	PE
disconnect	Terminates a line connection	PE
ip ssh crypto host-key generate	Generates the host key	PE
ip ssh crypto zeroize	Clear the host key from RAM	PE
ip ssh save host-key	Saves the host key from RAM to flash memory	PE
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE
show public-key	Shows the public key for the specified user or for the host	PE

Table 76: Secure Shell Commands (Continued)

Command	Function	Mode
<code>show ssh</code>	Displays the status of current SSH sessions	PE
<code>show users</code>	Shows SSH users, including privilege level and public key type	PE

Configuration Guidelines

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the `authentication login` command. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the `ip ssh crypto host-key generate` command to create a host public/private key pair.
2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

```
10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
15020245593199868544358361651999923329781766065830956
108259132128902337654680172627257141342876294130119619556678259566410486957427
888146206519417467729848654686157177393901647793559423035774130980227370877945
4524083971752646358058176716709574804776117
```

3. Import Client's Public Key to the Switch – Use the `copy tftp public-key` command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the `username` command.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

```
1024 35
134108168560989392104094492015542534763164192187295892114317388005553616163105
177594083868631109291232226828519254374603100937187721199696317813662774141689
851320491172048303392543241016379975923714490119380060902539484084827178194372
288402533115952134861022902978982721353267131629432532818915045306393916643
steve@192.168.1.19
```

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.
5. Enable SSH Service – Use the `ip ssh server` command to enable the SSH server on the switch.
6. *Authentication* – One of the following authentication methods is employed:

Password Authentication (for SSH v1.5 or V2 Clients)

- a. The client sends its password to the server.
- b. The switch compares the client's password to those stored in memory.
- c. If a match is found, the connection is allowed.



Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

Authenticating SSH v1.5 Clients

- a. The client sends its RSA public key to the switch.
- b. The switch compares the client's public key to those stored in memory.
- c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user's public key, and sends it to the client.
- d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.
- e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

- a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.
- b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.
- c. The client sends a signature generated using the private key to the switch.

- d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.



Note: The SSH server supports up to eight client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

Note: The SSH server can be accessed using any configured IPv4 or IPv6 interface address on the switch.

ip ssh authentication-retries This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

ip ssh authentication-retries *count*

no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retries 2
Console(config)#
```

Related Commands

[show ip ssh \(665\)](#)

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 \(663\)](#)

[show ssh \(666\)](#)

ip ssh server-key size This command sets the SSH server key size. Use the **no** form to restore the default setting.

Syntax

ip ssh server-key size *key-size*

no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

Default Setting

768 bits

Command Mode

Global Configuration

Command Usage

The server key is a private key that is never shared outside the switch.
The host key is shared with the SSH client, and is fixed at 1024 bits.

Example

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

ip ssh timeout This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout *seconds*

no ip ssh timeout

seconds – The timeout for client response during SSH negotiation.
(Range: 1-120)

Default Setting

120 seconds

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the [exec-timeout](#) command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

[exec-timeout \(554\)](#)

[show ip ssh \(665\)](#)

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 \(664\)](#)

[ip ssh save host-key \(664\)](#)

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 \(663\)](#)

[ip ssh save host-key \(664\)](#)

[no ip ssh server \(660\)](#)

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 \(663\)](#)

show ip ssh This command displays the connection settings used when authenticating client access to the SSH server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
SSH Enabled - Version 2.0
Negotiation Timeout : 120 seconds; Authentication Retries : 3
Server Key Size      : 768 bits
Console#
```

show public-key This command shows the public key for the specified user or for the host.

Syntax

show public-key [user [username]] host]

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

Default Setting

Shows all public keys.

Command Mode

Privileged Exec

Command Usage

- ◆ If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- ◆ When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

```
Console#show public-key host
Host:
RSA:
DSA:
Console#
```

show ssh This command displays the current SSH server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Connection Version State Username Encryption
1 2.0 Session-Started admin ctos aes128-cbc-hmac-md5
stoc aes128-cbc-hmac-md5
Console#
```

Table 77: show ssh - display description

Field	Description
Connection	The session number. (Range: 1-8)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.

802.1X Port Authentication

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Table 78: 802.1X Port Authentication Commands

Command	Function	Mode
<i>General Commands</i>		
dot1x default	Resets all dot1x parameters to their default values	GC
dot1x system-auth-control	Enables dot1x globally on the switch.	GC
<i>Authenticator Commands</i>		
dot1x intrusion-action	Sets the port response to intrusion when authentication fails	IC
dot1x max-reauth-req	Sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process	IC
dot1x max-req	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
dot1x operation-mode	Allows single or multiple hosts on an dot1x port	IC

Table 78: 802.1X Port Authentication Commands (Continued)

Command	Function	Mode
<code>dot1x port-control</code>	Sets dot1x mode for a port interface	IC
<code>dot1x re-authentication</code>	Enables re-authentication for all ports	IC
<code>dot1x timeout quiet-period</code>	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	IC
<code>dot1x timeout re-authperiod</code>	Sets the time period after which a connected client must be re-authenticated	IC
<code>dot1x timeout supp-timeout</code>	Sets the interval for a supplicant to respond	IC
<code>dot1x timeout tx-period</code>	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	IC
<code>dot1x re-authenticate</code>	Forces re-authentication on specific ports	PE
<i>Supplicant Commands</i>		
<code>dot1x 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 authenticator global and port settings to their default values.

Command Mode

Global Configuration

Command Usage

This command resets the following commands to their default settings:

- ◆ `dot1x system-auth-control`
- ◆ `dot1x eapol-pass-through`
- ◆ `dot1x port-control`
- ◆ `dot1x port-control multi-host max-count`
- ◆ `dot1x operation-mode`

- ◆ dot1x max-req
- ◆ dot1x timeout quiet-period
- ◆ dot1x timeout tx-period
- ◆ dot1x timeout re-authperiod
- ◆ dot1x timeout sup-timeout
- ◆ dot1x re-authentication
- ◆ dot1x intrusion-action

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x system-auth-control This command enables IEEE 802.1X port authentication globally on the switch. Use the **no** form to restore the default.

Syntax

[no] dot1x system-auth-control

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dot1x system-auth-control
Console(config)#
```

Authenticator Commands

dot1x intrusion-action This command sets the port's response to a failed authentication, either to block all traffic, or to assign all traffic for the port to a guest VLAN. Use the **no** form to reset the default.

Syntax

dot1x intrusion-action {block-traffic | guest-vlan}

no dot1x intrusion-action

block-traffic - Blocks traffic on this port.

guest-vlan - Assigns the user to the Guest VLAN.

Default

block-traffic

Command Mode

Interface Configuration

Command Usage

- ◆ For guest VLAN assignment to be successful, the VLAN must be configured and set as active (see the [vlan database](#) command) and assigned as the guest VLAN for the port (see the [network-access guest-vlan](#) command).
- ◆ A port can only be assigned to the guest VLAN in case of failed authentication, if [switchport mode](#) is set to Hybrid.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x intrusion-action guest-vlan
Console(config-if)#
```

dot1x max-reauth-req This command sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. Use the **no** form to restore the default.

Syntax

dot1x max-reauth-req *count*

no dot1x max-reauth-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-reauth-req 2
Console(config-if)#
```

dot1x max-req This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*

no dot1x max-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

dot1x operation-mode This command allows hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

Syntax

dot1x operation-mode {**single-host** | **multi-host** [**max-count** *count*] | **mac-based-auth**}

no dot1x operation-mode [**multi-host max-count**]

single-host – Allows only a single host to connect to this port.

multi-host – Allows multiple host to connect to this port.

max-count – Keyword for the maximum number of hosts.

count – The maximum number of hosts that can connect to a port.
(Range: 1-1024; Default: 5)

mac-based – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

Default

Single-host

Command Mode

Interface Configuration

Command Usage

- ◆ The “max-count” parameter specified by this command is only effective if the dot1x mode is set to “auto” by the `dot1x port-control` command.
- ◆ In “multi-host” mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
- ◆ In “mac-based-auth” mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x port-control This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

auto – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.

force-authorized – Configures the port to grant access to all clients, either dot1x-aware or otherwise.

force-unauthorized – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x re-authentication This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

Syntax

[no] **dot1x re-authentication**

Command Mode

Interface Configuration

Command Usage

- ◆ The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.
- ◆ The connected client is re-authenticated after the interval specified by the **dot1x timeout re-authperiod** command. The default is 3600 seconds.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

Related Commands

dot1x timeout re-authperiod (673)

dot1x timeout quiet-period This command sets the time that a switch port waits after the maximum request count (see [page 670](#)) 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)

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).

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) 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), 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)

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 668](#)).
- ◆ *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 670](#)).
 - Control Mode – Dot1x port control mode ([page 671](#)).
 - 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 672](#)).
 - Reauth Period – Time after which a connected client must be re-authenticated ([page 673](#)).
 - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client ([page 672](#)).
 - TX Period – Time a port waits during authentication session before re-transmitting EAP packet ([page 674](#)).
 - 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 670](#)).
 - 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 671](#)).
 - Intrusion Action– Shows the port response to intrusion when authentication fails ([page 668](#)).
 - Supplicant– MAC address of authorized client.
- ◆ *Authenticator PAE State Machine*
 - State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
 - Reauth Count– Number of times connecting state is re-entered.
 - Current Identifier– The integer (0-255) used by the Authenticator to identify the current authentication session.

◆ *Backend State Machine*

- State – Current state (including request, response, success, fail, timeout, idle, initialize).
- Request Count– Number of EAP Request packets sent to the Supplicant without receiving a response.
- Identifier (Server)– Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

◆ *Reauthentication State Machine*

State – Current state (including initialize, reauthenticate).

Example

```

Console#show dot1x
Global 802.1X Parameters
  System Auth Control      : Enabled

Authenticator Parameters:
  EAPOL Pass Through      : Disabled

802.1X Port Summary

Port      Type      Operation Mode Control Mode      Authorized
-----
Eth 1/ 1 Disabled    Single-Host    Force-Authorized  Yes
Eth 1/ 2 Disabled    Single-Host    Force-Authorized  Yes
'''
Eth 1/27 Disabled    Single-Host    Force-Authorized  Yes
Eth 1/28 Enabled     Single-Host    Auto              Yes

Console#show dot1x interface ethernet 1/2

802.1X Authenticator is enabled on port 2
Reauthentication      : Enabled
Reauth Period         : 3600
Quiet Period          : 60
TX Period             : 30
Supplicant Timeout    : 30
Server Timeout        : 10
Reauth Max Retries    : 2
Max Request           : 2
Operation Mode        : Multi-host
Port Control          : Auto
Intrusion Action      : Block traffic

Supplicant            : 00-e0-29-94-34-65

Authenticator PAE State Machine
State                 : Authenticated
Reauth Count          : 0
Current Identifier    : 3

Backend State Machine
State                 : Idle
Request Count         : 0
Identifier(Server)    : 2

Reauthentication State Machine
State                 : Initialize
Console#

```

Management IP Filter

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

Table 79: Management IP Filter Commands

Command	Function	Mode
<code>management</code>	Configures IP addresses that are allowed management access	GC
<code>show management</code>	Displays the switch to be monitored or configured from a browser	PE

management This command specifies the client IP addresses that are allowed management access to the switch through various protocols. A list of up to 15 IP addresses or IP address groups can be specified. Use the **no** form to restore the default setting.

Syntax

[no] management {all-client | http-client | snmp-client | telnet-client}
start-address [end-address]

all-client - Adds IP address(es) to all groups.

http-client - Adds IP address(es) to the web group.

snmp-client - Adds IP address(es) to the SNMP group.

telnet-client - Adds IP address(es) to the Telnet group.

start-address - A single IP address, or the starting address of a range.

end-address - The end address of a range.

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- ◆ The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- ◆ If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.

- ◆ IP address can be configured for SNMP, web, and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- ◆ When entering addresses for the same group (i.e., SNMP, web, or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- ◆ You cannot delete an individual address from a specified range. You must delete the entire range, and re-enter the addresses.
- ◆ You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {all-client | http-client | snmp-client | telnet-client}

all-client - Displays IP addresses for all groups.

http-client - Displays IP addresses for the web group.

snmp-client - Displays IP addresses for the SNMP group.

telnet-client - Displays IP addresses for the Telnet group.

Command Mode

Privileged Exec

Example

```
Console#show management all-client
Management Ip Filter
  HTTP-Client:
    Start IP address      End IP address
    -----
  1. 192.168.1.19         192.168.1.19
  2. 192.168.1.25         192.168.1.30

  SNMP-Client:
    Start IP address      End IP address
    -----
  1. 192.168.1.19         192.168.1.19
  2. 192.168.1.25         192.168.1.30
```

```
TELNET-Client:
  Start IP address      End IP address
-----
1. 192.168.1.19         192.168.1.19
2. 192.168.1.25         192.168.1.30

Console#
```

General Security Measures

This switch supports many methods of segregating traffic for clients attached to each of the data ports, and for ensuring that only authorized clients gain access to the network. Port-based authentication using IEEE 802.1X is commonly used for these purposes. In addition to these method, several other options of providing client security are described in this chapter. These include port-based authentication, which can be configured to allow network client access by specifying a fixed set of MAC addresses. The addresses assigned to DHCP clients can also be carefully controlled with IP Source Guard and DHCP Snooping commands.

Table 80: 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
Access Control Lists*	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)
DHCPv4 Snooping*	Filters untrusted DHCPv4 messages on unsecure ports by building and maintaining a DHCPv4 snooping binding table
IPv4 Source Guard*	Filters IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping nor static source bindings
ARP Inspection	Validates the MAC-to-IP address bindings in ARP packets
DoS Protection	Protects against Denial-of-Service attacks
Port-based Traffic Segmentation	Configures traffic segmentation for different client sessions based on specified downlink and uplink ports

* The priority of execution for these filtering commands is Port Security, Port Authentication, Network Access, Access Control Lists, DHCP Snooping, and then IPv4 Source Guard.

Port Security

These commands can be used to enable port security on a port.

When MAC address learning is disabled on an interface, only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network.

When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Table 81: Management IP Filter Commands

Command	Function	Mode
<code>mac-address-table static</code>	Maps a static address to a port in a VLAN	GC
<code>mac-learning</code>	Enables MAC address learning on the selected physical interface or VLAN	IC
<code>port security</code>	Configures a secure port	IC
<code>show mac-address-table</code>	Displays entries in the bridge-forwarding database	PE
<code>show port security</code>	Displays port security status and secure address count	PE

mac-learning This command enables MAC address learning on the selected interface. Use the **no** form to disable MAC address learning.

Syntax

[no] mac-learning

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet or Port Channel)

Command Usage

- ◆ The **no mac-learning** command immediately stops the switch from learning new MAC addresses on the specified port or trunk. Incoming traffic with source addresses not stored in the static address table, will be flooded. However, if a security function such as 802.1X or DHCP snooping is enabled and mac-learning is disabled, then only incoming traffic with source addresses stored in

the static address table will be accepted, all other packets are dropped. Note that the dynamic addresses stored in the address table when MAC address learning is disabled are flushed from the system, and no dynamic addresses are subsequently learned until MAC address learning has been re-enabled.

- ◆ The mac-learning commands cannot be used if 802.1X Port Authentication has been globally enabled on the switch with the [dot1x system-auth-control](#) command, or if MAC Address Security has been enabled by the [port security](#) command on the same interface.

Example

The following example disables MAC address learning for port 2.

```
Console(config)#interface ethernet 1/2
Console(config-if)#no mac-learning
Console(config-if)#
```

Related Commands

[show interfaces status \(772\)](#)

port security This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**} | **max-mac-count** *address-count*]

no port security [**action** | **max-mac-count**]

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable port.

max-mac-count

address-count - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

Default Setting

Status: Disabled

Action: None

Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The default maximum number of MAC addresses allowed on a secure port is zero (that is, port security is disabled). To use port security, you must configure the maximum number of addresses allowed on a port using the **port security max-mac-count** command.
- ◆ When port security is enabled using the **port security** command, or the maximum number or allowed addresses is set to a value lower than the current limit after port security has been enabled, the switch first clears all dynamically learned entries from the address table. It then starts learning new MAC addresses on the specified port, and stops learning addresses when it reaches a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- ◆ To configure the maximum number of address entries which can be learned on a port, specify the maximum number of dynamic addresses allowed. The switch will learn up to the maximum number of allowed address pairs <source MAC address, VLAN> for frames received on the port. (The specified maximum address count is effective when port security is enabled or disabled.) Note that you can manually add additional secure addresses to a port using the **mac-address-table static** command. When the port has reached the maximum number of MAC addresses, the port will stop learning new addresses. The MAC addresses already in the address table will be retained and will not be aged out.
- ◆ If port security is enabled, and the maximum number of allowed addresses are set to a non-zero value, any device not in the address table that attempts to use the port will be prevented from accessing the switch.
- ◆ If a port is disabled due to a security violation, it must be manually re-enabled using the **no shutdown** command.
- ◆ A secure port has the following restrictions:
 - Cannot be connected to a network interconnection device.
 - Cannot be a trunk port.
 - RSPAN and port security are mutually exclusive functions. If port security is enabled on a port, that port cannot be set as an RSPAN uplink port. Also, when a port is configured as an RSPAN uplink port, source port, or destination port, port security cannot be enabled on that port.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

Related Commands

[show interfaces status \(772\)](#)

[shutdown \(764\)](#)

[mac-address-table static \(821\)](#)

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)

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 82: show port security - display description

Field	Description
Port Security	The configured status (enabled or 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.
Intrusion Action	The configured intrusion response.

Table 82: show port security - display description (Continued)

Field	Description
MaxMacCnt	The maximum number of addresses which can be stored in the address table for this interface (either dynamic or static).
CurrMacCnt	The current number of secure entries in the address table.

The following example shows the port security settings and number of secure addresses for a specific port. The Last Intrusion MAC and Last Time Detected Intrusion MAC fields show information about the last detected intrusion MAC address. These fields are not applicable if no intrusion has been detected or port security is disabled. The MAC Filter ID field is configured by the [network-access mac-filter](#) command. If this field displays Disabled, then any unknown source MAC address can be learned as a secure MAC address. If it displays a filter identifier, then only source MAC address entries in MAC Filter table can be learned as secure MAC addresses.

```

Console#show port security interface ethernet 1/2
Global Port Security Parameters
  Secure MAC Aging Mode : Disabled

Port Security Details
  Port                  : 1/2
  Port Security         : Enabled
  Port Status           : Secure/Up
  Intrusion Action       : None
  Max MAC Count         : 0
  Current MAC Count     : 0
  MAC Filter            : Disabled
  Last Intrusion MAC     : NA
  Last Time Detected Intrusion MAC : NA
Console#

```

This example shows information about a detected intrusion.

```

Console#show port security interface ethernet 1/2
Global Port Security Parameters
  Secure MAC Aging Mode : Disabled

Port Security Details
  Port                  : 1/2
  Port Security         : Enabled
  Port Status           : Secure/Up
  Intrusion Action       : None
  Max MAC Count         : 0
  Current MAC Count     : 0
  MAC Filter            : Disabled
  Last Intrusion MAC     : 00-10-22-00-00-01
  Last Time Detected Intrusion MAC : 2015/7/29 15:13:03
Console#

```

Network Access (MAC Address Authentication)

Network Access authentication controls access to the network by authenticating the MAC address of each host that attempts to connect to a switch port. Traffic received from a specific MAC address is forwarded by the switch only if the source MAC address is successfully authenticated by a central RADIUS server. While authentication for a MAC address is in progress, all traffic is blocked until authentication is completed. Once successfully authenticated, the RADIUS server may optionally assign VLAN and QoS settings for the switch port.

Table 83: 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>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>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 670](#)).
- ◆ The maximum number of secure MAC addresses supported for the switch system is 1024.

Example

```
Console(config)#network-access aging
Console(config)#
```

network-access mac-filter Use this command to add a MAC address into a filter table. Use the **no** form of this command to remove the specified MAC address.

Syntax

[no] network-access mac-filter *filter-id*
mac-address *mac-address* [**mask** *mask-address*]

filter-id - Specifies a MAC address filter table. (Range: 1-64)

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

mask - Specifies a MAC address bit mask for a range of addresses.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Specified addresses are exempt from network access authentication.
- ◆ This command is different from configuring static addresses with the [mac-address-table static](#) command in that it allows you configure a range of addresses when using a mask, and then to assign these addresses to one or more ports with the [network-access mac-filter](#) command.
- ◆ Up to 64 filter tables can be defined.
- ◆ There is no limitation on the number of entries that can entered in a filter table.

Example

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66
Console(config)#
```

network-access Use this command to enable dynamic VLAN assignment for an authenticated port.
dynamic-vlan Use the **no** form to disable dynamic VLAN assignment.

Syntax

[no] **network-access dynamic-vlan**

Default Setting

Enabled

Command Mode

Interface Configuration

Command Usage

- ◆ When enabled, the VLAN identifiers returned by the RADIUS server through the 802.1X authentication process will be applied to the port, providing the VLANs have already been created on the switch.
- ◆ The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have same VLAN configuration, or they are treated as an authentication failure.
- ◆ If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host assigned to the default untagged VLAN.
- ◆ When the dynamic VLAN assignment status is changed on a port, all authenticated addresses are cleared from the secure MAC address table.

Example

The following example enables dynamic VLAN assignment on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```


network-access guest-vlan Use this command to assign all traffic on a port to a guest VLAN when 802.1x authentication or MAC authentication is rejected. Use the **no** form of this command to disable guest VLAN assignment.

Syntax

network-access guest-vlan *vlan-id*

no network-access guest-vlan

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

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ The VLAN to be used as the guest VLAN must be defined and set as active (See the [vlan database](#) command).
- ◆ When used with 802.1X authentication, the intrusion-action must be set for "guest-vlan" to be effective (see the [dot1x intrusion-action](#) command).
- ◆ A port can only be assigned to the guest VLAN in case of failed authentication, if [switchport mode](#) is set to Hybrid.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

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)

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)

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
MAC Address Aging                : Disabled

Port : 1/1
Dynamic VLAN Assignment          : Enabled
MAC Filter ID                   : Disabled
Guest VLAN                      : Disabled
Console#
```

show network-access mac-address-table Use this command to display secure MAC address table entries.

Syntax

show network-access mac-address-table [**static** | **dynamic**]
[**address** *mac-address* [*mask*]] [**interface** *interface*] [**sort** {**address** |
interface}]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

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

mask - Specifies a MAC address bit mask for filtering displayed addresses.

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

sort - Sorts displayed entries by either MAC address or interface.

Default Setting

Displays all filters.

Command Mode

Privileged Exec

Command Usage

When using a bit mask to filter displayed MAC addresses, a 1 means “care” and a 0 means “don't care”. For example, a MAC of 00-00-01-02-03-04 and mask FF-FF-FF-00-00-00 would result in all MACs in the range 00-00-01-00-00-00 to 00-00-01-FF-FF-FF to be displayed. All other MACs would be filtered out.

Example

```
Console#show network-access mac-address-table
Interface MAC Address      RADIUS Server  Time                Attribute
-----
1/1        00-00-01-02-03-04  172.155.120.17  00d06h32m50s       Static
1/1        00-00-01-02-03-05  172.155.120.17  00d06h33m20s       Dynamic
1/1        00-00-01-02-03-06  172.155.120.17  00d06h35m10s       Static
1/3        00-00-01-02-03-07  172.155.120.17  00d06h34m20s       Dynamic

Console#
```

show network-access mac-filter Use this command to display information for entries in the MAC filter tables.

Syntax

show network-access mac-filter *[filter-id]*

filter-id - Specifies a MAC address filter table. (Range: 1-64)

Default Setting

Displays all filters.

Command Mode

Privileged Exec

Example

```
Console#show network-access mac-filter
Filter ID MAC Address      MAC Mask
-----
1 00-00-01-02-03-08 FF-FF-FF-FF-FF-FF
Console#
```

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 84: DHCP Snooping Commands

Command	Function	Mode
<code>ip dhcp snooping</code>	Enables DHCP snooping globally	GC
<code>ip dhcp snooping information option</code>	Enables or disables the use of DHCP Option 82 information, and specifies frame format for the remote-id	GC
<code>ip dhcp snooping information option encode no-subtype</code>	Disables use of sub-type and sub-length for the CID/RID in Option 82 information	GC
<code>ip dhcp snooping information policy</code>	Sets the information option policy for DHCP client packets that include Option 82 information	GC
<code>ip dhcp snooping verify mac-address</code>	Verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header	GC
<code>ip dhcp snooping vlan</code>	Enables DHCP snooping on the specified VLAN	GC
<code>ip dhcp snooping information option circuit-id</code>	Enables or disables the use of DHCP Option 82 information circuit-id suboption	IC
<code>ip dhcp snooping max-number</code>	configures the maximum number of DHCP clients which can be supported per interface	IC
<code>ip dhcp snooping trust</code>	Configures the specified interface as trusted	IC

Table 84: DHCP Snooping Commands (Continued)

Command	Function	Mode
<code>clear ip dhcp snooping binding</code>	Clears DHCP snooping binding table entries from RAM	PE
<code>clear ip dhcp snooping database flash</code>	Removes all dynamically learned snooping entries from flash memory.	PE
<code>ip dhcp snooping database flash</code>	Writes all dynamically learned snooping entries to flash memory	PE
<code>show ip dhcp snooping</code>	Shows the DHCP snooping configuration settings	PE
<code>show ip dhcp snooping binding</code>	Shows the DHCP snooping binding table entries	PE

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

Syntax

[no] ip dhcp snooping

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or fire wall. When DHCP snooping is enabled globally by this command, and enabled on a VLAN interface by the `ip dhcp snooping vlan` command, DHCP messages received on an untrusted interface (as specified by the `no ip dhcp snooping trust` command) from a device not listed in the DHCP snooping table will be dropped.
- ◆ When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- ◆ Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- ◆ When DHCP snooping is enabled, the rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.

- ◆ Filtering rules are implemented as follows:
 - If global DHCP snooping is disabled, all DHCP packets are forwarded.
 - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.
 - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:
 - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
 - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
 - If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled (as specified by the [ip dhcp snooping verify mac-address](#) command). However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
 - If the DHCP packet is not a recognizable type, it is dropped.
 - If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
 - If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- ◆ If DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.
- ◆ *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted (using the [ip dhcp snooping trust](#) command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

Example

This example enables DHCP snooping globally for the switch.

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

Related Commands

[ip dhcp snooping vlan \(703\)](#)

[ip dhcp snooping trust \(706\)](#)

ip dhcp snooping information option

This command enables the use of DHCP Option 82 information for the switch, and specifies the frame format to use for the remote-id when Option 82 information is generated by the switch. Use the **no** form without any keywords to disable this function, the **no** form with the **encode no-subtype** keyword to enable use of sub-type and sub-length in CID/RID fields, or the **no** form with the **remote-id** keyword to set the remote ID to the switch's MAC address encoded in hexadecimal.

Syntax

ip dhcp snooping information option

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

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

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

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

mac-address - Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (that is, the MAC address of the switch's CPU).

ip-address - Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (that is, the IP address of the management interface).

encode - Indicates encoding in ASCII or hexadecimal.

string - An arbitrary string inserted into the remote identifier field.
(Range: 1-32 characters)

Default Setting

Option 82: Disabled

CID/RID sub-type: Enabled

Remote ID: MAC address (hexadecimal)

Command Mode

Global Configuration

Command Usage

- ◆ DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. Known as DHCP Option 82, it allows

compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients.

- ◆ When the DHCP Snooping Information Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server.
- ◆ When the DHCP Snooping Information Option is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCP client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.
- ◆ DHCP snooping must be enabled for the DHCP Option 82 information to be inserted into packets. When enabled, the switch will only add/remove option 82 information in incoming DHCP packets but not relay them. Packets are processed as follows:
 - If an incoming packet is a DHCP request packet with option 82 information, it will modify the option 82 information according to settings specified with [ip dhcp snooping information policy](#) command.
 - If an incoming packet is a DHCP request packet without option 82 information, enabling the DHCP snooping information option will add option 82 information to the packet.
 - If an incoming packet is a DHCP reply packet with option 82 information, enabling the DHCP snooping information option will remove option 82 information from the packet.

Example

This example enables the DHCP Snooping Information Option.

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

ip dhcp snooping information option encode no-subtype

This command disables the use of sub-type and sub-length fields for the circuit-ID (CID) and remote-ID (RID) in Option 82 information generated by the switch. Use the **no** form to enable the use of these fields.

Syntax

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

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- ◆ Option 82 information generated by the switch is based on TR-101 syntax as shown below:

Table 85: Option 82 information

82	3-69	1	1-67	x1	x2	x3	x4	x5	x63
opt82	opt-len	sub-opt1	string-len	R-124 string					

The circuit identifier used by this switch starts at sub-option1 and goes to the end of the R-124 string. The R-124 string includes the following information:

- sub-type - Distinguishes different types of circuit IDs.
- sub-length - Length of the circuit ID type
- access node identifier - ASCII string. Default is the MAC address of the switch's CPU. This field is set by the [ip dhcp snooping information option](#) command,
- eth - The second field is the fixed string "eth"
- slot - The slot represents the stack unit for this system.
- port - The port which received the DHCP request. If the packet arrives over a trunk, the value is the ifIndex of the trunk.
- vlan - Tag of the VLAN which received the DHCP request.

Note that the sub-type and sub-length fields can be enabled or disabled using the [ip dhcp snooping information option](#) command.

- The **ip dhcp snooping information option circuit-id** command can be used to modify the default settings described above.
- ◆ The format for TR101 option 82 is: "<IP> eth <SID>/<PORT>[:<VLAN>]". Note that the SID (Switch ID) is always 0. By default the PVID is added to the end of the TR101 field for untagged packets. For tagged packets, the VLAN ID is always added.

EXAMPLE

This example enables the use of sub-type and sub-length fields for the circuit-ID (CID) and remote-ID (RID).

```
Console(config)#no ip dhcp snooping information option encode no-subtype
Console(config)#
```

ip dhcp snooping information policy This command sets the DHCP snooping information option policy for DHCP client packets that include Option 82 information.

Syntax

ip dhcp snooping information policy {drop | keep | replace}

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

keep - Retains the Option 82 information in the client request, and forwards the packets to trusted ports.

replace - Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports.

Default Setting

replace

Command Mode

Global Configuration

Command Usage

When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

Example

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

ip dhcp snooping verify mac-address This command verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. Use the **no** form to disable this function.

Syntax

[no] ip dhcp snooping verify mac-address

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped.

Example

This example enables MAC address verification.

```
Console(config)#ip dhcp snooping verify mac-address  
Console(config)#
```

Related Commands

[ip dhcp snooping \(697\)](#)

[ip dhcp snooping vlan \(703\)](#)

[ip dhcp snooping trust \(706\)](#)

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

Syntax

[no] ip dhcp snooping vlan *vlan-id*

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

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

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

Example

This example enables DHCP snooping for VLAN 1.

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

Related Commands

[ip dhcp snooping \(697\)](#)

[ip dhcp snooping trust \(706\)](#)

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 86: 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 4500
Console(config-if)#
```

ip dhcp snooping max-number This command configures the maximum number of DHCP clients which can be supported per interface. Use the **no** form to restore the default setting.

Syntax

ip dhcp snooping max-number *max-number*

no dhcp snooping max-number

max-number - Maximum number of DHCP clients. (Range: 1-32)

Default Setting

16

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example sets the maximum number of DHCP clients supported on port 1 to 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip dhcp snooping max-number 2
Console(config-if)#
```

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

Syntax

[no] **ip dhcp snooping trust**

Default Setting

All interfaces are untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.
- ◆ Set all ports connected to DHCP servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.
- ◆ When DHCP snooping is enabled globally using the [ip dhcp snooping](#) command, and enabled on a VLAN with [ip dhcp snooping vlan](#) command, DHCP packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the **no ip dhcp snooping trust** command.
- ◆ When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- ◆ *Additional considerations when the switch itself is a DHCP client* – The port(s) through which it submits a client request to the DHCP server must be configured as trusted.

Example

This example sets port 5 to untrusted.

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

Related Commands

[ip dhcp snooping \(697\)](#)

[ip dhcp snooping vlan \(703\)](#)

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: 1-4094)

Command Mode

Privileged Exec

Example

```
Console#clear ip dhcp snooping binding 11-22-33-44-55-66 vlan 1
Console#
```

clear ip dhcp snooping database flash This command removes all dynamically learned snooping entries from flash memory.

Command Mode

Privileged Exec

Example

```
Console#clear ip dhcp snooping database flash
Console#
```

ip dhcp snooping database flash This command writes all dynamically learned snooping entries to flash memory.

Command Mode

Privileged Exec

Command Usage

This command can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

Example

```
Console#ip dhcp snooping database flash
Console#
```

show ip dhcp snooping This command shows the DHCP snooping configuration settings.

Command Mode
Privileged Exec

Example

```
Console#show ip dhcp snooping
Global DHCP Snooping Status: disabled
DHCP Snooping Information Option Status: disabled
DHCP Snooping Information Option Sub-option Format: extra subtype included
DHCP Snooping Information Option Remote ID: MAC Address (hex encoded)
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:

Verify Source MAC-Address: enabled
Interface   Trusted   Max-Number   Circuit-ID mode   Circuit-ID Value
-----
Eth 1/1     No        16           VLAN-Unit-Port   ---
Eth 1/2     No        16           VLAN-Unit-Port   ---
Eth 1/3     No        16           VLAN-Unit-Port   ---
Eth 1/4     No        16           VLAN-Unit-Port   ---
Eth 1/5     No        16           VLAN-Unit-Port   ---
.
.
.
```

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-DHCPSP 1     Eth 1/5
Console#
```


IPv4 Source Guard

IPv4 Source Guard is a security feature that filters IPv4 traffic on network interfaces based on manually configured entries in the IPv4 Source Guard table, or dynamic entries in the DHCPv4 Snooping table when enabled (see [“DHCPv4 Snooping” on page 696](#)). IPv4 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv4 address of a neighbor to access the network. This section describes commands used to configure IPv4 Source Guard.

Table 87: IPv4 Source Guard Commands

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

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

Syntax

ip source-guard binding [**mode** {**acl** | **mac**}] *mac-address*
vlan *vlan-id* *ip-address* **interface ethernet** *unit/port-list*

no ip source-guard binding [**mode** {**acl** | **mac**}] *mac-address* **vlan** *vlan-id*

mode - Specifies the binding mode.

acl - Adds binding to ACL table.

mac - Adds binding to MAC address table.

mac-address - A valid unicast MAC address.

vlan-id - ID of a configured VLAN for an ACL filtering table or a range of VLANs for a MAC address filtering table. To specify a list separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094)

ip-address - A valid unicast IP address, including classful types A, B or C.

unit - Unit identifier. (Range: 1)

port-list - Physical port number or list of port numbers. Separate nonconsecutive port numbers with a comma and no spaces; or use a hyphen to designate a range of port numbers. (Range: 1-28)

Default Setting

No configured entries

Command Mode

Global Configuration

Command Usage

- ◆ If the binding mode is not specified in this command, the entry is bound to the ACL table by default.
- ◆ Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding), VLAN identifier, and port identifier.
- ◆ All static entries are configured with an infinite lease time, which is indicated with a value of zero by the [show ip source-guard](#) command (page 715).
- ◆ When source guard is enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table with this command.
- ◆ An entry with same MAC address and a different VLAN ID cannot be added to the binding table.
- ◆ Static bindings are processed as follows:
 - A valid static IP source guard entry will be added to the binding table in ACL mode if one of the following conditions is true:
 - If there is no binding entry with the same VLAN ID and MAC address, a new entry will be added to the binding table using the type of static IP source guard binding.
 - If there is an entry with the same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
 - If there is an entry with the same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.
 - A valid static IP source guard entry will be added to the binding table in MAC mode if one of the following conditions are true:
 - If there is no binding entry with the same IP address and MAC address, a new entry will be added to the binding table using the type of static IP source guard binding entry.

- If there is a binding entry with same IP address and MAC address, then the new entry shall replace the old one.

◆ Only unicast addresses are accepted for static bindings.

Example

This example configures a static source-guard binding on port 5. Since the binding mode is not specified, the entry is bound to the ACL table by default.

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1 192.168.0.99
interface ethernet 1/5
Console(config-if)#
```

Related Commands

[ip source-guard \(711\)](#)

[ip dhcp snooping \(697\)](#)

[ip dhcp snooping vlan \(703\)](#)

ip source-guard This command configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address. Use the **no** form to disable this function.

Syntax

ip source-guard {sip | sip-mac}

no ip source-guard

sip - Filters traffic based on IP addresses stored in the binding table.

sip-mac - Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Source guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.
- ◆ Setting source guard mode to "sip" or "sip-mac" enables this function on the selected port. Use the "sip" option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the "sip-mac" option to check these same parameters, plus the source MAC address. Use the **no ip source guard** command to disable this function on the selected port.

- ◆ When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table.
- ◆ Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, VLAN identifier, and port identifier).
- ◆ Static addresses entered in the source guard binding table with the `ip source-guard binding` command are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.
- ◆ If the IP source guard is enabled, an inbound packet's IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- ◆ Filtering rules are implemented as follows:
 - If DHCPv4 snooping is disabled (see [page 697](#)), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.
 - If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.
 - If IP source guard is enabled on an interface for which IP source bindings (dynamically learned via DHCP snooping or manually configured) are not yet configured, the switch will drop all IP traffic on that port, except for DHCP packets allowed by DHCP snooping.
 - Only unicast addresses are accepted for static bindings.

Example

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

Related Commands

[ip source-guard binding \(709\)](#)

[ip dhcp snooping \(697\)](#)

[ip dhcp snooping vlan \(703\)](#)

ip source-guard max-binding This command sets the maximum number of entries that can be bound to an interface. Use the **no** form to restore the default setting.

Syntax

ip source-guard [mode {acl | mac}] max-binding *number*

no ip source-guard [mode {acl | mac}] max-binding

mode - Specifies the learning mode.

acl - Searches for addresses in the ACL table.

mac - Searches for addresses in the MAC address table.

number - The maximum number of IP addresses that can be mapped to an interface in the binding table. (Range: 1-5 for ACL mode; 1-32 for MAC mode)

Default Setting

Mode: ACL, Maximum Binding: 5

Mode: MAC, Maximum Binding: 16

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ This command sets the maximum number of address entries that can be mapped to an interface in the binding table for the specified mode (ACL binding table or MAC address table) including dynamic entries discovered by DHCP snooping and static entries set by the **ip source-guard** command.
- ◆ The maximum binding for ACL mode restricts the number of “active” entries per port. If binding entries exceed the maximum number in IP source guard, only the maximum number of binding entries will be set. Dynamic binding entries exceeding the maximum number will be created but will not be active.
- ◆ The maximum binding for MAC mode restricts the number of MAC addresses learned per port. Authenticated IP traffic with different source MAC addresses cannot be learned if it would exceed this maximum number.

Example

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry. The mode is not specified, and therefore defaults to the ACL binding table.

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

ip source-guard mode This command sets the source-guard learning mode to search for addresses in the ACL binding table or the MAC address binding table. Use the **no** form to restore the default setting.

Syntax

ip source-guard mode {acl | mac}

no ip source-guard mode

mode - Specifies the learning mode.

acl - Searches for addresses in the ACL binding table.

mac - Searches for addresses in the MAC address binding table.

Default Setting

ACL

Command Mode

Interface Configuration (Ethernet)

Command Usage

There are two modes for the filtering table:

- ◆ ACL - IP traffic will be forwarded if it passes the checking process in the ACL mode binding table.
- ◆ MAC - A MAC entry will be added in MAC address table if IP traffic passes the checking process in MAC mode binding table.

Example

This command sets the binding table mode for the specified interface to MAC mode:

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard mode mac
Console(config-if)#
```

clear ip source-guard binding blocked This command clears source-guard binding table entries from RAM.

Syntax

clear ip source-guard binding blocked

Command Mode

Privileged Exec

Command Usage

When IP Source-Guard detects an invalid packet it creates a blocked record. These records can be viewed using the [show ip source-guard binding blocked](#) command. A maximum of 512 blocked records can be

stored before the switch overwrites the oldest record with new blocked records. Use the **clear ip source-guard binding blocked** command to clear this table.

Example

This command clears the blocked record table.

```
Console(config)#clear ip source-guard binding blocked
Console(config)#
```

show ip source-guard This command shows whether source guard is enabled or disabled on each interface.

Command Mode

Privileged Exec

Example

```
Console#show ip source-guard
```

Interface	Filter-type	Filter-table	ACL Table Max-binding	MAC Table Max-binding
Eth 1/1	DISABLED	ACL	5	1024
Eth 1/2	DISABLED	ACL	5	1024
Eth 1/3	DISABLED	ACL	5	1024
Eth 1/4	DISABLED	ACL	5	1024
Eth 1/5	DISABLED	ACL	5	1024
:				

show ip source-guard binding This command shows the source guard binding table.

Syntax

show ip source-guard binding [**dhcp-snooping** | **static** [**acl** | **mac**] | **blocked** [**vlan** *vlan-id* | **interface** *interface*]

dhcp-snooping - Shows dynamic entries configured with DHCP Snooping commands (see [page 696](#))

static - Shows static entries configured with the **ip source-guard binding** command.

acl - Shows static entries in the ACL binding table.

mac - Shows static entries in the MAC address binding table.

blocked - Shows MAC addresses which have been blocked by IP Source Guard.

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

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

Command Mode

Privileged Exec

Example

```
Console#show ip source-guard binding
MAC Address      IP Address      Type      VLAN      Interface
-----
00-11-3b-f4-d0-01 10.2.44.96      static-acl 1 Eth 1/1
Console#
```

ARP Inspection

ARP Inspection validates the MAC-to-IP address bindings in Address Resolution Protocol (ARP) packets. It protects against ARP traffic with invalid address bindings, which forms the basis for certain “man-in-the-middle” attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination, dropping any invalid ARP packets.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

This section describes commands used to configure ARP Inspection.

Table 88: ARP Inspection Commands

Command	Function	Mode
<code>ip arp inspection</code>	Enables ARP Inspection globally on the switch	GC
<code>ip arp inspection filter</code>	Specifies an ARP ACL to apply to one or more VLANs	GC
<code>ip arp inspection log-buffer logs</code>	Sets the maximum number of entries saved in a log message, and the rate at these messages are sent	GC
<code>ip arp inspection validate</code>	Specifies additional validation of address components in an ARP packet	GC
<code>ip arp inspection vlan</code>	Enables ARP Inspection for a specified VLAN or range of VLANs	GC

Table 88: 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. Use the **no** form to remove an ACL binding.

Syntax

ip arp inspection filter *arp-acl-name* **vlan** {*vlan-id* | *vlan-range*} [**static**]

no ip arp inspection filter *arp-acl-name* **vlan** {*vlan-id* | *vlan-range*}

arp-acl-name - Name of an ARP ACL. (Maximum length: 16 characters)

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

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

static - ARP packets are only validated against the specified ACL, address bindings in the DHCP snooping database is not checked.

Default Setting

ARP ACLs are not bound to any VLAN
Static mode is not enabled

Command Mode

Global Configuration

Command Usage

- ◆ ARP ACLs are configured with the commands described [on page 752](#).
- ◆ If static mode is enabled, the switch compares ARP packets to the specified ARP ACLs. Packets matching an IP-to-MAC address binding in a permit or deny rule are processed accordingly. Packets not matching any of the ACL rules are dropped. Address bindings in the DHCP snooping database are not checked.
- ◆ If static mode is not enabled, packets are first validated against the specified ARP ACL. Packets matching a deny rule are dropped. All remaining packets are validated against the address bindings in the DHCP snooping database.

Example

```
Console(config)#ip arp inspection filter sales vlan 1  
Console(config)#
```

ip arp inspection log-buffer logs This command sets the maximum number of entries saved in a log message, and the rate at which these messages are sent. Use the **no** form to restore the default settings.

Syntax

ip arp inspection log-buffer logs *message-number* **interval** *seconds*

no ip arp inspection log-buffer logs

message-number - The maximum number of entries saved in a log message.
(Range: 0-256, where 0 means no events are saved and no messages sent)

seconds - The interval at which log messages are sent. (Range: 0-86400)

Default Setting

Message Number: 20

Interval: 10 seconds

Command Mode

Global Configuration

Command Usage

- ◆ ARP Inspection must be enabled with the **ip arp inspection** command before this command will be accepted by the switch.
- ◆ By default, logging is active for ARP Inspection, and cannot be disabled.
- ◆ When the switch drops a packet, it places an entry in the log buffer. Each entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- ◆ If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- ◆ The maximum number of entries that can be stored in the log buffer is determined by the *message-number* parameter. If the log buffer fills up before a message is sent, the oldest entry will be replaced with the newest one.
- ◆ The switch generates a system message on a rate-controlled basis determined by the *seconds* values. After the system message is generated, all entries are cleared from the log buffer.

Example

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

ip arp inspection validate This command specifies additional validation of address components in an ARP packet. Use the **no** form to restore the default setting.

Syntax

ip arp inspection validate
{**dst-mac** [**ip** [**allow-zeros**] [**src-mac**]] |
ip [**allow-zeros**] [**src-mac**]] | **src-mac**}

no ip arp inspection validate

dst-mac - Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ip - Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.

allow-zeros - Allows sender IP address to be 0.0.0.0.

src-mac - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

Default Setting

No additional validation is performed

Command Mode

Global Configuration

Command Usage

By default, ARP Inspection only checks the IP-to-MAC address bindings specified in an ARP ACL or in the DHCP Snooping database.

Example

```
Console(config)#ip arp inspection validate dst-mac
Console(config)#
```

ip arp inspection vlan This command enables ARP Inspection for a specified VLAN or range of VLANs. Use the **no** form to disable this function.

Syntax

[no] ip arp inspection vlan {*vlan-id* | *vlan-range*}

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

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Default Setting

Disabled on all VLANs

Command Mode

Global Configuration

Command Usage

- ◆ When ARP Inspection is enabled globally with the **ip arp inspection** command, it becomes active only on those VLANs where it has been enabled with this command.
- ◆ When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- ◆ When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- ◆ When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- ◆ Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.
- ◆ When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

Example

```
Console(config)#ip arp inspection vlan 1,2
Console(config)#
```

ip arp inspection limit This command sets a rate limit for the ARP packets received on a port. Use the **no** form to restore the default setting.

Syntax

ip arp inspection limit {rate *pps* | **none**}

no ip arp inspection limit

pps - The maximum number of ARP packets that can be processed by the CPU per second on trusted or untrusted ports. (Range: 0-2048, where 0 means that no ARP packets can be forwarded)

none - There is no limit on the number of ARP packets that can be processed by the CPU.

Default Setting

15

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

- ◆ This command applies to both trusted and untrusted ports.
- ◆ When the rate of incoming ARP packets exceeds the configured limit, the switch drops all ARP packets in excess of the limit.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit rate 150
Console(config-if)#
```

ip arp inspection trust This command sets a port as trusted, and thus exempted from ARP Inspection. Use the **no** form to restore the default setting.

Syntax

[no] ip arp inspection trust

Default Setting

Untrusted

Command Mode

Interface Configuration (Port, Static Aggregation)

Command Usage

Packets arriving on untrusted ports are subject to any configured ARP Inspection and additional validation checks. Packets arriving on trusted ports bypass all of these checks, and are forwarded according to normal switching rules.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```

show ip arp inspection configuration

This command displays the global configuration settings for ARP Inspection.

Command Mode

Privileged Exec

Example

```
Console#show ip arp inspection configuration

ARP Inspection Global Information:

Global IP ARP Inspection Status : disabled
Log Message Interval           : 1 s
Log Message Number             : 5
Need Additional Validation(s)   : Yes
Additional Validation Type       : Destination MAC address
Console#
```

show ip arp inspection interface

This command shows the trust status and ARP Inspection rate limit for ports.

Syntax

show ip arp inspection interface *[interface]*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

Command Mode

Privileged Exec

Example

```
Console#show ip arp inspection interface ethernet 1/1

Port Number      Trust Status      Rate Limit (pps)
-----
Eth 1/1          Trusted           150
Console#
```

show ip arp inspection log This command shows information about entries stored in the log, including the associated VLAN, port, and address components.

Command Mode
Privileged Exec

Example

```
Console#show ip arp inspection log
Total log entries number is 1

Num VLAN Port Src IP Address Dst IP Address Src MAC Address Dst MAC Address
-----
1 1 11 192.168.2.2 192.168.2.1 00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-FF
Console#
```

show ip arp inspection statistics This command shows statistics about the number of ARP packets processed, or dropped for various reasons.

Command Mode
Privileged Exec

Example

```
Console#show ip arp inspection statistics

ARP packets received : 150
ARP packets dropped due to rate limit : 5
Total ARP packets processed by ARP Inspection : 150
ARP packets dropped by additional validation (source MAC address) : 0
ARP packets dropped by additional validation (destination MAC address) : 0
ARP packets dropped by additional validation (IP address) : 0
ARP packets dropped by ARP ACLs : 0
ARP packets dropped by DHCP snooping : 0

Console#
```

show ip arp inspection vlan This command shows the configuration settings for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ARP ACL validation is completed.

Syntax

show ip arp inspection vlan [*vlan-id* | *vlan-range*]

vlan-id - Identifier for configured VLANs.

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Command Mode
Privileged Exec

Example

```
Console#show ip arp inspection vlan 1
```

VLAN ID	DAI Status	ACL Name	ACL Status
1	disabled	sales	static

```
Console#
```

Denial of Service Protection

A denial-of-service attack (DoS attack) is an attempt to block the services provided by a computer or network resource. This kind of attack tries to prevent an Internet site or service from functioning efficiently or at all. In general, DoS attacks are implemented by either forcing the target to reset, to consume most of its resources so that it can no longer provide its intended service, or to obstruct the communication media between the intended users and the target so that they can no longer communicate adequately.

This section describes commands used to protect against DoS attacks.

Table 89: DoS Protection Commands

Command	Function	Mode
<code>dos-protection smurf</code>	Protects against DoS smurf 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>show dos-protection</code>	Shows the configuration settings for DoS protection	PE

dos-protection smurf This command protects against DoS smurf attacks in which a perpetrator generates a large amount of spoofed ICMP Echo Request traffic to the broadcast destination IP address (255.255.255.255), all of which uses a spoofed source address of the intended victim. The victim should crash due to the many interrupts required to send ICMP Echo response packets. Use the **no** form to disable this feature.

Syntax

[no] dos-protection smurf

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection smurf
Console(config)#
```

dos-protection tcp-null-scan

This command protects against DoS TCP-null-scan attacks in which a TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. Use the **no** form to disable this feature.

Syntax

[no] **dos-protection tcp-null-scan**

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection tcp-null-scan
Console(config)#
```

dos-protection tcp-syn-fin-scan

This command protects against DoS TCP-SYN/FIN-scan attacks in which a TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. Use the **no** form to disable this feature.

Syntax

[no] **dos-protection tcp-syn-fin-scan**

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection syn-fin-scan
Console(config)#
```

dos-protection tcp-xmas-scan This command protects against DoS TCP-xmas-scan in which a so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. Use the **no** form to disable this feature.

Syntax

[no] **dos-protection tcp-xmas-scan**

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dos-protection tcp-xmas-scan
Console(config)#
```

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:

Smurf Attack           : Enabled
TCP Null Scan          : Enabled
TCP SYN/FIN Scan       : Enabled
TCP XMAS Scan          : Enabled
Console#
```

Port-based Traffic Segmentation

If tighter security is required for passing traffic from different clients through downlink ports on the local network and over uplink ports to the service provider, port-based traffic segmentation can be used to isolate traffic for individual clients.

Traffic belonging to each client is isolated to the allocated downlink ports. But the switch can be configured to either isolate traffic passing across a client's allocated uplink ports from the uplink ports assigned to other clients, or to forward traffic

through the uplink ports used by other clients, allowing different clients to share access to their uplink ports where security is less likely to be compromised.

Table 90: Commands for Configuring Traffic Segmentation

Command	Function	Mode
<code>traffic-segmentation</code>	Enables traffic segmentation	GC
<code>traffic-segmentation session</code>	Creates a client session	GC
<code>traffic-segmentation uplink/ downlink</code>	Configures uplink/downlink ports for client sessions	GC
<code>traffic-segmentation uplink-to-uplink</code>	Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions	GC
<code>show traffic-segmentation</code>	Displays the configured traffic segments	PE

traffic-segmentation This command enables traffic segmentation. Use the **no** form to disable traffic segmentation.

Syntax

[no] **traffic-segmentation**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Traffic segmentation provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the designated uplink port(s). Data cannot pass between downlink ports in the same segmented group, nor to ports which do not belong to the same group.
- ◆ Traffic segmentation and normal VLANs can exist simultaneously within the same switch. Traffic may pass freely between uplink ports in segmented groups and ports in normal VLANs.

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

Table 91: Traffic Segmentation Forwarding

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

* The forwarding state for uplink-to-uplink ports is configured by the [traffic-segmentation uplink-to-uplink](#) command.

- ◆ When traffic segmentation is disabled, all ports operate in normal forwarding mode based on the settings specified by other functions such as VLANs and spanning tree protocol.
- ◆ Enter the **traffic-segmentation** command without any parameters to enable traffic segmentation. Then set the interface members for segmented groups using the [traffic-segmentation uplink/downlink](#) command.
- ◆ Enter **no traffic-segmentation** to disable traffic segmentation and clear the configuration settings for segmented groups.

Example

This example enables traffic segmentation globally on the switch.

```
Console(config)#traffic-segmentation
Console(config)#
```

traffic-segmentation session This command creates a traffic-segmentation client session. Use the **no** form to remove a client session.

Syntax

[no] **traffic-segmentation session** *session-id*

session-id – Traffic segmentation session. (Range: 1-4)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Use this command to create a new traffic-segmentation client session.
- ◆ Using the **no** form of this command will remove any assigned uplink or downlink ports, restoring these interfaces to normal operating mode.

Example

```
Console(config)#traffic-segmentation session 1
Console(config)#
```

traffic-segmentation uplink/downlink This command configures the uplink and down-link ports for a segmented group of ports. Use the **no** form to remove a port from the segmented group.

Syntax

[no] **traffic-segmentation** [session *session-id*] {**uplink** *interface-list* [**downlink** *interface-list*] | **downlink** *interface-list*}

session-id – Traffic segmentation session. (Range: 1-4)

uplink – Specifies an uplink interface.

downlink – Specifies a downlink interface.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

Session 1 if not defined

No segmented port groups are defined.

Command Mode

Global Configuration

Command Usage

- ◆ A port cannot be configured in both an uplink and downlink list.
- ◆ A port can only be assigned to one traffic-segmentation session.
- ◆ When specifying an uplink or downlink, a list of ports may be entered by using a hyphen or comma in the *port* field. Note that lists are not supported for the *channel-id* field.

- ◆ A downlink port can only communicate with an uplink port in the same session. Therefore, if an uplink port is not configured for a session, the assigned downlink ports will not be able to communicate with any other ports.
- ◆ If a downlink port is not configured for the session, the assigned uplink ports will operate as normal ports.

Example

This example enables traffic segmentation, and then sets port 10 as the uplink and ports 5-8 as downlinks.

```
Console(config)#traffic-segmentation
Console(config)#traffic-segmentation uplink ethernet 1/10
downlink ethernet 1/5-8
Console(config)#
```

traffic-segmentation uplink-to-uplink

This command specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions. Use the **no** form to restore the default.

Syntax

[no] traffic-segmentation uplink-to-uplink {blocking | forwarding}

blocking – Blocks traffic between uplink ports assigned to different sessions.

forwarding – Forwards traffic between uplink ports assigned to different sessions.

Default Setting

Blocking

Command Mode

Global Configuration

Example

This example enables forwarding of traffic between uplink ports assigned to different client sessions.

```
Console(config)#traffic-segmentation uplink-to-uplink forwarding
Console(config)#
```

show traffic-segmentation This command displays the configured traffic segments.

Command Mode

Privileged Exec

Example

```
Console#show traffic-segmentation
```

```
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#
```


Access Control Lists

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, or next header type), or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, and then bind the list to a specific port. This section describes the Access Control List commands.

Table 92: 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 93: IPv4 ACL Commands

Command	Function	Mode
<code>access-list ip</code>	Creates an IP ACL and enters configuration mode for standard or extended IPv4 ACLs	GC
<code>permit, deny</code>	Filters packets matching a specified source IPv4 address	IPv4-STD-ACL
<code>permit, deny</code>	Filters packets meeting the specified criteria, including source and destination IPv4 address, TCP/UDP port number, protocol type, and TCP control code	IPv4-EXT-ACL
<code>ip access-group</code>	Binds an IPv4 ACL to a port	IC
<code>show ip access-group</code>	Shows port assignments for IPv4 ACLs	PE
<code>show ip access-list</code>	Displays the rules for configured IPv4 ACLs	PE

access-list ip This command adds an IP access list and enters configuration mode for standard or extended IPv4 ACLs. Use the **no** form to remove the specified ACL.

Syntax

[no] **access-list ip** {**standard** | **extended**} *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.

acl-name – Name of the ACL. (Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 1K rules.

Example

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

Related Commands

[permit, deny \(735\)](#)

[show ip access-list \(739\)](#)

permit, deny (Standard IP ACL) This command adds a rule to a Standard IPv4 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

```
{permit | deny} {any | source bitmask | host source}  
[time-range time-range-name]  
no {permit | deny} {any | source bitmask | host source}
```

any – Any source IP address.

source – Source IP address.

bitmask – Dotted decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

time-range-name - Name of the time range. (Range: 1-16 characters)

Default Setting

None

Command Mode

Standard IPv4 ACL

Command Usage

- ◆ New rules are appended to the end of the list.
- ◆ Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21  
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0  
Console(config-std-acl)#
```

Related Commands

[access-list ip \(734\)](#)

[Time Range \(587\)](#)

permit, deny (Extended IPv4 ACL) This command adds a rule to an Extended IPv4 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

```
{permit | deny} [protocol-number | udp]
  {any | source address-bitmask | host source}
  {any | destination address-bitmask | host destination}
  [dscp dscp] [precedence precedence]
  [source-port sport [bitmask]]
  [destination-port dport [port-bitmask]]
  [time-range time-range-name]
```

```
no {permit | deny} [protocol-number | udp]
  {any | source address-bitmask | host source}
  {any | destination address-bitmask | host destination}
  [dscp dscp] [precedence precedence]
  [source-port sport [bitmask]]
  [destination-port dport [port-bitmask]]
```

```
{permit | deny} tcp
  {any | source address-bitmask | host source}
  {any | destination address-bitmask | host destination}
  [dscp dscp] [precedence precedence]
  [source-port sport [bitmask]]
  [destination-port dport [port-bitmask]]
  [control-flag control-flags flag-bitmask]
  [time-range time-range-name]
```

```
no {permit | deny} tcp
  {any | source address-bitmask | host source}
  {any | destination address-bitmask | host destination}
  [dscp dscp] [precedence precedence]
  [source-port sport [bitmask]]
  [destination-port dport [port-bitmask]]
  [control-flag control-flags flag-bitmask]
```

protocol-number – A specific protocol number. (Range: 0-255)

source – Source IP address.

destination – Destination IP address.

address-bitmask – Decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

dscp – DSCP priority level. (Range: 0-63)

precedence – IP precedence level. (Range: 0-7)

sport – Protocol¹³ source port number. (Range: 0-65535)

dport – Protocol¹³ destination port number. (Range: 0-65535)

13. Includes TCP, UDP or other protocol types.

port-bitmask – Decimal number representing the port bits to match.
(Range: 0-65535)

control-flags – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

flag-bitmask – Decimal number representing the code bits to match.

time-range-name - Name of the time range. (Range: 1-16 characters)

Default Setting

None

Command Mode

Extended IPv4 ACL

Command Usage

- ◆ All new rules are appended to the end of the list.
- ◆ Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bit mask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- ◆ The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
 - 1 (fin) – Finish
 - 2 (syn) – Synchronize
 - 4 (rst) – Reset
 - 8 (psh) – Push
 - 16 (ack) – Acknowledgement
 - 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use “control-code 2 2”
 - Both SYN and ACK valid, use “control-code 18 18”
 - SYN valid and ACK invalid, use “control-code 2 18”
- ◆ If an Extended IPv4 rule and MAC rule match the same packet, and these rules specify a “permit” entry and “deny” entry, the “deny” action takes precedence.

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port
80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any control-
flag 2 2
Console(config-ext-acl)#
```

Related Commands

[access-list ip \(734\)](#)

[Time Range \(587\)](#)

ip access-group This command binds an IPv4 ACL to a port. Use the **no** form to remove the port.

Syntax

ip access-group *acl-name* **in**
[**time-range** *time-range-name*] [**counter**]

no ip access-group *acl-name* **in**

acl-name – Name of the ACL. (Maximum length: 32 characters)

in – Indicates that this list applies to ingress packets.

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

counter – Enables counter for ACL statistics.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

Example

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

Related Commands

[show ip access-list \(739\)](#)

[Time Range \(587\)](#)

show ip access-group This command shows the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/2
  IP access-list david in
Console#
```

show ip access-list This command displays the rules for configured IPv4 ACLs.

Syntax

show ip access-list {standard | extended} [acl-name]

standard – Specifies a standard IP ACL.

extended – Specifies an extended IP ACL.

acl-name – Name of the ACL. (Maximum length: 32 characters)

Command Mode

Privileged Exec

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
Console#
```

Related Commands

permit, deny (735)

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 94: IPv6 ACL Commands

Command	Function	Mode
<code>access-list ipv6</code>	Creates an IPv6 ACL and enters configuration mode for standard or extended IPv6 ACLs	GC
<code>permit, deny</code>	Filters packets matching a specified source IPv6 address	IPv6- STD-ACL
<code>permit, deny</code>	Filters packets meeting the specified criteria, including source or destination IPv6 address, DSCP traffic class, or next header type	IPv6- EXT-ACL
<code>ipv6 access-group</code>	Binds an IPv6 ACL to a port	IC
<code>show ipv6 access-group</code>	Shows port assignments for IPv6 ACLs	PE
<code>show ipv6 access-list</code>	Displays the rules for configured IPv6 ACLs	PE

access-list ipv6 This command adds an IP access list and enters configuration mode for standard or extended IPv6 ACLs. Use the **no** form to remove the specified ACL.

Syntax

[no] **access-list ipv6** {**standard** | **extended**} *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the destination IP address, and other more specific criteria.

acl-name – Name of the ACL. (Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.

- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 64 rules.

Example

```
Console(config)#access-list ipv6 standard david
Console(config-std-ipv6-acl)#
```

Related Commands

[permit, deny \(Standard IPv6 ACL\) \(741\)](#)

[permit, deny \(Extended IPv6 ACL\) \(742\)](#)

[ipv6 access-group \(745\)](#)

[show ipv6 access-list \(746\)](#)

permit, deny (Standard IPv6 ACL) This command adds a rule to a Standard IPv6 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

```
{permit | deny} {any | host source-ipv6-address |  
  source-ipv6-address/prefix-length}  
[time-range time-range-name]
```

```
no {permit | deny} {any | host source-ipv6-address |  
  source-ipv6-address/prefix-length}
```

any – Any source IP address.

host – Keyword followed by a specific IP address.

source-ipv6-address - An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128)

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

Default Setting

None

Command Mode

Standard IPv6 ACL

Command Usage

New rules are appended to the end of the list.

Example

This example configures one permit rule for the specific address 2000::4:213:19FF:FE7B:5004 and another rule for the addresses with the network prefix 2000:0:0:2::2/64.

```
Console(config)#access-list ipv6 standard david
Console(config-std-ipv6-acl)#permit host 2000::4:213:19FF:FE7B:5004
Console(config-std-ipv6-acl)#permit 2000:0:0:2::2/64
Console(config-std-ipv6-acl)#
```

Related Commands

[access-list ipv6 \(740\)](#)

[Time Range \(587\)](#)

permit, deny
(Extended IPv6 ACL)

This command adds a rule to an Extended IPv6 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, or next header type. Use the **no** form to remove a rule.

Syntax

```
{permit | deny}
{any | host source-ipv6-address | source-ipv6-address[/prefix-length]}
{any | destination-ipv6-address[/prefix-length]}
[dscp dscp] [next-header next-header]
[source-port sport [bitmask]]
[destination-port dport [port-bitmask]]
[time-range time-range-name]

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

any – Any IP address (an abbreviation for the IPv6 prefix ::/0).

host – Keyword followed by a specific source IP address.

source-ipv6-address - An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

destination-ipv6-address - An IPv6 destination address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (The switch only checks the first 128 bits of the destination address.)

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128 for source prefix, 0-128 for destination prefix)

dscp - DSCP traffic class. (Range: 0-63)

next-header - Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

sport - Protocol¹⁴ source port number. (Range: 0-65535)

dport - Protocol¹³ destination port number. (Range: 0-65535)

port-bitmask - Decimal number representing the port bits to match. (Range: 0-65535)

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

Default Setting

None

Command Mode

Extended IPv6 ACL

Command Usage

- ◆ All new rules are appended to the end of the list.
- ◆ Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, including these commonly used headers:

0	: Hop-by-Hop Options	(RFC 2460)
6	: TCP Upper-layer Header	(RFC 1700)
17	: UDP Upper-layer Header	(RFC 1700)
43	: Routing	(RFC 2460)
44	: Fragment	(RFC 2460)
51	: Authentication	(RFC 2402)
50	: Encapsulating Security Payload	(RFC 2406)
60	: Destination Options	(RFC 2460)

Example

This example accepts any incoming packets if the destination address is 2009:DB9:2229::79/8.

```
Console(config)#access-list ipv6 extended John
Console(config-ext-ipv6-acl)#permit any 2000::4:213:19FF:FE7B:5004/8
Console(config-ext-ipv6-acl)#
```

¹⁴. Includes TCP and UDP.

This allows packets to any destination address when the DSCP value is 5.

```
Console(config-ext-ipv6-acl)#permit any any dscp 5
Console(config-ext-ipv6-acl)#
```

This allows any packets sent from any source to any destination when the next header is 43."

```
Console(config-ext-ipv6-acl)#permit any any next-header 43
Console(config-ext-ipv6-acl)#
```

Here is a more detailed example for setting the CPU rate limit for SNMP packets.

```
Set ACL
Console(config)#access-list ip extended snmp-acl
Console(config-ext-acl)#permit any any destination-port 161
Console(config-ext-acl)#permit any any destination-port 162
Console(config-ext-acl)#exit

Set class map
Console(config)#class-map snmp-class
Console(config-cmap)#match access-list snmp-acl
Console(config-cmap)#

Set policy map and rate-limit
Console(config)#policy-map cpu-rate-limit-policy
Console(config-pmap)#class snmp-class
Console(config-pmap-c)police flow 10000 20000 conform-action transmit
violate-action drop
Console(config-pmap-c)exit
Console(config-pmap)#exit

Bind the service-policy to control-plane
Console(config)#control-plane
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input cpu-rate-limit-policy
Console(config-if)#
```

Related Commands

[access-list ipv6 \(740\)](#)

[Time Range \(587\)](#)

ipv6 access-group This command binds an IPv6 ACL to a port. Use the **no** form to remove the port.

Syntax

ipv6 access-group *acl-name* **in**
[**time-range** *time-range-name*] [**counter**]

no ipv6 access-group *acl-name* **in**

acl-name – Name of the ACL. (Maximum length: 32 characters)

in – Indicates that this list applies to ingress packets.

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

counter – Enables counter for ACL statistics.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#ipv6 access-group standard david in
Console(config-if)#
```

Related Commands

[show ipv6 access-list \(746\)](#)

[Time Range \(587\)](#)

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 \(745\)](#)

show ipv6 access-list This command displays the rules for configured IPv6 ACLs.

Syntax

show ipv6 access-list {**standard** | **extended**} [*acl-name*]

standard – Specifies a standard IPv6 ACL.

extended – Specifies an extended IPv6 ACL.

acl-name – Name of the ACL. (Maximum length: 32 characters)

Command Mode

Privileged Exec

Example

```
Console#show ipv6 access-list standard
IPv6 standard access-list david:
  permit host 2000::4:213:19ff:fe7b:5004
  permit 2000:0:0:2::2/64
  permit 2000:0:0:2::2/8
Console#
```

Related Commands

[permit, deny \(Standard IPv6 ACL\) \(741\)](#)

[permit, deny \(Extended IPv6 ACL\) \(742\)](#)

[ipv6 access-group \(745\)](#)

MAC ACLs

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. The ACLs can further specify optional IP and IPv6 addresses including protocol type and upper layer ports. To configure MAC ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 95: MAC ACL Commands

Command	Function	Mode
access-list mac	Creates a MAC ACL and enters configuration mode	GC
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type. They can be further specified using optional IP and IPv6 addresses including protocol type and upper layer ports.	MAC-ACL
mac access-group	Binds a MAC ACL to a port	IC
show mac access-group	Shows port assignments for MAC ACLs	PE
show mac access-list	Displays the rules for configured MAC ACLs	PE

access-list mac This command enters MAC ACL configuration mode. Rules can be added to filter packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Rules can also be used to filter packets based on IPv4/v6 addresses, including Layer 4 ports and protocol types. Use the **no** form to remove the specified ACL.

Syntax

[no] **access-list mac** *acl-name*

acl-name – Name of the ACL. (Maximum length: 32 characters,)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 2048 rules.

Example

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

Related Commands

[permit, deny \(747\)](#)

[mac access-group \(750\)](#)

[show mac access-list \(751\)](#)

permit, deny (MAC ACL) This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Rules can also filter packets based on IPv4/v6 addresses, including Layer 4 ports and protocol types. Use the **no** form to remove a rule.

Syntax

```
{permit | deny}
{any | host source | source address-bitmask}
{any | host destination | destination address-bitmask}
[cos cos cos-bitmask] [vid vid vid-bitmask]
[ethertype ethertype [ethertype-bitmask]]
[time-range time-range-name]
```

```
no {permit | deny}
    {any | host source | source address-bitmask}
    {any | host destination | destination address-bitmask}
    [cos cos cos-bitmask] [vid vid vid-bitmask]
    [ethertype ethertype [ethertype-bitmask]]
```



Note: The default is for Ethernet II packets.

```
{permit | deny} tagged-eth2
    {any | host source | source address-bitmask}
    {any | host destination | destination address-bitmask}
    [cos cos cos-bitmask] [vid vid vid-bitmask]
    [ethertype ethertype [ethertype-bitmask]]
    [time-range time-range-name]
```

```
no {permit | deny} tagged-eth2
    {any | host source | source address-bitmask}
    {any | host destination | destination address-bitmask}
    [cos cos cos-bitmask] [vid vid vid-bitmask]
    [ethertype ethertype [ethertype-bitmask]]
    {permit | deny} untagged-eth2
    {any | host source | source address-bitmask}
    {any | host destination | destination address-bitmask}
    [ethertype ethertype [ethertype-bitmask]]
    [time-range time-range-name]
```

```
no {permit | deny} untagged-eth2
    {any | host source | source address-bitmask}
    {any | host destination | destination address-bitmask}
    [ethertype ethertype [ethertype-bitmask]]
    {permit | deny} tagged-802.3
    {any | host source | source address-bitmask}
    {any | host destination | destination address-bitmask}
    [cos cos cos-bitmask] [vid vid vid-bitmask]
    [time-range time-range-name]
```

```
no {permit | deny} tagged-802.3
    {any | host source | source address-bitmask}
    {any | host destination | destination address-bitmask}
    [cos cos cos-bitmask] [vid vid vid-bitmask]
```

```
{permit | deny} untagged-802.3
    {any | host source | source address-bitmask}
    {any | host destination | destination address-bitmask}
    [time-range time-range-name]
```

```
no {permit | deny} untagged-802.3
    {any | host source | source address-bitmask}
    {any | host destination | destination address-bitmask}
```

tagged-eth2 – Tagged Ethernet II packets.

untagged-eth2 – Untagged Ethernet II packets.

tagged-802.3 – Tagged Ethernet 802.3 packets.

untagged-802.3 – Untagged Ethernet 802.3 packets.

any – Any MAC, IPv4 or IPv6 source or destination address.

host – A specific MAC, IPv4 or IPv6 address.

source – Source MAC, IPv4 or IPv6 address.

destination – Destination MAC, IPv4 or IPv6 address.

*address-bitmask*¹⁵ – Bitmask for MAC address (in hexadecimal format).

network-mask – Network mask for IP subnet. This mask identifies the host address bits used for routing to specific subnets.

prefix-length – Length of IPv6 prefix. A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128)

cos – Class-of-Service value (Range: 0-7)

*cos-bitmask*¹⁵ – Class-of-Service bitmask. (Range: 0-7)

vid – VLAN ID. (Range: 1-4094)

*vid-bitmask*¹⁵ – VLAN bitmask. (Range: 1-4095)

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

*ethertype-bitmask*¹⁵ – Protocol bitmask. (Range: 0-ffff hex)

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

Default Setting

None

Command Mode

MAC ACL

Command Usage

- ◆ New rules are added to the end of the list.
- ◆ The **ethertype** option can only be used to filter Ethernet II formatted packets.
- ◆ A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
 - 0800 - IP
 - 0806 - ARP
 - 8137 - IPX
- ◆ If an Extended IPv4 rule and MAC rule match the same packet, and these rules specify a “permit” entry and “deny” entry, the “deny” action takes precedence.

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

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

Related Commands

[access-list mac \(747\)](#)

[Time Range \(587\)](#)

mac access-group This command binds a MAC ACL to a port. Use the **no** form to remove the port.

Syntax

mac access-group *acl-name* **in**
[**time-range** *time-range-name*] [**counter**]

no mac access-group *acl-name* **in**

acl-name – Name of the ACL. (Maximum length: 32 characters)

in – Indicates that this list applies to ingress packets.

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

counter – Enables counter for ACL statistics.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

Related Commands

[show mac access-list \(751\)](#)

[Time Range \(587\)](#)

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 \(750\)](#)

show mac access-list This command displays the rules for configured MAC ACLs.

Syntax

show mac access-list [*acl-name*]

acl-name – Name of the ACL. (Maximum length: 32 characters)

Command Mode

Privileged Exec

Example

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

Related Commands

[permit, deny \(747\)](#)

[mac access-group \(750\)](#)

ARP ACLs

The commands in this section configure ACLs based on the IP or MAC address contained in ARP request and reply messages. To configure ARP ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more VLANs using the `ip arp inspection vlan` command.

Table 96: ARP ACL Commands

Command	Function	Mode
<code>access-list arp</code>	Creates a ARP ACL and enters configuration mode	GC
<code>permit, deny</code>	Filters packets matching a specified source or destination address in ARP messages	ARP-ACL
<code>show access-list arp</code>	Displays the rules for configured ARP ACLs	PE

access-list arp This command adds an ARP access list and enters ARP ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

[no] access-list arp *acl-name*

acl-name – Name of the ACL. (Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- ◆ To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- ◆ An ACL can contain up to 128 rules.

Example

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

Related Commands

`permit, deny` (753)

`show access-list arp` (754)

permit, deny (ARP ACL) This command adds a rule to an ARP ACL. The rule filters packets matching a specified source or destination address in ARP messages. Use the **no** form to remove a rule.

Syntax

```
[no] {permit | deny} ip
    {any | host source-ip | source-ip ip-address-bitmask}
    {any | host destination-ip | destination-ip ip-address-bitmask}
    mac {any | host source-mac | source-mac mac-address-bitmask}
    [any | host destination-mac | destination-mac mac-address-bitmask] [log]
```

This form indicates either request or response packets.

```
[no] {permit | deny} request
    ip {any | host source-ip | source-ip ip-address-bitmask}
    {any | host destination-ip | destination-ip ip-address-bitmask}
    mac {any | host source-mac | source-mac mac-address-bitmask}
    [any | host destination-mac | destination-mac mac-address-bitmask] [log]
```

```
[no] {permit | deny} response
    ip {any | host source-ip | source-ip ip-address-bitmask}
    {any | host destination-ip | destination-ip ip-address-bitmask}
    mac {any | host source-mac | source-mac mac-address-bitmask}
    [any | host destination-mac | destination-mac mac-address-bitmask] [log]
```

source-ip – Source IP address.

destination-ip – Destination IP address with bitmask.

*ip-address-bitmask*¹⁶ – IPv4 number representing the address bits to match.

source-mac – Source MAC address.

destination-mac – Destination MAC address range with bitmask.

*mac-address-bitmask*¹⁶ – 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.

16. 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 \(752\)](#)

show access-list arp This command displays the rules for configured ARP ACLs.

Syntax

show access-list arp [*acl-name*]
acl-name – Name of the ACL. (Maximum length: 32 characters)

Command Mode
Privileged Exec

Example

```
Console#show access-list arp
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#
```

Related Commands
[permit, deny \(753\)](#)

ACL Information

This section describes commands used to display ACL information.

Table 97: 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
[**direction in** [**interface** *interface*]] |
[**interface** *interface*] | [**name** *acl-name*]

in – Clears counter for ingress rules.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

acl-name – Name of the ACL. (Maximum length: 32 characters)

Command Mode

Privileged Exec

Example

```
Console#clear access-list hardware counters
Console#
```

show access-group This command shows the port assignments of ACLs.

Command Mode

Privileged Executive

Example

```
Console#show access-group
Interface ethernet 1/2
  IP access-list david
  MAC access-list jerry
Console#
```

show access-list This command shows all ACLs and associated rules.

Syntax

show access-list

[[arp [acl-name]] |
ip [extended [acl-name] | standard [acl-name]] |
ipv6 [extended [acl-name] | standard [acl-name]] |
mac [acl-name]] | [tcam-utilization] | [hardware counters]]

arp – Shows ingress or egress rules for ARP ACLs.

hardware counters – Shows statistics for all ACLs.¹⁷

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

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

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

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

mac – Shows ingress or egress rules for MAC ACLs.

tcam-utilization – Shows the percentage of user configured ACL rules as a percentage of total ACL rules

acl-name – Name of the ACL. (Maximum length: 32 characters)

Command Mode

Privileged Exec

Example

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
Console#
```

¹⁷ Due to a hardware limitation, this option only displays statistics for permit rules.

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN; or perform cable diagnostics on the specified interface.

Table 98: Interface Commands

Command	Function	Mode
<i>Interface Configuration</i>		
<code>interface</code>	Configures an interface type and enters interface configuration mode	GC
<code>capabilities</code>	Advertises the capabilities of a given interface for use in autonegotiation	IC
<code>description</code>	Adds a description to an interface configuration	IC
<code>flowcontrol</code>	Enables flow control on a given interface	IC
<code>history</code>	Configures a periodic sampling of statistics, specifying the sampling interval and number of samples	IC
<code>media-type</code>	Forces transceiver mode to use for SFP ports, or the port type to use for combination RJ-45/SFP ports	IC
<code>negotiation</code>	Enables autonegotiation of a given interface	IC
<code>shutdown</code>	Disables an interface	IC
<code>speed-duplex</code>	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC
<code>clear counters</code>	Clears statistics on an interface	PE
<code>show interfaces brief</code>	Displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type	PE
<code>show interfaces counters</code>	Displays statistics for the specified interfaces	NE, PE
<code>show interfaces history</code>	Displays periodic sampling of statistics, including the sampling interval, number of samples, and counter values	NE, PE
<code>show interfaces status</code>	Displays status for the specified interface	NE, PE
<code>show interfaces switchport</code>	Displays the administrative and operational status of an interface	NE, PE
<i>Transceiver Threshold Configuration</i>		
<code>transceiver-monitor</code>	Sends a trap when any of the transceiver's operational values fall outside specified thresholds	IC
<code>transceiver-threshold-auto</code>	Uses default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent	IC

Table 98: Interface Commands (Continued)

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

Interface Configuration

interface This command configures an interface type and enters interface configuration mode. Use the **no** form with a trunk to remove an inactive interface. Use the **no** form with a Layer 3 VLAN (normal type) to change it back to a Layer 2 interface.

Syntax

[no] interface *interface*

interface

ethernet *unit/port-list*

unit - Unit identifier. (Range: 1)

port-list - Physical port number or list of port numbers. Separate nonconsecutive port numbers with a comma and no spaces; or use a hyphen to designate a range of port numbers. (Range: 1-28)

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

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

Default Setting

None

Command Mode

Global Configuration

Example

To specify several different ports, enter the following command:

```
Console(config)#interface ethernet 1/17-20,23
Console(config-if)#
```

capabilities This command advertises the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

[no] **capabilities** {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol**}

1000full - Supports 1 Gbps full-duplex operation

100full - Supports 100 Mbps full-duplex operation

100half - Supports 100 Mbps half-duplex operation

10full - Supports 10 Mbps full-duplex operation

10half - Supports 10 Mbps half-duplex operation

flowcontrol - Supports flow control

Default Setting

1000BASE-T: 10half, 10full, 100half, 100full, 1000full

1000BASE-SX/LX/LHX/ZX (SFP): 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ 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 \(763\)](#)

[speed-duplex \(764\)](#)

[flowcontrol \(761\)](#)

description This command adds a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*

no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The description is displayed by the [show interfaces status](#) command and in the running-configuration file. An example of the value which a network manager might store in this object is the name of the manufacturer, and the product name.

Example

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

flowcontrol This command enables flow control. Use the **no** form to disable flow control.

Syntax

[no] **flowcontrol**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- ◆ Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.
- ◆ To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- ◆ When using the [negotiation](#) command to enable auto-negotiation, the optimal settings will be determined by the [capabilities](#) command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

[negotiation \(763\)](#)

[capabilities \(759\)](#)

history This command configures a periodic sampling of statistics, specifying the sampling interval and number of samples. Use the **no** form to remove a named entry from the sampling table.

Syntax

history *name interval buckets*

no history *name*

name - A symbolic name for this entry in the sampling table.
(Range: 1-32 characters)

interval - The interval for sampling statistics. (Range: 1-1440 minutes.)

buckets - The number of samples to take. (Range: 1-96)

Default Setting

15min - 15 minute interval, 96 buckets

1day - 1 day interval, 7 buckets

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example sets a interval of 15 minutes for sampling standard statistical values on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#history 15min 15 10
Console(config-if)#
```

media-type This command forces the transceiver mode to use for SFP ports. Use the **no** form to restore the default mode.

Syntax

media-type sfp-forced [*mode*]

no media-type

sfp-forced - Forces transceiver mode for the SFP port.

mode

1000sfp - Always uses 1000BASE SFP mode.

100fx - Always uses 100BASE-FX mode.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

Available sfp-forced modes include:

Ports 25-28 (1000BASE SFP) support 1000sfp, 100fx

Example

This forces the switch to use the 1000sfp mode for SFP port 28.

```
Console(config)#interface ethernet 1/28
Console(config-if)#media-type sfp-forced 1000sfp
Console(config-if)#
```

negotiation This command enables auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

Syntax

[no] **negotiation**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- ◆ When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the [capabilities](#) command. When auto-negotiation is disabled, you must manually specify the link attributes with the [speed-duplex](#) and [flowcontrol](#) commands.
- ◆ If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 10 to use auto-negotiation.

```
Console(config)#interface ethernet 1/10
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

[capabilities \(759\)](#)

[speed-duplex \(764\)](#)

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 \(763\)](#)

[capabilities \(759\)](#)

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)

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces brief This command displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type for all ports.

Command Mode

Privileged Exec

Command Usage

- ◆ If an SFP transceiver is inserted in a port, the Type field will show the SFP type as interpreted from Ethernet Compliance Codes (Data Byte 6 in Address A0h). The Ethernet Compliance Code is a bitmap value, of which one bit is supposedly turned on. However, if the read-out is not recognizable (e.g., 2 or more bits on, or all 0s), the Type field just displays the raw data (hexadecimal value).
- ◆ The Type field will always display "NA" for a trunk entry because a trunk allows for mixed port types such as 1000BASE-T and 1000BASE SFP.

Example

```
Console#show interfaces brief
Interface Name      Status    PVID Pri Speed/Duplex  Type           Trunk
-----
Eth 1/ 1           Down      1   0 Auto         1000BASE-T     None
Eth 1/ 2           Down      1   0 Auto         1000BASE-T     None
Eth 1/ 3           Down      1   0 Auto         1000BASE-T     None
Eth 1/ 4           Down      1   0 Auto         1000BASE-T     None
Eth 1/ 5           Down      1   0 Auto         1000BASE-T     None
Eth 1/ 6           Down      1   0 Auto         1000BASE-T     None
:
```

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

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

```
Console#show interfaces counters ethernet 1/1  
Ethernet 1/ 1  
===== IF table Stats =====  
2166458 Octets Input  
14734059 Octets Output  
14707 Unicast Input  
19806 Unicast Output  
0 Discard Input  
0 Discard Output  
0 Error Input  
===== Extended Iftable Stats =====  
23 Multi-cast Input  
5525 Multi-cast Output  
170 Broadcast Input  
11 Broadcast Output  
===== Ether-like Stats =====  
0 FCS Errors  
0 Single Collision Frames  
0 Multiple Collision Frames  
0 Deferred Transmissions  
0 Late Collisions  
0 Excessive Collisions  
0 Internal Mac Transmit Errors  
0 Frames Too Long  
0 Symbol Errors  
0 Pause Frames Input  
0 Pause Frames Output  
===== RMON Stats =====  
0 Drop Events  
16900558 Octets  
40243 Packets  
170 Broadcast PKTS  
23 Multi-cast PKTS  
0 Undersize PKTS
```

```

0 Oversize PKTS
0 Fragments
0 Jabbers
0 CRC Align Errors
0 Collisions
5271 Packet Size <= 64 Octets
3589 Packet Size 65 to 127 Octets
222 Packet Size 128 to 255 Octets
313 Packet Size 256 to 511 Octets
190 Packet Size 512 to 1023 Octets
444 Packet Size 1024 to 1518 Octets
===== Port Utilization =====
111 Octets Input in kbits per second
0 Packets Input per second
0.00 % Input Utilization
606 Octets Output in kbits per second
1 Packets Output per second
0.00 % Output Utilization
Console#

```

Table 99: show interfaces counters - display description

Parameter	Description
<i>IF Table Stats</i>	
Octets Input	The total number of octets received on the interface, including framing characters.
Octets Output	The total number of octets transmitted out of the interface, including framing characters.
Unicast Input	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Unicast Output	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Discard Input	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Discard Output	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Error Input	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
<i>Extended IF Table Stats</i>	
Multicast Input	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Multicast Output	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Broadcast Input	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Broadcast Output	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

Table 99: show interfaces counters - display description (Continued)

Parameter	Description
<i>Etherlike Statistics</i>	
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Symbol Errors	For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII
<i>RMON Statistics</i>	
Octets	Total number of octets of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Packets	The total number of packets (bad, broadcast and multicast) received.
Broadcast Packets	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Packets	The total number of good packets received that were directed to this multicast address.
Undersize Packets	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Packets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Table 99: show interfaces counters - display description (Continued)

Parameter	Description
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
CRC Align Errors	
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Octets	The total number of packets (including bad packets) received and transmitted that were less than 64 octets in length (excluding framing bits but including FCS octets).
65-127 Octets	The total number of packets (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
128-255 Octets	
256-511 Octets	
512-1023 Octets	
1024-1518 Octets	
Utilization Statistics	
Octets input per second	Number of octets entering this interface in kbits per second.
Packets input per second	Number of packets entering this interface in packets per second.
Input utilization	The input utilization rate for this interface.
Octets output per second	Number of octets leaving this interface in kbits per second.
Packets output per second	Number of packets leaving this interface in packets per second.
Output utilization	The output utilization rate for this interface.

show interfaces history This command displays periodic sampling of statistics, including the sampling interval, number of samples, and counter values.

Syntax

show interfaces history [*interface* [*name* [**current** | **previous** *index count*] [**input** | **output**]]]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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

name - Name of sample as defined in the [history](#) command.
(Range: 1-32 characters)

current - Statistics recorded in current interval.

previous - Statistics recorded in previous intervals.

index - An index into the buckets containing previous samples.
(Range: 1-96)

count - The number of historical samples to display. (Range: 1-96)

input - Ingress traffic.

output - Egress traffic.

Default Setting

Shows the historical settings and status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

```

Console#show interfaces history ethernet 1/1 15min
Interface      : Eth 1/ 1
Name           : 15min
Interval       : 900 second(s)
Buckets Requested : 96
Buckets Granted  : 1
Status         : Active

Current Entries

Start Time %      Octets Input  Unicast  Multicast  Broadcast
-----
00d 00:15:04  0.00          72675      524        35          41

Discards      Errors
-----
          41          0

%      Octets Output  Unicast  Multicast  Broadcast
-----
0.00          513760      653        336          0

Discards
-----
0

Previous Entries

Start Time %      Octets Input  Unicast  Multicast  Broadcast
-----
00d 00:00:03  0.66      80758067     106273     619717     69176

Start Time Discards      Errors
-----
00d 00:00:03          69176          2

Start Time %      Octets Output  Unicast  Multicast  Broadcast
-----
00d 00:00:03  0.00          677855      705        445          14

```

```

Start Time   Discards
-----
00d 00:00:03          0
Console#

```

show interfaces status This command displays the status for an interface.

Syntax

show interfaces status [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

```

Console#show interfaces status ethernet 1/1
Information of Eth 1/1
Basic Information:
  Port Type           : 1000BASE-T
  MAC Address         : 00-E0-0C-00-00-FE
Configuration:
  Name                :
  Port Admin          : Up
  Speed-duplex        : Auto
  Capabilities        : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm     : Enabled
  Broadcast Storm Limit : 500 packets/second
  Multicast Storm     : Disabled
  Multicast Storm Limit : 500 packets/second
  Unknown Unicast Storm : Disabled
  Unknown Unicast Storm Limit : 500 packets/second
  Flow Control        : Disabled
  LACP                : Disabled
  MAC Learning        : Enabled
  Link-up-down Trap   : Enabled
  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)

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

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 1.

```

Console#show interfaces switchport ethernet 1/1
Information of Eth 1/1
Broadcast Threshold           : Enabled, 500 packets/second
Multicast Threshold          : Disabled
Unknown Unicast Threshold    : Disabled
LACP Status                  : Disabled
Ingress Rate Limit           : Disabled, 1000M bits per second
Egress Rate Limit            : Disabled, 1000M bits per second
VLAN Membership Mode         : Hybrid
Ingress Rule                 : Disabled
Acceptable Frame Type        : All frames
Native VLAN                  : 1
Priority for Untagged Traffic : 0
Allowed VLAN                  :      1(u)
Forbidden VLAN                :
Console#

```

Table 100: 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 812).
Multicast Threshold	Shows if multicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 812).
Unknown Unicast Threshold	Shows if unknown unicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 812).
LACP Status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 790).
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 866).
Ingress Rule	Shows if ingress filtering is enabled or disabled (page 865).
Acceptable Frame Type	Shows if acceptable VLAN frames include all types or tagged frames only (page 863).
Native VLAN	Indicates the default Port VLAN ID (page 867).
Priority for Untagged Traffic	Indicates the default priority for untagged frames (page 884).
Allowed VLAN	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 864).
Forbidden VLAN	Shows the VLANs this interface can not join (page 858).

Transceiver Threshold Configuration

transceiver-monitor This command sends a trap when any of the transceiver's operational values fall outside of specified thresholds. Use the **no** form to disable trap messages.

Syntax

transceiver-monitor

Default Setting

Disabled

Command Mode

Interface Configuration (SFP Ports)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-monitor
Console#
```

transceiver-threshold-auto This command uses default threshold settings obtained from the transceiver to determine when an alarm or warning message should be sent. Use the **no** form to disable this feature.

Syntax

transceiver-threshold-auto

Default Setting

Enabled

Command Mode

Interface Configuration (SFP Ports)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold-auto
Console#
```

transceiver-threshold-current This command sets thresholds for transceiver current which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold current {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high current threshold for an alarm message.

high-warning – Sets the high current threshold for a warning message.

low-alarm – Sets the low current threshold for an alarm message.

low-warning – Sets the low current threshold for a warning message.

threshold-value – The threshold of the transceiver current.

(Range: 0-13100 in units of 0.01 mA)

Default Setting

High Alarm: 100 mA

High Warning: 90 mA

Low Warning: 7 mA

Low Alarm: 6 mA

Command Mode

Interface Configuration (SFP Ports)

Command Usage

- ◆ If trap messages are enabled with the [transceiver-monitor](#) command, and a high-threshold alarm or warning message is sent if the current value is greater than or equal to the threshold, and the last sample value was less than the

threshold. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the high threshold and reaches the low threshold.

- ◆ If trap messages are enabled with the [transceiver-monitor](#) command, and a low-threshold alarm or warning message is sent if the current value is less than or equal to the threshold, and the last sample value was greater than the threshold. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the low threshold and reaches the high threshold.
- ◆ Threshold events are triggered as described above to avoid a hysteresis effect which would continuously trigger event messages if the power level were to fluctuate just above and below either the high threshold or the low threshold.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the transceiver current at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold current low-alarm 100
Console(config-if)#transceiver-threshold rx-power high-alarm 700
Console#
```

transceiver-threshold rx-power This command sets thresholds for the transceiver power level of the received signal which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold rx-power {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high power threshold for an alarm message.

high-warning – Sets the high power threshold for a warning message.

low-alarm – Sets the low power threshold for an alarm message.

low-warning – Sets the low power threshold for a warning message.

threshold-value – The power threshold of the received signal.
(Range: -4000 - 820 in units of 0.01 dBm)

Default Setting

High Alarm: -3.00 dBm

High Warning: -3.50 dBm

Low Warning: -21.00 dBm

Low Alarm: -21.50 dBm

Command Mode

Interface Configuration (SFP Ports)

Command Usage

- ◆ The threshold value is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).
- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the signal power received at port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#transceiver-threshold rx-power low-alarm -21
Console(config-if)#transceiver-threshold rx-power high-alarm -3
Console#
```

transceiver-threshold temperature This command sets thresholds for the transceiver temperature which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold temperature {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high temperature threshold for an alarm message.

high-warning – Sets the high temperature threshold for a warning message.

low-alarm – Sets the low temperature threshold for an alarm message.

low-warning – Sets the low temperature threshold for a warning message.

threshold-value – The threshold of the transceiver temperature.
(Range: -12800 - 12800 in units of 0.01 Celsius)

Default Setting

High Alarm: 75.00 °C

High Warning: 70.00 °C

Low Alarm: -123.00 °C

Low Warning: 0.00 °C

Command Mode

Interface Configuration (SFP Ports)

Command Usage

- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the transceiver temperature at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold temperature low-alarm 97
Console(config-if)#transceiver-threshold temperature high-alarm -83
Console#
```

transceiver-threshold tx-power This command sets thresholds for the transceiver power level of the transmitted signal which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold tx-power {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high power threshold for an alarm message.

high-warning – Sets the high power threshold for a warning message.

low-alarm – Sets the low power threshold for an alarm message.

low-warning – Sets the low power threshold for a warning message.

threshold-value – The power threshold of the transmitted signal.
(Range: -4000 - 820 in units of 0.01 dBm)

Default Setting

High Alarm: -9.00 dBm
High Warning: -9.50 dBm
Low Warning: -11.50 dBm
Low Alarm: -12.00 dBm

Command Mode

Interface Configuration (SFP Ports)

Command Usage

- ◆ The threshold value is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).
- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.

- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the signal power transmitted at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold tx-power low-alarm 8
Console(config-if)#transceiver-threshold tx-power high-alarm -3
Console#
```

transceiver-threshold voltage This command sets thresholds for the transceiver voltage which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold voltage {high-alarm | high-warning | low-alarm | low-warning} threshold-value

high-alarm – Sets the high voltage threshold for an alarm message.

high-warning – Sets the high voltage threshold for a warning message.

low-alarm – Sets the low voltage threshold for an alarm message.

low-warning – Sets the low voltage threshold for a warning message.

threshold-value – The threshold of the transceiver voltage.
(Range: 0-655 in units of 0.01 Volt)

Default Setting

High Alarm: 3.50 Volts
High Warning: 3.45 Volts
Low Warning: 3.15 Volts
Low Alarm: 3.10 Volts

Command Mode

Interface Configuration (SFP Ports)

Command Usage

- ◆ Refer to the Command Usage section under the [transceiver-threshold current](#) command for more information on configuring transceiver thresholds.
- ◆ Trap messages enabled by the [transceiver-monitor](#) command are sent to any management station configured by the [snmp-server host](#) command.

Example

The following example sets alarm thresholds for the transceiver voltage at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold voltage low-alarm 4
Console(config-if)#transceiver-threshold voltage high-alarm 2
Console#
```

show interfaces transceiver This command displays identifying information for the specified transceiver, including connector type and vendor-related parameters, as well as the temperature, voltage, bias current, transmit power, and receive power.

Syntax

show interfaces transceiver [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 25-28)

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, and related alarm thresholds.

Example

```
Console#show interfaces transceiver ethernet 1/28
Information of Eth 1/28
Connector Type      : LC
Fiber Type          :
Eth Compliance Codes : 1
Baud Rate           : 1300 MBd
Vendor OUI          : 00-30-D3
Vendor Name         : OEM
Vendor PN           : M363B-20V7
Vendor Rev          :
Vendor SN           : J0110102
Date Code           : 11-01-24
```



```
DDM Info
DDM not supported
Console#
```

show interfaces transceiver-threshold This command Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power. Syntax

Syntax

show interfaces transceiver-threshold [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 25-28)

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, received optical power, and related alarm thresholds.
- ◆ The DDM thresholds displayed by this command only apply to ports which have a DDM-compliant transceiver inserted.

Example

```
Console#show interfaces transceiver-threshold ethernet 1/25
Information of Eth 1/25
DDM Thresholds
Transceiver-monitor      : Disabled
Transceiver-threshold-auto : Enabled
-----
Low Alarm  Low Warning  High Warning  High Alarm
-----
Temperature(Celsius)    -123.00      0.00        70.00       75.00
Voltage(Volts)          3.10        3.15        3.45        3.50
Current(mA)             6.00        7.00       90.00      100.00
TxPower(dBm)           -12.00     -11.50     -9.50       -9.00
RxPower(dBm)           -21.50     -21.00     -3.50       -3.00
Console#
```

Cable Diagnostics

test cable-diagnostics This command performs cable diagnostics on the specified port to diagnose any cable faults (short, open, etc.) and report the cable length.

Syntax

test cable-diagnostics dsp interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-24)

Command Mode

Privileged Exec

Command Usage

- ◆ Cable diagnostics are performed using Digital Signal Processing (DSP) test method when the port link-up speed is 1 Gbps. DSP analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse. If the port link-up speed is not 1 Gbps, then Time Domain Reflectometry (TDR) test method. TDR also detects a cable fault by sending a signal through the cable and reading the signal that is reflected back. However, note that TDR can only determine if a link is valid or faulty.
- ◆ This cable test is only accurate for Ethernet cables 7 - 100 meters long.
- ◆ The test takes approximately 5 seconds. Use the [show cable-diagnostics](#) command to display the results of the test, including common cable failures, as well as the status and approximate length of each cable pair.
- ◆ Ports are linked down while running cable diagnostics.
- ◆ To ensure more accurate measurement of the length to a fault, first disable power-saving mode (using the [no power-save](#) command) on the link partner before running cable diagnostics.

Example

```
Console#test cable-diagnostics interface ethernet 1/24
Console#
```

show cable-diagnostics This command shows the results of a cable diagnostics test.

Syntax

show cable-diagnostics dsp interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-24)

Command Mode

Privileged Exec

Command Usage

- ◆ The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found.
- ◆ For link-down ports, the reported distance to a fault is accurate to within +/- 2 meters. For link-up ports, the accuracy is +/- 10 meters.
- ◆ Potential conditions which may be listed by the diagnostics are shown by the legend in the following example. Additional information is provided for the following test results.
 - OK: Correctly terminated pair
 - ON: Open pair, no link partner
 - IE (Impedance mismatch): Terminating impedance is not in the reference range.
 - NS (Not Supported): This message is displayed for any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps.
 - UN: Unknown Error

Example

```
Console#show cable-diagnostics interface ethernet 1/24
Cable Diagnostics on interface Ethernet 1/1:
Cable Open with accuracy 0 meters.
  Pair A Open, length 2 meters
  Pair B Open, length 2 meters
  Pair C Short, length 0 meters
  Pair D Short, length 0 meters
Last Update On 2011-02-16 02:32:56
Console#
```

Power Savings

power-save This command enables power savings mode on the specified port. Use the **no** form to disable this feature.

Syntax

[no] **power-save**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet ports 1-24)

Command Usage

- ◆ IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can reduce power used for cable lengths of 60 meters or less, with more significant reduction for cables of 20 meters or less, and continue to ensure signal integrity.
- ◆ Power saving mode only applies to the Gigabit Ethernet ports using copper media.
- ◆ Power savings can be enabled on Gigabit Ethernet RJ-45 ports.
- ◆ The power-saving methods provided by this switch include:
 - Power saving when there is no link partner:

Under normal operation, the switch continuously auto-negotiates to find a link partner, keeping the MAC interface powered up even if no link connection exists. When using power-savings mode, the switch checks for energy on the circuit to determine if there is a link partner. If none is detected, the switch automatically turns off the transmitter, and most of the receive circuitry (entering Sleep Mode). In this mode, the low-power energy-detection circuit continuously checks for energy on the cable. If none is detected, the MAC interface is also powered down to save additional energy. If energy is detected, the switch immediately turns on both the transmitter and receiver functions, and powers up the MAC interface.
 - Power saving when there is a link partner:

Traditional Ethernet connections typically operate with enough power to support at least 100 meters of cable even though average network cable length is shorter. When cable length is shorter, power consumption can be reduced since signal attenuation is proportional to cable length. When power-savings mode is enabled, the switch analyzes cable length to

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



Note: Power savings can only be implemented on Gigabit Ethernet ports using twisted-pair cabling. Power-savings mode on a active link only works when connection speed is 1 Gbps, and line length is less than 60 meters.

Example

```
Console(config)#interface ethernet 1/8
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)

Command Mode

Privileged Exec

Example

```
Console#show power-save interface ethernet 1/8
Power Saving Status:
 Ethernet 1/8 : Enabled
Console#
```

Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to 8 trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 101: 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: 1-8)

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- ◆ Use **no channel-group** to remove a port group from a trunk.
- ◆ Use **no interface port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 10:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/10
Console(config-if)#channel-group 1
Console(config-if)#
```

Dynamic Configuration Commands

lacp This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

[no] lacp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- ◆ A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- ◆ If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- ◆ If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 1-3. Because LACP has also been enabled on the ports at the other end of the links, the [show interfaces status port-channel 1](#) command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/2
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/3
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic Information:
  Port Type           : 1000BASE-T
  MAC Address         : 12-34-12-34-12-3F
Configuration:
  Name                :
  Port Admin          : Up
  Speed-duplex        : Auto
  Capabilities        : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm     : Enabled
  Broadcast Storm Limit : 500 packets/second
```

```
Multicast Storm      : Disabled
Multicast Storm Limit : 500 packets/second
Unknown Unicast Storm : Disabled
Unknown Unicast Storm Limit : 500 packets/second
Storm Threshold Resolution : 1 packets/second
Flow Control         : Disabled
MAC Learning         : Enabled
Link-up-down Trap    : Enabled
Current status:
Created By           : LACP
Link Status          : Up
Port Operation Status : Up
Operation Speed-duplex : 1000full
Up Time              : 0w 0d 0h 0m 53s (53 seconds)
Flow Control Type    : None
Max Frame Size       : 1518 bytes (1522 bytes for tagged frames)
MAC Learning Status  : Enabled
Member Ports         : Eth1/1, Eth1/2, Eth1/3,
Active Member Ports  : Eth1/1, Eth1/2, Eth1/3,
Console#
```

lacp admin-key (Ethernet Interface) This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

Syntax

lacp {actor | partner} admin-key key

no lacp {actor | partner} admin-key

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

key - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

Default Setting

Actor: 1, Partner: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- ◆ If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.

- ◆ Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state.



Note: Configuring the partner admin-key does not affect remote or local switch operation. The local switch just records the partner admin-key for user reference.

- ◆ By default, the actor's operational key is determined by port's link speed (1000f - 4, 100f - 3, 10f - 2), and copied to the admin key.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp port-priority This command configures LACP port priority. Use the **no** form to restore the default setting.

Syntax

lacp {actor | partner} port-priority priority

no lacp {actor | partner} port-priority

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

priority - LACP port priority is used to select a backup link. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Setting a lower value indicates a higher effective priority.
- ◆ If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- ◆ If an LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace an existing port member that has a lower priority.

- ◆ Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

lacp system-priority This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

Syntax

lacp {actor | partner} system-priority *priority*

no lacp {actor | partner} system-priority

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

priority - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- ◆ Port must be configured with the same system priority to join the same LAG.
- ◆ System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- ◆ Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key This command configures a port channel's LACP administration key string. Use the
(Port Channel) **no** form to restore the default setting.

Syntax

lacp admin-key *key*

no lacp admin-key

key - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch.
(Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Port Channel)

Command Usage

- ◆ Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- ◆ If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.
- ◆ If the port channel admin key is set to a non-default value, the operational key is based upon LACP PDUs received from the partner, and the channel admin key is reset to the default value. The trunk identifier will also be changed by this process.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp timeout This command configures the timeout to wait for the next LACP data unit (LACPDU). Use the no form to restore the default setting.

Syntax

lacp timeout {long | short}

no lacp timeout

long - Specifies a slow timeout of 90 seconds.

short - Specifies a fast timeout of 3 seconds.

Default Setting

long

Command Mode

Interface Configuration (Port Channel)

Command Usage

- ◆ The timeout configured by this command is set in the LACP timeout bit of the Actor State field in transmitted LACPDU. When the partner switch receives an LACPDU set with a short timeout from the actor switch, the partner adjusts the transmit LACPDU interval to 1 second. When it receives an LACPDU set with a long timeout from the actor, it adjusts the transmit LACPDU interval to 30 seconds.
- ◆ If the actor does not receive an LACPDU from its partner before the configured timeout expires, the partner port information will be deleted from the LACP group.
- ◆ When a dynamic port-channel member leaves a port-channel, the default timeout value will be restored on that port.
- ◆ When a dynamic port-channel is torn down, the configured timeout value will be retained. When the dynamic port-channel is constructed again, that timeout value will be used.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp timeout short
Console(config-if)#
```

Trunk Status Display Commands

show lacp This command displays LACP information.

Syntax

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sysid**}

port-channel - Local identifier for a link aggregation group. (Range: 1-8)

counters - Statistics for LACP protocol messages.

internal - Configuration settings and operational state for local side.

neighbors - Configuration settings and operational state for remote side.

sysid - Summary of system priority and MAC address for all channel groups.

Default Setting

Port Channel: all

Command Mode

Privileged Exec

Example

```
Console#show lacp 1 counters
Port Channel: 1
Member Port           : Eth 1/24
LACPDU Sent           : 7
LACPDU Received       : 6
MarkerPDU Sent        : 0
MarkerPDU Received    : 0
MarkerResponsePDU Sent : 0
MarkerResponsePDU Received : 0
Unknown Packet Received : 0
Illegal Packet Received : 0
:
```

Table 102: show lacp counters - display description

Field	Description
LACPDU Sent	Number of valid LACPDU transmitted from this channel group.
LACPDU Received	Number of valid LACPDU received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
MarkerResponsePDU Sent	Number of valid MarkerResponse PDUs transmitted from this channel group.
MarkerResponsePDU Received	Number of valid MarkerResponse PDUs received by this channel group.

Table 102: show lacp counters - display description (Continued)

Field	Description
Unknown Packet Received	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Unknown Packet Received	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```

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

```

Table 103: show lacp internal - display description

Field	Description
Admin Key	Current administrative value of the key for the aggregation port.
Oper Key	Current operational value of the key for the aggregation port.
Timeout	Time to wait for the next LACPDU before deleting partner port information.
Periodic Time	Number of seconds before invalidating received LACPDU information.
System Priority	LACP system priority assigned to this port channel.
Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: ◆ 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 103: show lacp internal - display description (Continued)

Field	Description
Admin State, Oper State (continued)	◆ 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
-----
Member Port           : Eth 1/24
Partner Admin System ID : 32768, 00-00-00-00-00-00
Partner Oper System ID  : 32768, FC-0A-81-B7-C7-E0
Partner Admin Port ID   : 32768, 24
Partner Oper Port ID    : 32768, 24
Partner Admin Key        : 0
Partner Oper Key         : 4
Partner Admin State      : Defaulted, Distributing, Collecting,
                          Synchronization, Long Timeout, Passive LACP
Partner Oper State       : Distributing, Collecting, Synchronization,
                          Aggregatable, Long Timeout, Active LACP
:

```

Table 104: show lacp neighbors - display description

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

```

Console#show lacp sysid
Port Channel    System Priority    System MAC Address
-----
                32768      00-11-3B-8F-2C-A7
                32768      00-11-3B-8F-2C-A7
                32768      00-11-3B-8F-2C-A7

```

```

4          32768      00-11-3B-8F-2C-A7
5          32768      00-11-3B-8F-2C-A7
6          32768      00-11-3B-8F-2C-A7
7          32768      00-11-3B-D4-73-A0
8          32768      00-11-3B-D4-73-A0
9          32768      00-11-3B-D4-73-A0
10         32768      00-11-3B-D4-73-A0
11         32768      00-11-3B-D4-73-A0
12         32768      00-11-3B-D4-73-A0
:
```

Table 105: show lacp sysid - display description

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

show port-channel load-balance

This command shows the load-distribution method used on aggregated links.

Command Mode

Privileged Exec

Example

```

Console#show port-channel load-balance
Trunk Load Balance Mode: Destination IP address
Console#
```

Port Mirroring Commands

Data can be mirrored from a local port on the same switch or from a remote port on another switch for analysis at the target port using software monitoring tools or a hardware probe. This switch supports the following mirroring modes.

Table 106: 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 107: 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)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

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

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

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

Default Setting

- ◆ No mirror session is defined.
- ◆ When enabled for an interface, default mirroring is for both received and transmitted packets.
- ◆ When enabled for a VLAN or a MAC address, mirroring is restricted to received packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- ◆ You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- ◆ Set the destination port by specifying an Ethernet interface with the [interface](#) configuration command, and then use the [port monitor](#) command to specify the source of the traffic to mirror. Note that the destination port cannot be a trunk or trunk member port.
- ◆ When mirroring traffic from a port, the mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port. When mirroring traffic from a VLAN, traffic may also be dropped under heavy loads.
- ◆ When VLAN mirroring and port mirroring are both enabled, the target port can receive a mirrored packet twice; once from the source mirror port and again from the source mirror VLAN.
- ◆ When mirroring traffic from a MAC address, ingress traffic with the specified source address entering any port in the switch, other than the target port, will be mirrored to the destination port.
- ◆ Spanning Tree BPDU packets are not mirrored to the target port.
- ◆ When mirroring VLAN traffic or packets based on a source MAC address, the target port cannot be set to the same target port as that used for basic port mirroring.

- ◆ You can create multiple mirror sessions, but all sessions must share the same destination port.
- ◆ The destination port cannot be a trunk or trunk member port.
- ◆ ACL-based mirroring is only used for ingress traffic. To mirror an ACL, follow these steps:
 1. Use the **access-list** command to add an ACL.
 2. Use the **access-group** command to add a mirrored port to access control list.
 3. Use the **port monitor access-list** command to specify the destination port to which traffic matching the ACL will be mirrored.

Example

The following example configures the switch to mirror all packets from port 6 to 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

This example configures port 2 to monitor packets matching the MAC address 00-11-3B-XX-XX-XX received by port 1:

```
Console(config)#access-list mac m1
Console(config-mac-acl)#permit 00-11-3b-00-00-00 ff-ff-ff-00-00-00 any
Console(config-mac-acl)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#mac access-group m1 in
Console(config-if)#interface ethernet 1/2
Console(config-if)#port monitor access-list m1
Console(config-if)#
```

show port monitor This command displays mirror information.

Syntax

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

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

unit - Unit identifier. (Range: 1)

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

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

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

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

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-----
Destination Port (listen port) : Eth 1/12
Source Port (monitored Port)  : Eth 1/ 1
Mode                          : RX/TX
Console#
```

RSPAN Mirroring Commands

Remote Switched Port Analyzer (RSPAN) allows you to mirror traffic from remote switches for analysis on a local destination port.

Table 108: RSPAN Commands

Command	Function	Mode
<code>vlan rspan</code>	Creates a VLAN dedicated to carrying RSPAN traffic	VC
<code>rspan source</code>	Specifies the source port and traffic type to be mirrored	GC
<code>rspan destination</code>	Specifies the destination port to monitor the mirrored traffic	GC
<code>rspan remote vlan</code>	Specifies the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports	GC
<code>no rspan session</code>	Deletes a configured RSPAN session	GC
<code>show rspan</code>	Displays the configuration settings for an RSPAN session	PE

Configuration Guidelines

Take the following steps to configure an RSPAN session:

1. Use the `vlan rspan` command to configure a VLAN to use for RSPAN. (Default VLAN 1 is prohibited.)
2. Use the `rspan source` command to specify the interfaces and the traffic type (RX, TX or both) to be monitored.
3. Use the `rspan destination` command to specify the destination port for the traffic mirrored by an RSPAN session.
4. Use the `rspan remote vlan` command to specify the VLAN to be used for an RSPAN session, to specify the switch's role as a source, intermediate relay, or destination of the mirrored traffic, and to configure the uplink ports designated to carry this traffic.

RSPAN Limitations

The following limitations apply to the use of RSPAN on this switch:

- ◆ *RSPAN Ports* – Only ports can be configured as an RSPAN source, destination, or uplink; static and dynamic trunks are not allowed. A port can only be configured as one type of RSPAN interface – source, destination, or uplink. Also, note that the source port and destination port cannot be configured on the same switch.

Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN uplink or destination port – access ports are not allowed (see `switchport mode`).

- ◆ *Local/Remote Mirror* – The destination of a local mirror session (created with the `port monitor` command) cannot be used as the destination for RSPAN traffic.
- ◆ *Spanning Tree* – If the spanning tree is disabled, BPDUs will not be flooded onto the RSPAN VLAN.

MAC address learning is not supported on RSPAN uplink ports when RSPAN is enabled on the switch. Therefore, even if spanning tree is enabled after RSPAN has been configured, MAC address learning will still not be re-started on the RSPAN uplink ports.

- ◆ *IEEE 802.1X* – RSPAN and 802.1X are mutually exclusive functions. When 802.1X is enabled globally, RSPAN uplink ports cannot be configured, even though RSPAN source and destination ports can still be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally.

RSPAN uplink ports cannot be configured to use IEEE 802.1X Port Authentication, but RSPAN source ports and destination ports can be configured to use it

- ◆ *Port Security* – If port security is enabled on any port, that port cannot be set as an RSPAN uplink port, even though it can still be configured as an RSPAN source or destination port. Also, when a port is configured as an RSPAN uplink port, port security cannot be enabled on that port.

rspan source Use this command to specify the source port and traffic type to be mirrored remotely. Use the **no** form to disable RSPAN on the specified port, or with a traffic type keyword to disable mirroring for the specified type.

Syntax

[no] **rspan session** *session-id* **source interface** *interface-list* [**rx** | **tx** | **both**]

session-id – A number identifying this RSPAN session. (Range: 1-3)

Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.

interface-list – One or more source ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

Default Setting

Both TX and RX traffic is mirrored

Command Mode

Global Configuration

Command Usage

- ◆ One or more source ports can be assigned to the same RSPAN session, either on the same switch or on different switches.
- ◆ Only ports can be configured as an RSPAN source – static and dynamic trunks are not allowed.
- ◆ Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN source port – access ports are not allowed (see [switchport mode](#)).
- ◆ The source port and destination port cannot be configured on the same switch.

Example

The following example configures the switch to mirror received packets from port 2 and 3:

```
Console(config)#rspan session 1 source interface ethernet 1/2
Console(config)#rspan session 1 source interface ethernet 1/3
Console(config)#
```

rspan destination Use this command to specify the destination port to monitor the mirrored traffic. Use the **no** form to disable RSPAN on the specified port.

Syntax

rspan session *session-id* **destination interface** *interface* [**tagged** | **untagged**]

no rspan session *session-id* **destination interface** *interface*

session-id – A number identifying this RSPAN session. (Range: 1-3)

Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

tagged - Traffic exiting the destination port carries the RSPAN VLAN tag.

untagged - Traffic exiting the destination port is untagged.

Default Setting

Traffic exiting the destination port is untagged.

Command Mode

Global Configuration

Command Usage

- ◆ Only one destination port can be configured on the same switch per session, but a destination port can be configured on more than one switch for the same session.
- ◆ Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN destination port – access ports are not allowed (see [switchport mode](#)).
- ◆ Only ports can be configured as an RSPAN destination – static and dynamic trunks are not allowed.
- ◆ The source port and destination port cannot be configured on the same switch.

- ◆ A destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.

Example

The following example configures port 4 to receive mirrored RSPAN traffic:

```
Console(config)#rspan session 1 destination interface ethernet 1/2
Console(config)#
```

rspan remote vlan Use this command to specify the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports. Use the **no** form to disable the RSPAN on the specified VLAN.

Syntax

[no] **rspan session** *session-id* **remote vlan** *vlan-id*
{**source** | **intermediate** | **destination**} **uplink** *interface*

session-id – A number identifying this RSPAN session. (Range: 1-3)

Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.

vlan-id - ID of configured RSPAN VLAN. (Range: 1-4094)

Use the **vlan rspan** command to reserve a VLAN for RSPAN mirroring before enabling RSPAN with this command.

source - Specifies this device as the source of remotely mirrored traffic.

intermediate - Specifies this device as an intermediate switch, transparently passing mirrored traffic from one or more sources to one or more destinations.

destination - Specifies this device as a switch configured with a destination port which is to receive mirrored traffic for this session.

uplink - A port configured to receive or transmit remotely mirrored traffic.

interface - **ethernet** *unit/port*

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN uplink port – access ports are not allowed (see [switchport mode](#)).
- ◆ Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch.
- ◆ Only destination and uplink ports will be assigned by the switch as members of this VLAN. Ports cannot be manually assigned to an RSPAN VLAN with the [switchport allowed vlan](#) command. Also, note that the [show vlan](#) command will not display any members for an RSPAN VLAN, but will only show configured RSPAN VLAN identifiers.

Example

The following example enables RSPAN on VLAN 2, specifies this device as an RSPAN destination switch, and the uplink interface as port 3:

```
Console(config)#rspan session 1 remote vlan 2 destination uplink ethernet 1/3
Console(config)#
```

no rspan session Use this command to delete a configured RSPAN session.

Syntax

no rspan session *session-id*

session-id – A number identifying this RSPAN session. (Range: 1-3)

Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.

Command Mode

Global Configuration

Command Usage

The **no rspan session** command must be used to disable an RSPAN VLAN before it can be deleted from the VLAN database (see the [vlan](#) command).

Example

```
Console(config)#no rspan session 1
Console(config)#
```

show rspan Use this command to displays the configuration settings for an RSPAN session.

Syntax

show rspan session [*session-id*]

session-id – A number identifying this RSPAN session. (Range: 1)

Three sessions are allowed, including both local and remote mirroring, using different VLANs for RSPAN sessions.

Command Mode

Privileged Exec

Example

```
Console#show rspan session
RSPAN Session ID           : 1
Source Ports (mirrored ports) : None
  RX Only                  : None
  TX Only                  : None
  BOTH                     : None
Destination Port (monitor port) : Eth 1/2
Destination Tagged Mode      : Untagged
Switch Role                  : Destination
RSPAN VLAN                   : 2
RSPAN Uplink Ports           : Eth 1/3
Operation Status              : Up
Console#
```

Congestion Control Commands

The switch can set the maximum upload or download data transfer rate for any port. It can control traffic storms by setting a maximum threshold for broadcast traffic or multicast traffic. It can also set bounding thresholds for broadcast and multicast storms which can be used to automatically trigger rate limits or to shut down a port.

Table 109: Congestion Control Commands

Command Group	Function
Rate Limiting	Sets the input and output rate limits for a port.
Storm Control	Sets the traffic storm threshold for each port.

Rate Limit Commands

Rate limit commands allow the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped.

Table 110: Rate Limit Commands

Command	Function	Mode
rate-limit	Configures the maximum input or output rate for an interface	IC

rate-limit This command defines the rate limit for a specific interface. Use this command without specifying a rate to enable rate limiting. Use the **no** form to disable rate limiting.

Syntax

rate-limit {input | output} [*rate*]

no rate-limit {input | output}

input – Input rate for specified interface

output – Output rate for specified interface

rate – Maximum value in kbps.

(Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports;

64 - 10,000,000 kbits per second for 10 Gigabit Ethernet ports)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Using both rate limiting and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these commands on the same interface.

Example

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

Related Command

[show interfaces switchport \(773\)](#)

Storm Control Commands

Storm control commands can be used to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

Table 111: Rate Limit Commands

Command	Function	Mode
<code>switchport packet-rate</code>	Configures broadcast, multicast, and unknown unicast storm control thresholds	IC
<code>show interfaces switchport</code>	Displays the administrative and operational status of an interface	NE, PE

switchport packet-rate This command configures broadcast, multicast and unknown unicast storm control. Use the **no** form to restore the default setting.

Syntax

switchport {broadcast | multicast | unknown-unicast} packet-rate rate

no switchport {broadcast | multicast | unknown-unicast}

broadcast - Specifies storm control for broadcast traffic.

multicast - Specifies storm control for multicast traffic.

unknown-unicast - Specifies storm control for unknown unicast traffic.

rate - Threshold level as a rate; i.e. (Range: 500-262142 pps)

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.
- ◆ Using both rate limiting and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these commands on the same interface.

Example

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

Related Commands

[show interfaces switchport \(773\)](#)

Loopback Detection Commands

The switch can be configured to detect general loopback conditions caused by hardware problems or faulty protocol settings. When enabled, a control frame is transmitted on the participating ports, and the switch monitors inbound traffic to see if the frame is looped back.

Table 112: Loopback Detection Commands

Command	Function	Mode
<code>loopback-detection</code>	Enables loopback detection globally on the switch or on a specified interface	GC, IC
<code>loopback-detection action</code>	Specifies the response to take for a detected loopback condition	GC
<code>loopback-detection recover-time</code>	Specifies the interval to wait before releasing an interface from shutdown state	GC
<code>loopback-detection transmit-interval</code>	Specifies the interval at which to transmit loopback detection control frames	GC
<code>loopback detection trap</code>	Configures the switch to send a trap when a loopback condition is detected or the switch recover from a loopback	GC
<code>loopback-detection release</code>	Manually releases all interfaces currently shut down by the loopback detection feature	PE
<code>show loopback-detection</code>	Shows loopback detection configuration settings for the switch or for a specified interface	PE

Usage Guidelines

- ◆ The default settings for the control frame transmit interval and recover time may be adjusted to improve performance for your specific environment. The shutdown mode may also need to be changed once you determine what kind of packets are being looped back.
- ◆ General loopback detection provided by the commands described in this section and loopback detection provided by the spanning tree protocol cannot both be enabled at the same time. If loopback detection is enabled for the spanning tree protocol, general loopback detection cannot be enabled on the same interface.
- ◆ When a loopback event is detected on an interface or when an interface is released from a shutdown state caused by a loopback event, a trap message is sent and the event recorded in the system log.
- ◆ Loopback detection must be enabled both globally and on an interface for loopback detection to take effect.

loopback-detection This command enables loopback detection globally on the switch or on a specified interface. Use the **no** form to disable loopback detection.

Syntax

[no] loopback-detection

Default Setting

Enabled

Command Mode

Global Configuration

Interface Configuration (Ethernet, Port Channel)

Command Usage

Loopback detection must be enabled globally for the switch by this command and enabled for a specific interface for this function to take effect.

Example

This example enables general loopback detection on the switch, disables loopback detection provided for the spanning tree protocol on port 1, and then enables general loopback detection for that port.

```
Console(config)#loopback-detection
Console(config)#interface ethernet 1/1
Console(config-if)#no spanning-tree loopback-detection
Console(config-if)#loopback-detection
Console(config)#
```

loopback-detection action This command specifies the protective action the switch takes when a loopback condition is detected. Use the **no** form to restore the default setting.

Syntax

loopback-detection action {none | shutdown}

no loopback-detection action

none - No action is taken.

shutdown - Shuts down the interface.

Default Setting

Shut down

Command Mode

Global Configuration

Command Usage

- ◆ When a port receives a control frame sent by itself, this means that the port is in looped state, and the VLAN in the frame payload is also in looped state with the wrong VLAN tag. The looped port is therefore shut down.
- ◆ Use the `loopback-detection recover-time` command to set the time to wait before re-enabling an interface shut down by the loopback detection process.
- ◆ When the loopback detection response is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.

Example

This example sets the loopback detection mode to shut down user traffic.

```
Console(config)#loopback-detection action shutdown
Console(config)#
```

**loopback-detection
recover-time**

This command specifies the interval to wait before the switch automatically releases an interface from shutdown state. Use the **no** form to restore the default setting.

Syntax

loopback-detection recover-time *seconds*

no loopback-detection recover-time

seconds - Recovery time from shutdown state. (Range: 60-1,000,000 seconds, or 0 to disable automatic recovery)

Default Setting

60 seconds

Command Mode

Global Configuration

Command Usage

- ◆ When the loopback detection mode is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.
- ◆ If the recovery time is set to zero, all ports placed in shutdown state can be restored to operation using the `loopback-detection release` command. To restore a specific port, use the `no shutdown` command.

Example

```
Console(config)#loopback-detection recover-time 120
Console(config-if)#
```

loopback-detection transmit-interval This command specifies the interval at which to transmit loopback detection control frames. Use the **no** form to restore the default setting.

Syntax

loopback-detection transmit-interval *seconds*

no loopback-detection transmit-interval

seconds - The transmission interval for loopback detection control frames.
(Range: 1-32767 seconds)

Default Setting

10 seconds

Command Mode

Global Configuration

Example

```
Console(config)#loopback-detection transmit-interval 60
Console(config)#
```

loopback detection trap This command sends a trap when a loopback condition is detected, or when the switch recovers from a loopback condition. Use the **no** form to restore the default state.

Syntax

loopback-detection trap [**both** | **detect** | **none** | **recover**]

no loopback-detection trap

both - Sends an SNMP trap message when a loopback condition is detected, or when the switch recovers from a loopback condition.

detect - Sends an SNMP trap message when a loopback condition is detected.

none - Does not send an SNMP trap for loopback detection or recovery.

recover - Sends an SNMP trap message when the switch recovers from a loopback condition.

Default Setting

None

Command Mode

Global Configuration

Command Usage

Refer to the [loopback-detection recover-time](#) command for information on conditions which constitute loopback recovery.

Example

```
Console(config)#loopback-detection trap both
Console(config)#
```

loopback-detection release This command releases all interfaces currently shut down by the loopback detection feature.

Syntax**loopback-detection release****Command Mode**

Privileged Exec

Example

```
Console#loopback-detection release
Console(config)#
```

show loopback-detection This command shows loopback detection configuration settings for the switch or for a specified interface.

Syntax**show loopback-detection** [*interface*]*interface***ethernet** *unit/port**unit* - Unit identifier. (Range: 1-8)*port* - Port number. (Range: 1-28)**Command Mode**

Privileged Exec

Example

```
Console#show loopback-detection
Loopback Detection Global Information
Global Status      : Enabled
Transmit Interval  : 10
```

```
Recover Time      : 60
Action            : Shutdown
Trap              : None
Loopback Detection Port Information
Port      Admin State Oper State
-----
Eth 1/ 1   Enabled     Normal
Eth 1/ 2   Disabled    Disabled
Eth 1/ 3   Disabled    Disabled
:
Console#show loopback-detection ethernet 1/1
Loopback Detection Information of Eth 1/1
Admin State : Enabled
Oper State  : Normal
Looped VLAN : None
Console#
```

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Table 113: Address Table Commands

Command	Function	Mode
<code>mac-address-table aging-time</code>	Sets the aging time of the address table	GC
<code>mac-address-table static</code>	Maps a static address to a port in a VLAN	GC
<code>clear collision-mac-address-table</code>	Removes all entries from the collision MAC address table	PE
<code>clear mac-address-table dynamic</code>	Removes any learned entries from the forwarding database	PE
<code>show collision-mac-address-table</code>	Shows a shows a list of MAC addresses that cannot be learned by the switch due to hash collisions	PE
<code>show mac-address-table</code>	Displays entries in the bridge-forwarding database	PE
<code>show mac-address-table aging-time</code>	Shows the aging time for the address table	PE
<code>show mac-address-table count</code>	Shows the number of MAC addresses used and the number of available MAC addresses	PE

mac-address-table aging-time This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*

no mac-address-table aging-time

seconds - Aging time. (Range: 6-7200 seconds; 0 to disable aging)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

mac-address-table static This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

mac-address - MAC address.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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

action -

delete-on-reset - Assignment lasts until the switch is reset.

permanent - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- ◆ Static addresses will not be removed from the address table when a given interface link is down.
- ◆ Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- ◆ A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
1/1 vlan 1 delete-on-reset
Console(config)#
```

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

Default Setting

None

Command Mode

Privileged Exec

Example

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

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Even if a hash collision for a MAC address is resolved, entries in collision MAC address table are not removed until this command is issued to reset the table, or the system is reset.

Example

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

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

Command Mode

Privileged Exec

Example

```

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

```

show mac-address-table This command shows classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

mac-address - MAC address.

mask - Bits to match in the address.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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

sort - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
 - Learn - Dynamic address entries
 - Config - Static entry
 - Security - Port Security
- ◆ The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit "0" means to match a bit and "1" means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."
- ◆ The maximum number of address entries is 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)

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

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table count interface ethernet 1/1

MAC Entries for Eth 1/1
Total Address Count      :0
Static Address Count     :0
Dynamic Address Count    :0

Console#show mac-address-table count

Compute the number of MAC Address...

Maximum number of MAC Address which can be created in the system:
Total Number of MAC Address      : 16384
Number of Static MAC Address     : 1024

Current number of entries which have been created in the system:
Total Number of MAC Address      : 3
Number of Static MAC Address     : 1
Number of Dynamic MAC Address    : 2
Console#
```

Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Table 114: Spanning Tree Commands

Command	Function	Mode
<code>spanning-tree</code>	Enables the spanning tree protocol	GC
<code>spanning-tree cisco-prestandard</code>	Configures spanning tree operation to be compatible with Cisco prestandard versions	GC
<code>spanning-tree forward-time</code>	Configures the spanning tree bridge forward time	GC
<code>spanning-tree hello-time</code>	Configures the spanning tree bridge hello time	GC
<code>spanning-tree max-age</code>	Configures the spanning tree bridge maximum age	GC
<code>spanning-tree mode</code>	Configures STP, RSTP or MSTP mode	GC
<code>spanning-tree mst configuration</code>	Changes to MSTP configuration mode	GC
<code>spanning-tree pathcost method</code>	Configures the path cost method for RSTP/MSTP	GC
<code>spanning-tree priority</code>	Configures the spanning tree bridge priority	GC
<code>spanning-tree system-bpdu-flooding</code>	Floods BPDUs to all other ports or just to all other ports in the same VLAN when global spanning tree is disabled	GC
<code>spanning-tree transmission-limit</code>	Configures the transmission limit for RSTP/MSTP	GC
<code>max-hops</code>	Configures the maximum number of hops allowed in the region before a BPDU is discarded	MST
<code>mst priority</code>	Configures the priority of a spanning tree instance	MST
<code>mst vlan</code>	Adds VLANs to a spanning tree instance	MST
<code>name</code>	Configures the name for the multiple spanning tree	MST
<code>revision</code>	Configures the revision number for the multiple spanning tree	MST
<code>spanning-tree bpdu-filter</code>	Filters BPDUs for edge ports	IC
<code>spanning-tree bpdu-guard</code>	Shuts down an edge port if it receives a BPDU	IC
<code>spanning-tree cost</code>	Configures the spanning tree path cost of an interface	IC
<code>spanning-tree edge-port</code>	Enables fast forwarding for edge ports	IC
<code>spanning-tree link-type</code>	Configures the link type for RSTP/MSTP	IC
<code>spanning-tree loopback-detection</code>	Enables BPDU loopback detection for a port	IC

Table 114: Spanning Tree Commands (Continued)

Command	Function	Mode
<code>spanning-tree loopback-detection action</code>	Configures the response for loopback detection to block user traffic or shut down the interface	IC
<code>spanning-tree loopback-detection release-mode</code>	Configures loopback release mode for a port	IC
<code>spanning-tree loopback-detection trap</code>	Enables BPDU loopback SNMP trap notification for a port	IC
<code>spanning-tree mst cost</code>	Configures the path cost of an instance in the MST	IC
<code>spanning-tree mst port-priority</code>	Configures the priority of an instance in the MST	IC
<code>spanning-tree port-bpdu-flooding</code>	Floods BPDUs to other ports when global spanning tree is disabled	IC
<code>spanning-tree port-priority</code>	Configures the spanning tree priority of an interface	IC
<code>spanning-tree root-guard</code>	Prevents a designated port from passing superior BPDUs	IC
<code>spanning-tree spanning-disabled</code>	Disables spanning tree for an interface	IC
<code>spanning-tree tc-prop-stop</code>	Stops propagation of topology change information	IC
<code>spanning-tree loopback-detection release</code>	Manually releases a port placed in discarding state by loopback-detection	PE
<code>spanning-tree protocol-migration</code>	Re-checks the appropriate BPDU format	PE
<code>show spanning-tree</code>	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE
<code>show spanning-tree mst configuration</code>	Shows the multiple spanning tree configuration	PE
<code>show spanning-tree tc-prop</code>	Shows configuration of topology change propagation domains	PE

spanning-tree This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

[no] spanning-tree

Default Setting

Spanning tree is disabled.

Command Mode

Global Configuration

Command Usage

- ◆ The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This

allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

- ◆ When spanning tree is enabled globally by this command or enabled on an interface ([spanning-tree spanning-disabled](#) command), loopback detection is disabled.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree cisco-prestandard This command configures spanning tree operation to be compatible with Cisco prestandard versions. Use the **no** form to restore the default setting.

[no] spanning-tree cisco-prestandard

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Cisco prestandard versions prior to Cisco IOS Release 12.2(25)SEC do not fully follow the IEEE standard, causing some state machine procedures to function incorrectly. The command forces the spanning tree protocol to function in a manner compatible with Cisco prestandard versions.

Example

```
Console(config)#spanning-tree cisco-prestandard
Console(config)#
```

spanning-tree forward-time This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)

The minimum value is the higher of 4 or $[(\text{max-age} / 2) + 1]$.

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a port will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*

no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).

The maximum value is the lower of 10 or $[(\text{max-age} / 2) - 1]$.

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

Related Commands

[spanning-tree forward-time \(828\)](#)

[spanning-tree max-age \(830\)](#)

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 \(828\)](#)

[spanning-tree hello-time \(829\)](#)

spanning-tree mode This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {**stp** | **rstp** | **mstp**}

no spanning-tree mode

stp - Spanning Tree Protocol (IEEE 802.1D)

rstp - Rapid Spanning Tree Protocol (IEEE 802.1w)

mstp - Multiple Spanning Tree (IEEE 802.1s)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- ◆ **Spanning Tree Protocol**
This option uses RSTP set to STP forced compatibility mode. It uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.
- ◆ **Rapid Spanning Tree Protocol**
RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
 - **STP Mode** – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
 - **RSTP Mode** – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.
- ◆ **Multiple Spanning Tree Protocol**
 - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
 - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
 - Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

**spanning-tree
mst configuration**

This command changes to Multiple Spanning Tree (MST) configuration mode.

Default Setting

No VLANs are mapped to any MST instance.
The region name is set the switch's MAC address.

Command Mode

Global Configuration

Example

```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

Related Commands

[mst vlan \(837\)](#)
[mst priority \(836\)](#)
[name \(838\)](#)
[revision \(838\)](#)
[max-hops \(836\)](#)

**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 841](#)) takes precedence over port priority ([page 848](#)).

- ◆ The path cost methods apply to all spanning tree modes (STP, RSTP and MSTP). Specifically, the long method can be applied to STP since this mode is supported by a backward compatible mode of RSTP.

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree priority This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

priority - Priority of the bridge. (Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40960
Console(config)#
```

spanning-tree system-bpdu-flooding This command configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port. Use the **no** form to restore the default.

Syntax

spanning-tree system-bpdu-flooding {to-all | to-vlan}

no spanning-tree system-bpdu-flooding

to-all - Floods BPDUs to all other ports on the switch.

to-vlan - Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID).

Default Setting

Floods to all other ports in the same VLAN.

Command Mode

Global Configuration

Command Usage

The **spanning-tree system-bpdu-flooding** command has no effect if BPDU flooding is disabled on a port (see the [spanning-tree port-bpdu-flooding](#) command).

Example

```
Console(config)#spanning-tree system-bpdu-flooding
Console(config)#
```

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

Syntax

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

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

interface - *unit/port*

unit - Unit identifier. (Range: 1)

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

trunk-id - Trunk index (Range: 1-8)

Default Setting

All ports and trunks belong to a common group.

Command Mode

Global Configuration

Command Usage

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

Example

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

**spanning-tree
transmission-limit**

This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

max-hops This command configures the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

Syntax

max-hops *hop-number*

hop-number - Maximum hop number for multiple spanning tree.
(Range: 1-40)

Default Setting

20

Command Mode

MST Configuration

Command Usage

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Example

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

mst priority This command configures the priority of a spanning tree instance. Use the **no** form to restore the default.

Syntax

mst *instance-id* **priority** *priority*

no mst *instance-id* **priority**

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

priority - Priority of the a spanning tree instance.

(Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

MST Configuration

Command Usage

- ◆ MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- ◆ You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

Example

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

mst vlan This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

Syntax

[no] **mst** *instance-id* **vlan** *vlan-range*

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

vlan-range - Range of VLANs. (Range: 1-4094)

Default Setting

none

Command Mode

MST Configuration

Command Usage

- ◆ Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.
- ◆ By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 64 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region ([page 838](#)) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

Example

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

name This command configures the name for the multiple spanning tree region in which this switch is located. Use the **no** form to clear the name.

Syntax

name *name*

name - Name of multiple spanning tree region. (Range: 1-32 alphanumeric characters)

Default Setting

Switch's MAC address

Command Mode

MST Configuration

Command Usage

The MST region name and revision number ([page 838](#)) 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 \(838\)](#)

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 838) 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 \(838\)](#)

spanning-tree bpd-filter This command allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. Use the **no** form to disable this feature.

Syntax

[no] spanning-tree bpd-filter

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command stops all Bridge Protocol Data Units (BPDUs) from being transmitted on configured edge ports to save CPU processing time. This function is designed to work in conjunction with edge ports which should only connect end stations to the switch, and therefore do not need to process BPDUs. However, note that if a trunking port connected to another switch or bridging device is mistakenly configured as an edge port, and BPDU filtering is enabled on this port, this might cause a loop in the spanning tree.
- ◆ BPDU filter can only be configured on an interface if the edge port attribute is not disabled (that is, if edge port is set to enabled or auto with the [spanning-tree edge-port](#) command).

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpd-filter
Console(config-if)#
```

Related Commands

[spanning-tree edge-port \(842\)](#)

spanning-tree bpduguard This command shuts down an edge port (i.e., an interface set for fast forwarding) if it receives a BPDU. Use the **no** form without any keywords to disable this feature, or with a keyword to restore the default settings.

Syntax

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

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

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

interval - The time to wait before re-enabling an interface. (Range: 30-86400 seconds)

Default Setting

BPDU Guard: Disabled

Auto-Recovery: Disabled

Auto-Recovery Interval: 300 seconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ An edge port should only be connected to end nodes which do not generate BPDUs. If a BPDU is received on an edge port, this indicates an invalid network configuration, or that the switch may be under attack by a hacker. If an interface is shut down by BPDU Guard, it must be manually re-enabled using the **no spanning-tree spanning-disabled** command if the auto-recovery interval is not specified.
- ◆ BPDU guard can only be configured on an interface if the edge port attribute is not disabled (that is, if edge port is set to enabled or auto with the **spanning-tree edge-port** command).

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpduguard
Console(config-if)#
```

Related Commands

spanning-tree edge-port (842)

spanning-tree spanning-disabled (850)

spanning-tree cost This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default auto-configuration mode.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

cost - The path cost for the port. (Range: 0 for auto-configuration, 1-65535 for short path cost method, 1-200,000,000 for long path cost method)¹⁸

Table 115: Recommended STA Path Cost Range

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (IEEE 802.1D-2004)
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 116: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (IEEE 802.1D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.

18. Use the [spanning-tree pathcost method](#) command to set the path cost method. The range displayed in the CLI prompt message shows the maximum value for path cost. However, note that the switch still enforces the rules for path cost based on the specified path cost method (long or short).

- ◆ Path cost takes precedence over port priority.
- ◆ When the path cost method ([page 832](#)) is set to short, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree edge-port This command specifies an interface as an edge port. Use the **no** form to restore the default.

Syntax

spanning-tree edge-port [auto]

no spanning-tree edge-port

auto - Automatically determines if an interface is an edge port.

Default Setting

Auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related time out problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- ◆ When edge port is set as auto, the operational state is determined automatically by the Bridge Detection State Machine described in 802.1D-2004, where the edge port state may change dynamically based on environment changes (e.g., receiving a BPDU or not within the required interval).

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

spanning-tree link-type This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}

no spanning-tree link-type

auto - Automatically derived from the duplex mode setting.

point-to-point - Point-to-point link.

shared - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- ◆ When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- ◆ RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree loopback-detection This command enables the detection and response to Spanning Tree loopback BPDUs on the port. Use the **no** form to disable this feature.

Syntax

[no] spanning-tree loopback-detection

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If Port Loopback Detection is not enabled and a port receives its own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- ◆ Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

**spanning-tree
loopback-detection
action**

This command configures the response for loopback detection to shut down the interface. Use the **no** form to restore the default.

Syntax

spanning-tree loopback-detection action {block | shutdown *duration*}

no spanning-tree loopback-detection action

shutdown - Shuts down the interface.

duration - The duration to shut down the interface.
(Range: 60-86400 seconds)

Default Setting

shutdown, 60 seconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If an interface is shut down by this command, and the release mode is set to "auto" with the [spanning-tree loopback-detection release-mode](#) command, the selected interface will be automatically enabled when the shutdown interval has expired.
- ◆ If an interface is shut down by this command, and the release mode is set to "manual," the interface can be re-enabled using the [spanning-tree loopback-detection release](#) command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection action shutdown 600
Console(config-if)#
```


spanning-tree loopback-detection release-mode This command configures the release mode for a port that was placed in the discarding state because a loopback BPDU was received. Use the **no** form to restore the default.

Syntax

spanning-tree loopback-detection release-mode {auto | manual}

no spanning-tree loopback-detection release-mode

auto - Allows a port to automatically be released from the discarding state when the loopback state ends.

manual - The port can only be released from the discarding state manually.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If the port is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:
 - The port receives any other BPDU except for its own, or;
 - The port's link status changes to link down and then link up again, or;
 - The port ceases to receive its own BPDUs in a forward delay interval.
- ◆ If Port Loopback Detection is not enabled and a port receives its own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- ◆ Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.
- ◆ When configured for manual release mode, then a link down / up event will not release the port from the discarding state. It can only be released using the **spanning-tree loopback-detection release** command.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode manual
Console(config-if)#
```

spanning-tree loopback-detection trap This command enables SNMP trap notification for Spanning Tree loopback BPDU detections. Use the **no** form to restore the default.

Syntax

[no] spanning-tree loopback-detection trap

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

spanning-tree 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 method¹⁹, 1-200,000,000 for long path cost method)

The recommended path cost range is listed in [Table 115 on page 841](#).

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 116 on page 841](#).

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Each spanning-tree instance is associated with a unique set of VLAN IDs.
- ◆ This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to

¹⁹. Use the [spanning-tree pathcost method](#) command to set the path cost method.

interfaces attached to faster media, and higher values assigned to interfaces with slower media.

- ◆ Use the **no spanning-tree mst cost** command to specify auto-configuration mode.
- ◆ Path cost takes precedence over interface priority.

Example

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

Related Commands

[spanning-tree mst port-priority \(847\)](#)

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 \(846\)](#)**spanning-tree
port-bpdu-flooding**

This command floods BPDUs to other ports when spanning tree is disabled globally or disabled on a specific port. Use the **no** form to restore the default setting.

Syntax

[no] spanning-tree port-bpdu-flooding

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port's native VLAN as specified by the [spanning-tree system-bpdu-flooding](#) command.
- ◆ The [spanning-tree system-bpdu-flooding](#) command has no effect if BPDU flooding is disabled on a port by the **spanning-tree port-bpdu-flooding** command.

Example

```

Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-bpdu-flooding
Console(config-if)#

```

**spanning-tree
port-priority**

This command configures the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- ◆ Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
- ◆ The criteria used for determining the port role is based on root bridge ID, root path cost, designated bridge, designated port, port priority, and port number, in that order and as applicable to the role under question.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands

[spanning-tree cost \(841\)](#)

spanning-tree root-guard This command prevents a designated port from taking superior BPDUs into account and allowing a new STP root port to be elected. Use the **no** form to disable this feature.

Syntax

[no] spanning-tree root-guard

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ A bridge with a lower bridge identifier (or same identifier and lower MAC address) can take over as the root bridge at any time.
- ◆ When Root Guard is enabled, and the switch receives a superior BPDU on this port, it is set to the Discarding state until it stops receiving superior BPDUs for a fixed recovery period. While in the discarding state, no traffic is forwarded across the port.
- ◆ Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It

could also be used to form a border around part of the network where the root bridge is allowed.

- ◆ When spanning tree is initialized globally on the switch or on an interface, the switch will wait for 20 seconds to ensure that the spanning tree has converged before enabling Root Guard.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

spanning-tree spanning-disabled This command disables the spanning tree algorithm for the specified interface. Use the **no** form to re-enable the spanning tree algorithm for the specified interface.

Syntax

[no] spanning-tree spanning-disabled

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When spanning tree is enabled globally (**spanning-tree** command) or enabled on an interface by this command, loopback detection is disabled.

Example

This example disables the spanning tree algorithm for port 5.

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

spanning-tree tc-prop-stop This command stops the propagation of topology change notifications (TCN). Use the **no** form to allow propagation of TCN messages.

Syntax

[no] spanning-tree tc-prop-stop

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When this command is enabled on an interface, topology change information originating from the interface will still be propagated.

This command should not be used on an interface which is purposely configured in a ring topology.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#spanning-tree tc-prop-stop
Console(config-if)#
```

**spanning-tree
loopback-detection
release**

This command manually releases a port placed in discarding state by loopback-detection.

Syntax

spanning-tree loopback-detection release *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Command Mode

Privileged Exec

Command Usage

Use this command to release an interface from discarding state if loopback detection release mode is set to "manual" by the [spanning-tree loopback-detection release-mode](#) command and BPDU loopback occurs.

Example

```
Console#spanning-tree loopback-detection release ethernet 1/1
Console#
```

spanning-tree protocol-migration This command re-checks the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console#spanning-tree protocol-migration ethernet 1/5
Console#
```

show spanning-tree This command shows the configuration for the common spanning tree (CST), for all instances within the multiple spanning tree (MST), or for a specific instance within the multiple spanning tree (MST).

Syntax

show spanning-tree [*interface* | **mst** *instance-id* | **brief** | **stp-enabled-only**]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

instance-id - Instance identifier of the multiple spanning tree.
(Range: 0-4094)

brief - Shows a summary of global and interface settings.

stp-enabled-only - Displays global settings, and settings for interfaces for which STP is enabled.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.
- ◆ Use the **show spanning-tree interface** command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- ◆ Use the **show spanning-tree mst** command to display the spanning tree configuration for all instances within the Multiple Spanning Tree (MST), including global settings and settings for active interfaces.
- ◆ Use the **show spanning-tree mst instance-id** command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST), including global settings and settings for all interfaces.

Example

```

Console#show spanning-tree
Spanning Tree Information
-----
Spanning Tree Mode           : RSTP
Spanning Tree Enabled/Disabled : Disabled
Instance                     : 0
VLANs Configured             : 1-4094
Priority                     : 32768
Bridge Hello Time (sec.)     : 2
Bridge Max. Age (sec.)       : 20
Bridge Forward Delay (sec.)  : 15
Root Hello Time (sec.)       : 2
Root Max. Age (sec.)         : 20
Root Forward Delay (sec.)    : 15
Max. Hops                     : 20
Remaining Hops               : 20
Designated Root              : 32768.CC37ABD7A684
Current Root Port            : 0
Current Root Cost             : 0
Number of Topology Changes   : 0
Last Topology Change Time (sec.): 96853
Transmission Limit           : 3
Path Cost Method              : Long
Flooding Behavior             : To VLAN
Console#

```

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 : Disabled
Designated Root              : 32768.CC37ABD7A684
Current Root Port            : 0
Current Root Cost             : 0

Interface Pri Designated      Designated Oper    STP   Role State Oper
              Bridge ID        Port ID   Cost    Status  Role State Oper
-----
Eth 1/ 1  128 32768.CC37ABD7A684 128.1      10000 EN    DISB BLK No
Eth 1/ 2  128 32768.CC37ABD7A684 128.2      10000 EN    DISB FWD No
Eth 1/ 3  128 32768.CC37ABD7A684 128.3      10000 EN    DISB BLK No
Eth 1/ 4  128 32768.CC37ABD7A684 128.4      10000 EN    DISB BLK No
Eth 1/ 5  128 32768.CC37ABD7A684 128.5      10000 EN    DISB BLK No
Eth 1/ 6  128 32768.CC37ABD7A684 128.6      10000 EN    DISB BLK No
Eth 1/ 7  128 32768.CC37ABD7A684 128.7      10000 EN    DISB BLK No
Eth 1/ 8  128 32768.CC37ABD7A684 128.8      10000 EN    DISB BLK No
Eth 1/ 9  128 32768.CC37ABD7A684 128.9      10000 EN    DISB BLK No
Eth 1/10  128 32768.CC37ABD7A684 128.10     10000 EN    DISB BLK No
Console#

```

show spanning-tree mst configuration This command shows the configuration of the multiple spanning tree.

Command Mode

Privileged Exec

Example

```

Console#show spanning-tree mst configuration
Mstp Configuration Information
-----
Configuration Name : R&D
Revision Level      :0

Instance VLANs
-----
0      1-4094
Console#

```

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

Syntax

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

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

Command Mode

Privileged Exec

Example

```
Console#show spanning-tree tc-prop group 1
  Group 1
    Eth 1/ 1, Eth 1/ 2, Eth 1/ 3, Eth 1/ 4, Eth 1/ 5
Console#
```

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Table 117: VLAN Commands

Command Group	Function
Bridge Extension Commands	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, and PVID
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses
Configuring Protocol-based VLANs	Configures protocol-based VLANs based on frame type and protocol
Configuring Voice VLANs	Configures VoIP traffic detection and enables a Voice VLAN

Bridge Extension Commands

This section describes how to display default configuration settings for the Bridge Extension MIB.

Table 118: Bridge Extension Commands

Command	Function	Mode
<code>switchport forbidden vlan</code>	Configures forbidden VLANs for an interface	IC
<code>show bridge-ext</code>	Shows the global bridge extension configuration	PE

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

Syntax

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

no garp timer {join | leave | leaveall}

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

timer-value - Value of timer.

Ranges:

join: 20-1000 centiseconds

leave: 60-3000 centiseconds

leaveall: 500-18000 centiseconds

Default Setting

join: 20 centiseconds

leave: 60 centiseconds

leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

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



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

Example

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

Related Commands

[show garp timer \(859\)](#)

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

Syntax

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

no switchport forbidden vlan

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

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

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command prevents a VLAN from being added to the specified interface.
- ◆ 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.
- ◆ This command will not be accepted if the specified VLAN does not exist on the switch.

Example

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

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

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

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show bridge-ext
Maximum Supported VLAN Numbers      : 4094
Maximum Supported VLAN ID           : 4094
```

```
Extended Multicast Filtering Services : No
Static Entry Individual Port          : Yes
VLAN Version Number                  : 2
VLAN Learning                        : IVL
Configurable PVID Tagging            : Yes
Local VLAN Capable                   : No
Traffic Classes                      : Enabled
Console#
```

Table 119: show bridge-ext - display description

Field	Description
Maximum Supported VLAN Numbers	The maximum number of VLANs supported on this switch.
Maximum Supported VLAN ID	The maximum configurable VLAN identifier supported on this switch.
Extended Multicast Filtering Services	This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
Static Entry Individual Port	This switch allows static filtering for unicast and multicast addresses. (Refer to the mac-address-table static command.)
VLAN Version Number	Based on IEEE 802.1Q, "1" indicates Bridges that support only single spanning tree (SST) operation, and "2" indicates Bridges that support multiple spanning tree (MST) operation.
VLAN Learning	This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
Configurable PVID Tagging	This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to the switchport allowed vlan command.)
Local VLAN Capable	This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.
Traffic Classes	This switch provides mapping of user priorities to multiple traffic classes. (Refer to "Class of Service Commands" on page 881.)

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

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 \(857\)](#)

Editing VLAN Groups

Table 120: 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 \(869\)](#)

vlan This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}] [**rspan**]

no vlan *vlan-id* [**name** | **state**]

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

media ethernet - Ethernet media type.

state - Keyword to be followed by the VLAN state.

active - VLAN is operational.

suspend - VLAN is suspended. Suspended VLANs do not pass packets.

rspan - Keyword to create a VLAN used for mirroring traffic from remote switches. The VLAN used for RSPAN cannot include VLAN 1 (the switch's default VLAN). Nor should it include VLAN 4093 (which is used for switch clustering). Configuring VLAN 4093 for other purposes may cause problems in the Clustering operation. For more information on configuring RSPAN through the CLI, see ["RSPAN Mirroring Commands" on page 803](#).

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- ◆ **no vlan** *vlan-id* deletes the VLAN.
- ◆ **no vlan** *vlan-id* **name** removes the VLAN name.
- ◆ **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- ◆ You can configure up to 4094 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

[show vlan \(869\)](#)

Configuring VLAN Interfaces

Table 121: 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 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: 1-4094)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Creating a “normal” VLAN with the `vlan` command initializes it as a Layer 2 interface. To change it to a Layer 3 interface, use the `interface` command to enter interface configuration for the desired VLAN, enter any Layer 3 configuration commands, and save the configuration settings.
- ◆ To change a Layer 3 normal VLAN back to a Layer 2 VLAN, use the `no interface` command.

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

`shutdown` (764)

`interface` (758)

`vlan` (861)

`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 \(866\)](#)

switchport allowed vlan This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {*vlan-list* | **add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}

no switchport allowed vlan

vlan-list - If a VLAN list is entered without using the **add** option, the interface is assigned to the specified VLANs, and membership in all previous VLANs is removed. The interface is added as a tagged member if [switchport mode](#) is set to hybrid or access, or as an untagged member if switchport mode is set to trunk.

Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

add *vlan-list* - List of VLAN identifiers to add. When the **add** option is used, the interface is assigned to the specified VLANs, and membership in all previous VLANs is retained.

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

Default Setting

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If a port or trunk has switchport mode set to **access**, then only one VLAN can be added with this command. If a VLAN list is specified, only the last VLAN in the list will be added to the interface.
- ◆ A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.

- ◆ If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- ◆ Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- ◆ If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- ◆ If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport ingress-filtering

This command enables ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

[no] switchport ingress-filtering

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Ingress filtering only affects tagged frames.
- ◆ If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- ◆ If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.

- ◆ Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

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

switchport mode This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {access | hybrid | trunk}

no switchport mode

access - Specifies an access VLAN interface. The port transmits and receives untagged frames on a single VLAN only.

hybrid - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

trunk - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

Default Setting

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 \(863\)](#)

switchport native vlan This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*

no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.
- ◆ If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

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

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

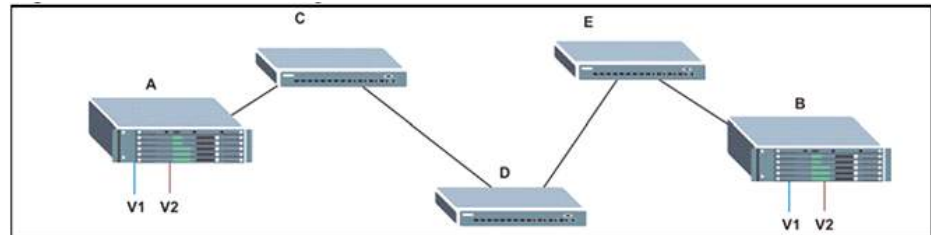
Interface Configuration (Ethernet, Port Channel)

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 313: 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 122: Commands for Displaying VLAN Information

Command	Function	Mode
<code>show interfaces status vlan</code>	Displays status for the specified VLAN interface	NE, PE
<code>show interfaces switchport</code>	Displays the administrative and operational status of an interface	NE, PE
<code>show vlan</code>	Shows VLAN information	NE, PE

show vlan This command shows VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

id - Keyword to be followed by the VLAN ID.

vlan-id - ID of the configured VLAN. (Range: 1-4094)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

```

Console#show vlan id 1

VLAN ID:                1
Type:                   Static
Name:                   DefaultVlan
Status:                 Active
Ports/Port Channels :  Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                        Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                        Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                        Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                        Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                        Eth1/26(S) Eth1/27(S) Eth1/28(S)

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 123: 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 861](#)). 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*²⁰ - Frame type used by this protocol. (Options: ethernet, rfc_1042, llc_other)

protocol - Protocol type. The only option for the llc_other frame type is ipx_raw. The options for all other frames types include: arp, ip, ipv6, rarp.

Default Setting

No protocol groups are configured.

Command Mode

Global Configuration

Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet  
protocol-type ip  
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet  
protocol-type arp  
Console(config)#
```

**protocol-vlan
protocol-group**
(Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the **no** form to remove the protocol mapping for this interface.

Syntax

protocol-vlan protocol-group *group-id* **vlan** *vlan-id* **priority** *priority*

no protocol-vlan protocol-group *group-id* **vlan**

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

vlan-id - VLAN to which matching protocol traffic is forwarded.
(Range: 1-4094)

priority - The priority assigned to untagged ingress traffic.
(Range: 0-7, where 7 is the highest priority)

²⁰. SNAP frame types are not supported by this switch due to hardware limitations.

Default Setting

No protocol groups are mapped for any interface.

Priority: 0

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as the `vlan` command), these interfaces will admit traffic of any protocol type into the associated VLAN.
- ◆ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.
- ◆ When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
 - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
 - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
 - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Example

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2 priority 0
Console(config-if)#
```

show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

Syntax

show protocol-vlan protocol-group [*group-id*]

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

Default Setting

All protocol groups are displayed.

Command Mode

Privileged Exec

Example

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

Protocol Group ID  Frame Type  Protocol Type
-----
                  1      ethernet    08 00
Console#
```

show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

Syntax

show interfaces protocol-vlan protocol-group [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

The mapping for all interfaces is displayed.

Command Mode

Privileged Exec

Example

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group
Port      Protocol Group ID  VLAN ID  Priority
-----
Eth 1/1          1    vlan2      0
Console#
```

Configuring 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 124: Voice VLAN Commands

Command	Function	Mode
<code>voice vlan</code>	Defines the Voice VLAN ID	GC
<code>voice vlan aging</code>	Configures the aging time for Voice VLAN ports	GC
<code>voice vlan mac-address</code>	Configures VoIP device MAC addresses	GC
<code>switchport voice vlan</code>	Sets the Voice VLAN port mode	IC
<code>switchport voice vlan priority</code>	Sets the VoIP traffic priority for ports	IC
<code>switchport voice vlan rule</code>	Sets the automatic VoIP traffic detection method for ports	IC
<code>switchport voice vlan security</code>	Enables Voice VLAN security on ports	IC
<code>show voice vlan</code>	Displays Voice VLAN settings	PE

voice vlan This command enables VoIP traffic detection and defines the Voice VLAN ID. Use the **no** form to disable the Voice VLAN.

Syntax

voice vlan *voice-vlan-id*

no voice vlan

voice-vlan-id - Specifies the voice VLAN ID. (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation helps prevent excessive packet delays, packet loss, and jitter, which results in higher voice quality. This is best achieved by assigning all VoIP traffic to a single VLAN.

- ◆ VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member of the Voice VLAN.
- ◆ Only one Voice VLAN is supported and it must already be created on the switch before it can be specified as the Voice VLAN.
- ◆ The Voice VLAN ID cannot be modified when the global auto-detection status is enabled (see the [switchport voice vlan](#) command).

Example

The following example enables VoIP traffic detection and specifies the Voice VLAN ID as 1234.

```
Console(config)#voice vlan 1234
Console(config)#
```

voice vlan aging This command sets the Voice VLAN ID time out. Use the **no** form to restore the default.

Syntax

voice vlan aging *minutes*

no voice vlan

minutes - Specifies the port Voice VLAN membership time out.
(Range: 5-43200 minutes)

Default Setting

1440 minutes

Command Mode

Global Configuration

Command Usage

The Voice VLAN aging time is the time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port.

The VoIP aging time starts to count down when the OUI's MAC address expires from the MAC address table. Therefore, the MAC address aging time should be added to the overall aging time. For example, if you configure the MAC address table aging time to 30 seconds, and voice VLAN aging time to 5 minutes, then after 5.5 minutes, a port will be removed from the voice VLAN when VoIP traffic is no longer received on the port. Alternatively, if you clear the MAC address table manually, then the switch will also start counting down the voice VLAN aging time.

Note that when the `switchport voice vlan` command is set to auto mode, the remaining aging time displayed by the `show voice vlan` command will be displayed. Otherwise, if the `switchport voice vlan` command is disabled or set to manual mode, the remaining aging time will display “NA.”

Example

The following example configures the Voice VLAN aging time as 3000 minutes.

```
Console(config)#voice vlan aging 3000
Console(config)#
```

voice vlan mac-address This command specifies MAC address ranges to add to the OUI Telephony list. Use the **no** form to remove an entry from the list.

Syntax

voice vlan mac-address *mac-address* **mask** *mask-address*
[**description** *description*]

no voice vlan mac-address *mac-address* **mask** *mask-address*

mac-address - Defines a MAC address OUI that identifies VoIP devices in the network. (Format: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx; for example, 01-23-45-00-00-00)

mask-address - Identifies a range of MAC addresses. (Range: 80-00-00-00-00-00 to FF-FF-FF-FF-FF-FF)

description - User-defined text that identifies the VoIP devices. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP.
- ◆ Setting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Setting a mask of FF-FF-FF-FF-FF-FF specifies a single MAC address.

Example

The following example adds a MAC OUI to the OUI Telephony list.

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-ff-ff-00-00-00 description A new phone
Console(config)#
```

switchport voice vlan This command specifies the Voice VLAN mode for ports. Use the **no** form to disable the Voice VLAN feature on the port.

Syntax

switchport voice vlan {manual | auto}

no switchport voice vlan

manual - The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

auto - The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port.

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ When auto is selected, you must select the method to use for detecting VoIP traffic, either OUI or 802.1AB (LLDP) using the [switchport voice vlan rule](#) command. When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list using the [voice vlan mac-address](#) command.
- ◆ All ports are set to VLAN hybrid mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), ensure that VLAN membership is not set to access mode using the [switchport mode](#) command.

Example

The following example sets port 1 to Voice VLAN auto mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

switchport voice vlan priority This command specifies a CoS priority for VoIP traffic on a port. Use the **no** form to restore the default priority on a port.

Syntax

switchport voice vlan priority *priority-value*

no switchport voice vlan priority

priority-value - The CoS priority value. (Range: 0-6)

Default Setting

6

Command Mode

Interface Configuration

Command Usage

Specifies a CoS priority to apply to the port VoIP traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port.

Example

The following example sets the CoS priority to 5 on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan priority 5
Console(config-if)#
```

switchport voice vlan rule This command selects a method for detecting VoIP traffic on a port. Use the **no** form to disable the detection method on the port.

Syntax

[**no**] **switchport voice vlan rule** {**oui** | **lldp**}

oui - Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address.

lldp - Uses LLDP to discover VoIP devices attached to the port.

Default Setting

OUI: Enabled

LLDP: Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list (see the [voice vlan mac-address](#) command. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.
- ◆ LLDP checks that the “telephone bit” in the system capability TLV is turned on. See [“LLDP Commands” on page 962](#) for more information on LLDP.

Example

The following example enables the OUI method on port 1 for detecting VoIP traffic.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan rule oui
Console(config-if)#
```

switchport voice vlan security This command enables security filtering for VoIP traffic on a port. Use the **no** form to disable filtering on a port.

Syntax

[no] **switchport voice vlan security**

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- ◆ Security filtering discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped.
- ◆ When enabled, be sure the MAC address ranges for VoIP devices are configured in the Telephony OUI list ([voice vlan mac-address](#)).

Example

The following example enables security filtering on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

show voice vlan This command displays the Voice VLAN settings on the switch and the OUI Telephony list.

Syntax

show voice vlan {oui | status}

oui - Displays the OUI Telephony list.

status - Displays the global and port Voice VLAN settings.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

When the **switchport voice vlan** command is set to auto mode, the remaining aging time displayed by the **show voice vlan** command will be displayed (or "Not Start" will be displayed). Otherwise, if the switchport voice vlan command is disabled or set to manual mode, the remaining aging time will display "NA."

Example

```

Console#show voice vlan status
Global Voice VLAN Status
Voice VLAN Status      : Enabled
Voice VLAN ID          : 1234
Voice VLAN aging time  : 1440 minutes

Voice VLAN Port Summary
Port      Mode      Security Rule      Priority Remaining Age
                                   (minutes)
-----
Eth 1/ 1 Auto      Enabled OUI                6 100
Eth 1/ 2 Disabled Disabled OUI                6 NA
Eth 1/ 3 Manual    Enabled OUI                5 100
Eth 1/ 4 Auto      Disabled OUI                6 Not Start
Eth 1/ 5 Disabled Disabled OUI                6 NA
Eth 1/ 6 Disabled Disabled OUI                6 NA
Eth 1/ 7 Disabled Disabled OUI                6 NA
Eth 1/ 8 Disabled Disabled OUI                6 NA
Eth 1/ 9 Disabled Disabled OUI                6 NA
Eth 1/10 Disabled Disabled OUI                6 NA
...
Console#show voice vlan oui
OUI Address      Mask      Description
-----
00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones
00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone

Console#

```

Class of Service Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. The default priority can be set for each interface, also the queue service mode and the mapping of frame priority tags to the switch's priority queues can be configured.

Table 125: 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 126: 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	IC
queue weight	Assigns round-robin weights to the priority queues	IC
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 queuing. Use the **no** form to restore the default value.

Syntax

queue mode {**strict** | **wrr** | **strict-wrr** [*queue-type-list*]}

no queue mode

strict - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

wrr - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights (based on the [queue weight](#) command), and servicing each queue in a round-robin fashion.

strict-wrr - Uses strict or weighted service as specified for each queue.

queue-type-list - Indicates if the queue is a normal or strict type.
(Options: 0 indicates a normal queue, 1 indicates a strict queue)

Default Setting

WRR

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ The switch can be set to service the port queues based on strict priority, WRR, or a combination of strict and weighted queuing.
- ◆ Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- ◆ Weighted Round Robin (WRR) uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing. Use the [queue weight](#) command to assign weights for WRR queuing to the eight priority queues.
- ◆ If Strict and WRR mode is selected, a combination of strict and weighted service is used as specified for each queue. The queues assigned to use strict or WRR priority should be specified using the *queue-type-list* parameter.
- ◆ A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

- ◆ Service time is shared at the egress ports by defining scheduling weights for WRR, or for the queuing mode that uses a combination of strict and weighted queuing. Service time is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.
- ◆ The specified queue mode applies to all interfaces.

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue mode strict
Console(config-if)#
```

Related Commands

[queue weight \(883\)](#)

[show queue mode \(885\)](#)

queue weight This command assigns weights to the eight class of service (CoS) priority queues when using weighted queuing, or one of the queuing modes that use a combination of strict and weighted queuing. Use the **no** form to restore the default weights.

Syntax

queue weight *weight0...weight7*

no queue weight

weight0...weight7 - The ratio of weights for queues 0 - 7 determines the weights used by the WRR scheduler. (Range: 1-255)

Default Setting

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This command shares bandwidth at the egress port by defining scheduling weights for Weighted Round-Robin, or for the queuing mode that uses a combination of strict and weighted queuing ([page 882](#)).
- ◆ Bandwidth is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

Example

The following example shows how to assign round-robin weights of 1 - 8 to the CoS priority queues 0 - 7.

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue weight 1 2 3 4 5 6 7 8
Console(config-if)#
```

Related Commands

[queue mode \(882\)](#)

[show queue weight \(885\)](#)

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 \(773\)](#)

show queue mode This command shows the current queue mode.

Command Mode

Privileged Exec

Example

```
Console#show queue mode
Unit   Port   queue mode
----   -
      1     1   Weighted Round Robin
...
```

show queue weight This command displays the weights used for the weighted queues.

Command Mode

Privileged Exec

Example

```
Console#show queue weight
Information of Eth 1/1
Queue ID  Weight
-----
        0         1
        1         2
        2         4
        3         6
        4         8
        5        10
        6        12
        7        14
...
```

Priority Commands (Layer 3 and 4)

This section describes commands used to configure Layer 3 and 4 traffic priority mapping on the switch.

Table 127: 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 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 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 for 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 128: 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 (Ethernet, Port Channel)

Command Usage

- ◆ The default mapping of CoS to PHB values shown in [Table 128](#) 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 1/2
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 for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

dscp - DSCP value in ingress packets. (Range: 0-63)

DEFAULT SETTING.

Table 129: 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 (Ethernet, Port Channel)

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 129](#), 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 1/2
Console(config-if)#qos map dscp-mutation 3 1 from 1
Console(config-if)#
```

qos map trust-mode This command sets QoS mapping to DSCP or CoS. Use the **no** form to restore the default setting.

Syntax

qos map trust-mode {dscp | cos}

no qos map trust-mode

dscp - Sets the QoS mapping mode to DSCP.

cos - Sets the QoS mapping mode to CoS.

Default Setting

CoS

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ If the QoS mapping mode is set to DSCP with this command, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.
- ◆ If the QoS mapping mode is set to DSCP, and a non-IP packet is received, the packet's CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority (see [page 884](#)) 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 884](#)) is used for priority processing.

Example

This example sets the QoS priority mapping mode to use DSCP based on the conditions described in the Command Usage section.

```
Console(config)#interface 1/1
Console(config-if)#qos map trust-mode cos
Console(config-if)#
```

show qos map cos-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)
```

Command Mode

Privileged Exec

Example

```
Console#show qos map cos-dscp interface ethernet 1/5
CoS Information of Eth 1/5
CoS-DSCP Map. (CoS,CFI) - PHB
CoS  : CFI  0          1
-----
0          0          0
1          1          1
2          2          2
3          3          3
4          4          4
5          5          5
6          6          6
7          7          7
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)

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    0    0    0    0    0    1    1
1 :    1    1    1    1    1    1    2    2    2    2
2 :    2    2    2    2    3    3    3    3    3    3
3 :    3    3    4    4    4    4    4    4    4    4
4 :    5    5    5    5    5    5    5    5    6    6
5 :    6    6    6    6    6    6    7    7    7    7
6 :    7    7    7    7
Console#
```

show qos map trust-mode This command shows the QoS mapping mode.

Syntax

show qos map trust-mode interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

Command Mode

Privileged Exec

Example

The following shows that the trust mode is set to CoS:

```
Console#show qos map trust-mode interface ethernet 1/5
Information of Eth 1/5
  CoS Map Mode:          CoS mode
Console#
```


Quality of Service Commands

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. You can classify traffic based on access lists, IP Precedence or DSCP values, or VLANs. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

Table 130: Quality of Service Commands

Command	Function	Mode
<code>class-map</code>	Creates a class map for a type of traffic	GC
<code>description</code>	Specifies the description of a class map	CM
<code>match</code>	Defines the criteria used to classify traffic	CM
<code>rename</code>	Redefines the name of a class map	CM
<code>policy-map</code>	Creates a policy map for multiple interfaces	GC
<code>description</code>	Specifies the description of a policy map	PM
<code>class</code>	Defines a traffic classification for the policy to act on	PM
<code>rename</code>	Redefines the name of a policy map	PM
<code>police rate</code>	Defines an enforcer for classified traffic based on the metered flow rate	PM-C
<code>set cos</code>	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 ingress or egress traffic, and may include policers for bandwidth limitations	PE
<code>show policy-map interface</code>	Displays the configuration of all classes configured for all service policies on the specified interface	PE

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the `class-map` command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.
2. Use the `match` command to select a specific type of traffic based on an access list, an IPv4 DSCP value, IPv4 Precedence value, IPv6 DSCP value, a VLAN, or a CoS value. Note that a class map can include match settings for both IP values and a VLAN.
3. Use the `policy-map` command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.
4. Use the `class` command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain up to 16 class maps.
5. Use the `set 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*

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

match-any

Command Mode

Global Configuration

Command Usage

- ◆ First enter this command to designate a class map and enter the Class Map configuration mode. Then use `match` commands to specify the criteria for ingress traffic that will be classified under this class map.

- ◆ One or more class maps can be assigned to a policy map ([page 897](#)). The policy map is then bound by a service policy to an interface ([page 903](#)). A service policy defines packet classification, service tagging, and bandwidth policing. Once a policy map has been bound to an interface, no additional class maps may be added to the policy map, nor any changes made to the assigned class maps with the **match** or **set** commands.

Example

This example creates a class map call "rd-class," and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd-class
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

Related Commands

[show class-map \(903\)](#)

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 | vlan vlan}
```

acl-name - Name of the access control list. Any type of ACL can be specified, including standard or extended IPv4/IPv6 ACLs and MAC ACLs.
(Range: 1-16 characters)

cos - A Class of Service value. (Range: 0-7)

dscp - A Differentiated Service Code Point value. (Range: 0-63)

ip-precedence - An IP Precedence value. (Range: 0-7)

vlan - A VLAN. (Range:1-4094)

Default Setting

None

Command Mode

Class Map Configuration

Command Usage

- ◆ First enter the **class-map** command to designate a class map and enter the Class Map configuration mode. Then use **match** commands to specify the fields within ingress packets that must match to qualify for this class map.
- ◆ If an ingress packet matches an ACL specified by this command, any deny rules included in the ACL will be ignored.
- ◆ If match criteria includes an IP ACL or IP priority rule, then a VLAN rule cannot be included in the same class map.
- ◆ If match criteria includes a MAC ACL or VLAN rule, then neither an IP ACL nor IP priority rule can be included in the same class map.
- ◆ Up to 16 match entries can be included in a class map.

Example

This example creates a class map called "rd-class#1," and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd-class#1  
Console(config-cmap)#match ip dscp 3  
Console(config-cmap)#
```

This example creates a class map call "rd-class#2," and sets it to match packets marked for IP Precedence service value 5.

```
Console(config)#class-map rd-class#2
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

This example creates a class map call "rd-class#3," and sets it to match packets marked for VLAN 1.

```
Console(config)#class-map rd-class#3
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

rename This command redefines the name of a class map or policy map.

Syntax

rename *map-name*

map-name - Name of the class map or policy map. (Range: 1-32 characters)

Command Mode

Class Map Configuration

Policy Map Configuration

Example

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

policy-map This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map.

Syntax

[**no**] **policy-map** *policy-map-name*

policy-map-name - Name of the policy map. (Range: 1-32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Use the **policy-map** command to specify the name of the policy map, and then use the **class** command to configure policies for traffic that matches the criteria defined in a class map.
- ◆ A policy map can contain multiple class statements that can be applied to the same interface with the **service-policy** command.
- ◆ Create a Class Map (page 897) before assigning it to a Policy Map.

Example

This example creates a policy called "rd-policy," uses the **class** command to specify the previously defined "rd-class," uses the **set** command to classify the service that incoming packets will receive.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 0
Console(config-pmap-c)#
```

class This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map.

Syntax

[no] class *class-map-name*

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

None

Command Mode

Policy Map Configuration

Command Usage

- ◆ Use the **policy-map** command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the **set** command and one of the **police** commands to specify the match criteria, where the:
 - **set 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.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#
```

police rate This command defines an enforcer for classified traffic based on the metered flow rate. Use the **no** form to remove a policer.

Syntax

[no] **police rate** *committed-rate*

committed-rate - Committed information rate in kilobits per second.
(Range: 16-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

- ◆ You can configure up to 16 policers (i.e., class maps) for ingress ports.
- ◆ The *committed-rate* cannot exceed the configured interface speed.
- ◆ Policing is based on a token bucket, where bucket depth is the maximum burst before the bucket overflows, and the average rate tokens that are added to the bucket is by specified by the *committed-rate* option. Note that the token bucket functions similar to that described in RFC 2697 and RFC 2698.
- ◆ The behavior of the meter is specified in terms of one token bucket (C), the rate at which the tokens are incremented (CIR – Committed Information Rate), and the maximum size of the token bucket (BC – Committed Burst Size).

The token bucket C is initially full, that is, the token count $T_c(0) = BC$. Thereafter, the token count T_c is updated CIR times per second as follows:

- If T_c is less than BC , T_c is incremented by one, else
- T_c is not incremented.

When a packet of size B bytes arrives at time t, the following happens:

- If $T_c(t) - B \geq 0$, the packet is green and T_c is decremented by B down to the minimum value of 0,
- else the packet is red and T_c is not decremented.

Example

This example creates a policy called “rd-policy,” uses the `class` command to specify the previously defined “rd-class,” uses the `set phb` command to classify the service that incoming packets will receive, and then uses the **police rate** command to limit the average bandwidth to 100,000 Kbps.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police rate 100000
Console(config-pmap-c)#
```

set cos This command modifies the class of service (CoS) value for a matching packet (as specified by the `match` command) in the packet’s VLAN tag. Use the **no** form to remove this setting.

Syntax

[no] set cos *cos-value*

cos-value - Class of Service value. (Range: 0-7)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

- ◆ The **set cos** command is used to set the CoS value in the VLAN tag for matching packets.
- ◆ 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.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
Console(config-pmap-c)#
```

set ip dscp This command modifies the IP DSCP value in a matching packet (as specified by the `match` command). Use the **no** form to remove this traffic classification.

Syntax

[no] set ip dscp *new-dscp*

new-dscp - New Differentiated Service Code Point (DSCP) value.
(Range: 0-63)

Default Setting

None

Command Mode

Policy Map Class Configuration

Command Usage

The **set ip dscp** command is used to set the priority values in the packet’s ToS field for matching packets.

Example

This example creates a policy called “rd-policy,” uses the `class` command to specify the previously defined “rd-class,” uses the **set ip dscp** command to classify the service that incoming packets will receive, and then uses the `police rate` command to limit the average bandwidth to 100,000 Kbps.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police rate 100000
Console(config-pmap-c)#
```

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 129, "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.
- ◆ 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 rate](#) command to limit the average bandwidth to 100,000 Kbps.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police rate 100000
Console(config-pmap-c)#
```

service-policy This command applies a policy map defined by the **policy-map** command to the ingress or egress side of a particular interface. Use the **no** form to remove this mapping.

Syntax

[no] **service-policy** {input | output} *policy-map-name*

input - Apply to the input traffic.

policy-map-name - Name of the policy map for this interface.
(Range: 1-32 characters)

Default Setting

No policy map is attached to an interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Only one policy map can be assigned to an interface.
- ◆ First define a class map, then define a policy map, and finally use the **service-policy** command to bind the policy map to the required interface.

Example

This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd-policy
Console(config-if)#
```

show class-map This command displays the QoS class maps which define matching criteria used for classifying traffic.

Syntax

show class-map [*class-map-name*]

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

Displays all class maps.

Command Mode

Privileged Exec

Example

```

Console#show class-map
Class Map match-any rd-class#1
Description:
  Match ip dscp 10
  Match access-list rd-access
  Match ip dscp 0

Class Map match-any rd-class#2
  Match ip precedence 5

Class Map match-any rd-class#3
  Match vlan 1

Console#

```

show policy-map This command displays the QoS policy maps which define classification criteria for ingress or egress traffic, and may include policers for bandwidth limitations.

Syntax

show policy-map [*policy-map-name* [**class** *class-map-name*]]

policy-map-name - Name of the policy map. (Range: 1-32 characters)

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Setting

Displays all policy maps and all classes.

Command Mode

Privileged Exec

Example

```

Console#show policy-map
Policy Map rd-policy
Description:
  class rd-class
  set PHB 3
  class finance-class
  police rate 100 class rd-class
Policy Map rd-policy
  class rd-class
  set PHB 3
Console#

```

show policy-map interface This command displays the service policy assigned to the specified interface.

Syntax

show policy-map interface [*interface input*]

interface

unit/port

unit - Unit identifier. (Range: 1)

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

Command Mode

Privileged Exec

Example

```
Console#show policy-map interface 1/5 input
Service-policy rd-policy
Console#show policy-map interface
Interface ethernet 1/2
  service-policy input policy-map
Interface ethernet 1/3
  service-policy input policy-map
Interface ethernet 1/4
  service-policy input policy-map
Interface ethernet 1/5
  service-policy input policy-map
Console#
```

Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to check for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Table 131: Multicast Filtering Commands

Command Group	Function
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, enables proxy reporting, displays current snooping settings, and displays the multicast service and group members
Static Multicast Routing	Configures static multicast router ports which forward all inbound multicast traffic to the attached VLANs
IGMP Filtering and Throttling	Configures IGMP filtering and throttling
MLD Snooping	Configures multicast snooping for IPv6
MLD Filtering and Throttling	Configures MLD filtering and throttling for IPv6.

IGMP Snooping

This section describes commands used to configure IGMP snooping on the switch.

Table 132: 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
<code>ip igmp snooping tcn-flood</code>	Floods multicast traffic when a Spanning Tree topology change occurs	GC

Table 132: IGMP Snooping Commands (Continued)

Command	Function	Mode
<code>ip igmp snooping tcn-query-solicit</code>	Sends an IGMP Query Solicitation when a Spanning Tree topology change occurs	GC
<code>ip igmp snooping unregistered-data-flood</code>	Floods unregistered multicast traffic into the attached VLAN	GC
<code>ip igmp snooping unsolicited-report-interval</code>	Specifies how often the upstream interface should transmit unsolicited IGMP reports (when proxy reporting is enabled)	GC
<code>ip igmp snooping version</code>	Configures the IGMP version for snooping	GC
<code>ip igmp snooping version-exclusive</code>	Discards received IGMP messages which use a version different to that currently configured	GC
<code>ip igmp snooping vlan general-query-suppression</code>	Suppresses general queries except for ports attached to downstream multicast hosts	GC
<code>ip igmp snooping vlan immediate-leave</code>	Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN	GC
<code>ip igmp snooping vlan last-memb-query-count</code>	Configures the number of IGMP proxy query messages that are sent out before the system assumes there are no local members	GC
<code>ip igmp snooping vlan last-memb-query-intvl</code>	Configures the last-member-query interval	GC
<code>ip igmp snooping vlan mrd</code>	Sends multicast router solicitation messages	GC
<code>ip igmp snooping vlan proxy-address</code>	Configures a static address for proxy IGMP query and reporting	GC
<code>ip igmp snooping vlan proxy-reporting</code>	Enables IGMP Snooping with Proxy Reporting	GC
<code>ip igmp snooping vlan query-interval</code>	Configures the interval between sending IGMP general queries	GC
<code>ip igmp snooping vlan query-resp-intvl</code>	Configures the maximum time the system waits for a response to general queries	GC
<code>ip igmp snooping vlan static</code>	Adds an interface as a member of a multicast group	GC
<code>ip igmp snooping vlan version</code>	Configures the IGMP version for snooping	GC
<code>ip igmp snooping vlan version-exclusive</code>	Discards received IGMP messages which use a version different to that currently configured	GC
<code>clear ip igmp snooping groups dynamic</code>	Clears multicast group information dynamically learned through IGMP snooping	PE
<code>clear ip igmp snooping statistics</code>	Clears IGMP snooping statistics	PE
<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

Table 132: IGMP Snooping Commands (Continued)

Command	Function	Mode
<code>show ip igmp snooping mrouter</code>	Shows multicast router ports	PE
<code>show ip igmp snooping statistics</code>	Shows IGMP snooping protocol statistics for the specified interface	PE

ip igmp snooping This command enables IGMP snooping globally on the switch or on a selected VLAN interface. Use the **no** form to disable it.

Syntax

`[no] ip igmp snooping [vlan vlan-id]`

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

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence.
- ◆ When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

Example

The following example enables IGMP snooping globally.

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


ip igmp snooping priority This command assigns a priority to all multicast traffic. Use the **no** form to restore the default setting.

Syntax

ip igmp snooping priority *priority*

no ip igmp snooping priority

priority - The CoS priority assigned to all multicast traffic. (Range: 0-7, where 7 is the highest priority)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

Example

```
Console(config)#ip igmp snooping priority 6
Console(config)#
```

Related Commands

[show ip igmp snooping \(925\)](#)

ip igmp snooping proxy-reporting This command enables IGMP Snooping with Proxy Reporting. Use the **no** form to restore the default setting.

Syntax

[no] ip igmp snooping proxy-reporting

ip igmp snooping vlan *vlan-id* **proxy-reporting** {**enable** | **disable**}

no ip igmp snooping vlan *vlan-id* **proxy-reporting**

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

enable - Enable on the specified VLAN.

disable - Disable on the specified VLAN.

Default Setting

Global: Disabled

VLAN: Based on global setting

Command Mode

Global Configuration

Command Usage

- ◆ When proxy reporting is enabled with this command, the switch performs “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.
- ◆ If the IGMP proxy reporting is configured on a VLAN, this setting takes precedence over the global configuration.

Example

```
Console(config)#ip igmp snooping proxy-reporting
Console(config)#
```

ip igmp snooping querier This command enables the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

[no] ip igmp snooping querier

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ IGMP snooping querier is not supported for IGMPv3 snooping (see [ip igmp snooping version](#)).
- ◆ If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping router-alert-option-check This command discards any IGMPv2/v3 packets that do not include the Router Alert option. Use the **no** form to ignore the Router Alert Option when receiving IGMP messages.

Syntax

[no] ip igmp snooping router-alert-option-check

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value.

To protect against this kind of attack, (1) routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option. (2) Also, when the switch is acting in the role of a multicast host (such as when using proxy routing), it should ignore version 2 or 3 queries that do not contain the Router Alert option.

Example

```
Console(config)#ip igmp snooping router-alert-option-check
Console(config)#
```

ip igmp snooping router-port-expire-time This command configures the querier timeout. Use the **no** form to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535;
Recommended Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the timeout to 400 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 400
Console(config)#
```

ip igmp snooping tcn-flood This command enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable flooding.

Syntax

[no] ip igmp snooping tcn-flood

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When a spanning tree topology change occurs, the multicast membership information learned by the switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, a switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with the TC bit set (by the root bridge) will enter into “multicast flooding mode” for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned.
- ◆ If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a timeout mechanism is used to delete all of the currently learned multicast channels.
- ◆ When a new uplink port starts up, the switch sends unsolicited reports for all current learned channels out through the new uplink port.
- ◆ By default, the switch immediately enters into “multicast flooding mode” when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive loading on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned.
- ◆ When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN.

The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

Example

The following example enables TCN flooding.

```
Console(config)#ip igmp snooping tcn-flood
Console(config)#
```

ip igmp snooping tcn-query-solicit

This command instructs the switch to send out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable this feature.

Syntax

[no] ip igmp snooping tcn-query-solicit

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When the root bridge in a spanning tree receives a topology change notification for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred. When an upstream multicast router receives this solicitation, it will also immediately 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 unsolicited-report-interval

seconds - The interval at which to issue unsolicited reports. (Range: 1-65535 seconds)

Default Setting

400 seconds

Command Mode

Global Configuration

Command Usage

- ◆ When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.
- ◆ This command only applies when proxy reporting is enabled (see [page 909](#)).

Example

```
Console(config)#ip igmp snooping unsolicited-report-interval 5
Console(config)#
```

ip igmp snooping version This command configures the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping [vlan *vlan-id*] version {1 | 2 | 3}

no ip igmp snooping version

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

1 - IGMP Version 1

2 - IGMP Version 2

3 - IGMP Version 3

Default Setting

Global: IGMP Version 2

VLAN: Not configured, based on global setting

Command Mode

Global Configuration

Command Usage

- ◆ This command configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.
- ◆ If the IGMP snooping version is configured on a VLAN, this setting takes precedence over the global configuration.

Example

The following configures the global setting for IGMP snooping to version 1.

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

ip igmp snooping version-exclusive This command discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the [ip igmp snooping version](#) command. Use the **no** form to disable this feature.

Syntax

ip igmp snooping [vlan *vlan-id*] version-exclusive

no ip igmp snooping version-exclusive

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

Default Setting

Global: Disabled

VLAN: Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If version exclusive is disabled on a VLAN, then this setting is based on the global setting. If it is enabled on a VLAN, then this setting takes precedence over the global setting.
- ◆ When this function is disabled, the currently selected version is backward compatible (see the [ip igmp snooping version](#) command).

Example

```
Console(config)#ip igmp snooping version-exclusive
Console(config)#
```

ip igmp snooping vlan general-query-suppression This command suppresses general queries except for ports attached to downstream multicast hosts. Use the **no** form to flood general queries to all ports except for the multicast router port.

Syntax

[no] ip igmp snooping vlan *vlan-id* general-query-suppression

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

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ By default, general query messages are flooded to all ports, except for the multicast router through which they are received.
- ◆ If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

Example

```
Console(config)#ip igmp snooping vlan 1 general-query-suppression
Console(config)#
```

ip igmp snooping vlan immediate-leave This command immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* immediate-leave [by-host-ip]

no ip igmp snooping vlan *vlan-id* immediate-leave

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

by-host-ip - Specifies that the member port will be deleted only when there are no hosts joining this group.

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the timeout period. (The timeout for this release is defined by Last Member Query Interval (fixed at one second) * Robustness Variable (fixed at 2) as defined in RFC 2236.)
- ◆ If immediate-leave is used, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- ◆ If the "by-host-ip" option is used, the router/querier will not send out a group-specific query when an IGMPv2/v3 leave message is received. But will check if there are other hosts joining the multicast group. Only when all hosts on that port leave the group will the member port be deleted.

- ◆ This command is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

Example

The following shows how to enable immediate leave.

```
Console(config)#ip igmp snooping vlan 1 immediate-leave
Console(config)#
```

ip igmp snooping vlan last-memb-query- count

This command configures the number of IGMP proxy group-specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* last-memb-query-count *count*

no ip igmp snooping vlan *vlan-id* last-memb-query-count

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

count - The number of proxy group-specific or group-and-source-specific query messages to issue before assuming that there are no more group members. (Range: 1-255)

Default Setting

2

Command Mode

Global Configuration

Command Usage

This command will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled ([page 909](#)).

Example

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-count 7
Console(config)#
```

ip igmp snooping vlan last-memb-query-intvl This command configures the last-member-query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* last-memb-query-intvl *interval*

no ip igmp snooping vlan *vlan-id* last-memb-query-intvl

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

interval - The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31744 tenths of a second)

Default Setting

10 (1 second)

Command Mode

Global Configuration

Command Usage

- ◆ When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router.
- ◆ A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more bursty traffic.
- ◆ This command will take effect only if IGMP snooping proxy reporting is enabled (page 909).

Example

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-intvl 700
Console(config)#
```

ip igmp snooping vlan mrd This command enables sending of multicast router solicitation messages. Use the **no** form to disable these messages.

Syntax

[no] ip igmp snooping vlan *vlan-id* mrd

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

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ Multicast Router Discovery (MRD) uses multicast router advertisement, multicast router solicitation, and multicast router termination messages to discover multicast routers. Devices send solicitation messages in order to solicit advertisement messages from multicast routers. These messages are used to discover multicast routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an advertisement.
- ◆ Advertisements are sent by routers to advertise that IP multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the expiration of a periodic timer, as a part of a router's start up procedure, during the restart of a multicast forwarding interface, and on receipt of a solicitation message. When the multicast services provided to a VLAN is relatively stable, the use of solicitation messages is not required and may be disabled using the **no ip igmp snooping vlan mrd** command.
- ◆ This command may also be used to disable multicast router solicitation messages when the upstream router does not support MRD, to reduce the loading on a busy upstream router, or when IGMP snooping is disabled in a VLAN.

Example

This example disables sending of multicast router solicitation messages on VLAN 1.

```
Console(config)#no ip igmp snooping vlan 1 mrd
Console(config)#
```

ip igmp snooping vlan proxy-address This command configures a static source address for locally generated query and report messages used by IGMP proxy reporting. Use the **no** form to restore the default source address.

Syntax

[no] ip igmp snooping vlan *vlan-id* proxy-address *source-address*

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

source-address - The source address used for proxied IGMP query and report, and leave messages. (Any valid IP unicast address)

Default Setting

0.0.0.0

Command Mode

Global Configuration

Command Usage

IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports.

Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.

To resolve this problem, the source address in proxied IGMP query and report messages can be replaced with any valid unicast address (other than the router's own address) using this command.

Rules Used for Proxy Reporting

When IGMP Proxy Reporting is disabled, the switch will use a null IP address for the source of IGMP query and report messages unless a proxy query address has been set.

When IGMP Proxy Reporting is enabled, the source address is based on the following criteria:

- ◆ If a proxy query address is configured, the switch will use that address as the source IP address in general and group-specific query messages sent to downstream hosts, and in report and leave messages sent upstream from the multicast router port.
- ◆ If a proxy query address is not configured, the switch will use the VLAN's IP address as the IP source address in general and group-specific query messages sent downstream, and use the source address of the last IGMP message received from a downstream host in report and leave messages sent upstream from the multicast router port.

Example

The following example sets the source address for proxied IGMP query messages to 10.0.1.8.

```
Console(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8
Console(config)#
```

ip igmp snooping vlan query-interval This command configures the interval between sending IGMP general queries. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* query-interval *interval*

no ip igmp snooping vlan *vlan-id* query-interval

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

interval - The interval between sending IGMP general queries.
(Range: 2-31744 seconds)

Default Setting

125 seconds

Command Mode

Global Configuration

Command Usage

- ◆ An IGMP general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined.
- ◆ This command applies when the switch is serving as the querier ([page 910](#)), or as a proxy host when IGMP snooping proxy reporting is enabled ([page 909](#)).

Example

```
Console(config)#ip igmp snooping vlan 1 query-interval 150
Console(config)#
```

ip igmp snooping vlan query-resp-intvl This command configures the maximum time the system waits for a response to general queries. Use the **no** form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* query-resp-intvl *interval*

no ip igmp snooping vlan *vlan-id* query-resp-intvl

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

interval - The maximum time the system waits for a response to general queries. (Range: 10-31740 tenths of a second)

Default Setting

100 (10 seconds)

Command Mode

Global Configuration

Command Usage

This command applies when the switch is serving as the querier (page 910), or as a proxy host when IGMP snooping proxy reporting is enabled (page 909).

Example

```
Console(config)#ip igmp snooping vlan 1 query-resp-intvl 20
Console(config)#
```

ip igmp snooping vlan static This command adds a port to a multicast group. Use the **no** form to remove the port.

Syntax

[no] ip igmp snooping vlan *vlan-id* static *ip-address* *interface*

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

ip-address - IP address for multicast group

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

- ◆ Static multicast entries are never aged out.
- ◆ When a multicast entry is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Example

The following shows how to statically configure a multicast group on a port.

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

clear ip igmp snooping groups dynamic

This command clears multicast group information dynamically learned through IGMP snooping.

Syntax

clear ip igmp snooping groups dynamic

Command Mode

Privileged Exec

Command Usage

This command only clears entries learned through IGMP snooping. Statically configured multicast address are not cleared.

Example

```
Console#clear ip igmp snooping groups dynamic
Console#
```

clear ip igmp snooping statistics

This command clears IGMP snooping statistics.

Syntax

clear ip igmp snooping statistics [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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

Command Mode

Privileged Exec

Example

```
Console#clear ip igmp snooping statistics
Console#
```


show ip igmp snooping This command shows the IGMP snooping, proxy, and query configuration settings.

Syntax

show ip igmp snooping [**vlan** *vlan-id*]
vlan-id - VLAN ID (1-4094)

Command Mode

Privileged Exec

Command Usage

This command displays global and VLAN-specific IGMP configuration settings.

Example

The following shows the current IGMP snooping configuration:

```

Console#show ip igmp snooping
IGMP Snooping                : Enabled
Router Port Expire Time      : 300 s
Router Alert Check           : Disabled
Router Port Mode              : Forward
TCN Flood                     : Disabled
TCN Query Solicit             : Disabled
Unregistered Data Flood       : Disabled
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)

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

igmpsnp - Display only entries learned through IGMP snooping.

sort-by-port - Display entries sorted by port.

user - Display only the user-configured multicast entries.

vlan-id - VLAN ID (1-4094)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1.

```
Console#show ip igmp snooping group vlan 1
Bridge Multicast Forwarding Entry Count:1
Flag: R - Router port, M - Group member port
      H - Host counts (number of hosts join the group on this port).
      P - Port counts (number of ports join the group).
Up time: Group elapsed time (d:h:m:s).
Expire : Group remaining time (m:s).
```

VLAN	Group	Port	Up time	Expire	Count
1	224.1.1.1	Eth 1/ 1 (R)	00:00:00:37	2 (P)	
		Eth 1/ 2 (M)		0 (H)	

```
Console#
```

show ip igmp snooping mrouter This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [vlan *vlan-id*]

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

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows the ports in VLAN 1 which are attached to multicast routers.

```
Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Port Type      Expire
-----
1    Eth 1/4                Dynamic 0:4:28
1    Eth 1/10               Static
Console#
```

show ip igmp snooping statistics This command shows IGMP snooping protocol statistics for the specified interface.

Syntax

show ip igmp snooping statistics

{input [interface *interface*] |

output [interface *interface*] |

query [vlan *vlan-id*]}

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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

query - Displays IGMP snooping-related statistics.

Default Setting

None

Command Mode
Privileged Exec**Example**

The following shows IGMP protocol statistics input:

```
Console#show ip igmp snooping statistics input interface ethernet 1/1
Input Statistics:
Interface Report    Leave    G Query  G(-S)-S Query Drop    Join Succ Group
-----
Eth 1/ 1           23       11        4          10      5        14      5
Console#
```

Table 133: show ip igmp snooping statistics input - display description

Field	Description
Interface	Shows interface.
Report	The number of IGMP membership reports received on this interface.
Leave	The number of leave messages received on this interface.
G Query	The number of general query messages received on this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages received on this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, or packet content not allowed.
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of multicast groups active on this interface.

The following shows IGMP protocol statistics output:

```
Console#show ip igmp snooping statistics output interface ethernet 1/1
Output Statistics:
Interface Report    Leave    G Query  G(-S)-S Query Drop    Group
-----
Eth 1/ 1           12        0        1          0      0        0
Console#
```

Table 134: show ip igmp snooping statistics output - display description

Field	Description
Interface	Shows interface.
Report	The number of IGMP membership reports sent from this interface.
Leave	The number of leave messages sent from this interface.
G Query	The number of general query messages sent from this interface.

Table 134: show ip igmp snooping statistics output - display description

Field	Description
G(-S)-S Query	The number of group specific or group-and-source specific query messages sent from this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, or packet content not allowed.
Group	The number of multicast groups active on this interface.

The following shows IGMP query-related statistics for VLAN 1:

```

Console#show ip igmp snooping statistics query vlan 1
  Other Querier           : None
  Other Querier Expire    : 0(m):0(s)
  Other Querier Uptime    : 0(h):0(m):0(s)
  Self Querier            : 192.168.2.12
  Self Querier Expire     : 0(m):0(s)
  Self Querier Uptime     : 0(h):0(m):0(s)
  General Query Received  : 0
  General Query Sent      : 0
  Specific Query Received : 0
  Specific Query Sent     : 0
  Warn Rate Limit        : 0 sec.
  V1 Warning Count       : 0
  V2 Warning Count       : 0
  V3 Warning Count       : 0
Console#

```

Table 135: show ip igmp snooping statistics vlan query - display description

Field	Description
Other Querier	IP address of remote querier on this interface.
Other Querier Expire	Time after which remote querier is assumed to have expired.
Other Querier Uptime	Time remote querier has been up.
Self Querier	IP address of local querier on this interface.
Self Querier Expire	Time after which local querier is assumed to have expired.
Self Querier Uptime	Time local querier has been up.
General Query Received	The number of general queries received on this interface.
General Query Sent	The number of general queries sent from this interface.
Specific Query Received	The number of specific queries received on this interface.
Specific Query Sent	The number of specific queries sent from this interface.
Warn Rate Limit	The rate at which received query messages of the wrong version type cause the Vx warning count to increment. Note that "0 sec" means that the Vx warning count is incremented for each wrong message version received.
V1 Warning Count	The number of times the query version received (Version 1) does not match the version configured for this interface.

Table 135: show ip igmp snooping statistics vlan query - display description

Field	Description
V2 Warning Count	The number of times the query version received (Version 2) does not match the version configured for this interface.
V3 Warning Count	The number of times the query version received (Version 3) does not match the version configured for this interface.

Static Multicast Routing

This section describes commands used to configure static multicast routing on the switch.

Table 136: Static Multicast Interface Commands

Command	Function	Mode
<code>ip igmp snooping vlan mrouter</code>	Adds a multicast router port	GC
<code>show ip igmp snooping mrouter</code>	Shows multicast router ports	PE

ip igmp snooping vlan mrouter This command statically configures a (Layer 2) multicast router port on the specified VLAN. Use the **no** form to remove the configuration.

Syntax

[no] ip igmp snooping vlan *vlan-id* mrouter *interface*

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

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

- ◆ Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router or switch connected over the network to an interface (port or

trunk) on this switch, that interface can be manually configured to join all the current multicast groups.

- ◆ IGMP Snooping must be enabled globally on the switch (using the `ip igmp snooping` command) before a multicast router port can take effect.

Example

The following shows how to configure port 10 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/10
Console(config)#
```

IGMP Filtering and Throttling

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

Table 137: 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>ip multicast-data-drop</code>	Drops all multicast data 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
<code>show ip multicast-data-drop</code>	Shows if the interface is configured to drop multicast data packets	PE

ip igmp filter (Global Configuration) This command globally enables IGMP filtering and throttling on the switch. Use the **no** form to disable the feature.

Syntax

[no] **ip igmp filter**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.
- ◆ IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.
- ◆ The IGMP filtering feature operates in the same manner when MVR is used to forward multicast traffic.

Example

```
Console(config)#ip igmp filter
Console(config)#
```

ip igmp profile This command creates an IGMP filter profile number and enters IGMP profile configuration mode. Use the **no** form to delete a profile number.

Syntax

[no] **ip igmp profile** *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

permit, deny This command sets the access mode for an IGMP filter profile. Use the **no** form to delete a profile number.

Syntax

{**permit** | **deny**}

Default Setting

Deny

Command Mode

IGMP Profile Configuration

Command Usage

- ◆ Each profile has only one access mode; either permit or deny.
- ◆ When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when a multicast group is not in the controlled range.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

range This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

Syntax

[**no**] **range** *low-ip-address* [*high-ip-address*]

low-ip-address - A valid IP address of a multicast group or start of a group range.

high-ip-address - A valid IP address for the end of a multicast group range.

Default Setting

None

Command Mode

IGMP Profile Configuration

Command Usage

Enter this command multiple times to specify more than one multicast address or address range for a profile.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

ip igmp filter (Interface Configuration) This command assigns an IGMP filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

Syntax

[no] ip igmp filter *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

Default Setting

None

Command Mode

Interface Configuration

Command Usage

- ◆ The IGMP filtering profile must first be created with the [ip igmp profile](#) command before being able to assign it to an interface.
- ◆ Only one profile can be assigned to an interface.
- ◆ A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

ip igmp max-groups This command sets the IGMP throttling number for an interface on the switch. Use the **no** form to restore the default setting.

Syntax

ip igmp max-groups *number*

no ip igmp max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 1-1024)

Default Setting

1024

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace” (see the [ip igmp max-groups action](#) command). If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.
- ◆ IGMP throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

ip igmp max-groups action This command sets the IGMP throttling action for an interface on the switch.

Syntax

ip igmp max-groups action {**deny** | **replace**}

deny - The new multicast group join report is dropped.

replace - The new multicast group replaces an existing group.

Default Setting

Deny

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

ip igmp query-drop This command drops any received IGMP query packets. Use the **no** form to restore the default setting.

Syntax

[no] ip igmp query-drop

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp query-drop
Console(config-if)#
```

ip multicast-data-drop This command drops all multicast data packets. Use the **no** form to disable this feature.

Syntax

[no] ip multicast-data-drop

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command can be used to stop multicast services from being forwarded to users attached to the downstream port (i.e., the interfaces specified by this command).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip multicast-data-drop
Console(config-if)#
```

show ip igmp 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)

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

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip igmp filter
IGMP filter enabled
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
-----
IGMP Profile 19
Deny
Range 239.1.1.1 239.1.1.1
Range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp profile This command displays IGMP filtering profiles created on the switch.

Syntax

show ip igmp profile [*profile-number*]

profile-number - An existing IGMP filter profile number.
(Range: 1-4294967295)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
  Deny
  Range 239.1.1.1 239.1.1.1
  Range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp query-drop This command shows if the specified interface is configured to drop IGMP query packets.

Syntax

show ip igmp throttle interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ip igmp query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

show ip igmp throttle interface This command displays the interface settings for IGMP throttling.

Syntax

show ip igmp throttle interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays information for all interfaces.

Example

```
Console#show ip igmp throttle interface ethernet 1/1
Eth 1/1 Information
                Status : FALSE
                Action : Deny
        Max Multicast Groups : 1024
        Current Multicast Groups : 0

Console#
```

show ip multicast-data-drop This command shows if the specified interface is configured to drop multicast data packets.

Syntax

show ip igmp throttle interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ip multicast-data-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

MLD Snooping

Multicast Listener Discovery (MLD) snooping operates on IPv6 traffic and performs a similar function to IGMP snooping for IPv4. That is, MLD snooping dynamically configures switch ports to limit IPv6 multicast traffic so that it is forwarded only to ports with users that want to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs.

There are two versions of the MLD protocol, version 1 and version 2. MLDv1 control packets include Listener Query, Listener Report, and Listener Done messages (equivalent to IGMPv2 query, report, and leave messages). MLDv2 control packets include MLDv2 query and report messages, as well as MLDv1 report and done messages.

Remember that IGMP Snooping and MLD Snooping are independent functions, and can therefore both function at the same time.

Table 138: MLD Snooping Commands

Command	Function	Mode
ipv6 mld snooping	Enables MLD Snooping globally	GC
ipv6 mld snooping proxy-reporting	Enables MLD Snooping with Proxy Reporting	GC
ipv6 mld snooping querier	Allows the switch to act as the querier for MLD snooping	GC
ipv6 mld snooping query-interval	Configures the interval between sending MLD general query messages	GC
ipv6 mld snooping query-max-response-time	Configures the maximum response time for a general queries	GC
ipv6 mld snooping robustness	Configures the robustness variable	GC
ipv6 mld snooping router-port-expire-time	Configures the router port expire time	GC
ipv6 mld snooping unknown-multicast mode	Sets an action for unknown multicast packets	GC
ipv6 mld snooping unsolicited-report-interval	Specifies how often the upstream interface should transmit unsolicited IGMP reports (when proxy reporting is enabled)	GC
ipv6 mld snooping version	Configures the MLD Snooping version	GC
ipv6 mld snooping vlan immediate-leave	Removes a member port of an IPv6 multicast service if a leave packet is received at that port and MLD immediate-leave is enabled for the parent VLAN	GC
ipv6 mld snooping vlan mrouter	Adds an IPv6 multicast router port	GC
ipv6 mld snooping vlan static	Adds an interface as a member of a multicast group	GC
clear ipv6 mld snooping groups dynamic	Clears multicast group information dynamically learned through MLD snooping	PE
clear ipv6 mld snooping statistics	Clears MLD snooping statistics	PE
show ipv6 mld snooping	Displays MLD Snooping configuration	PE
show ipv6 mld snooping group	Displays the learned groups	PE
show ipv6 mld snooping group source-list	Displays the learned groups and corresponding source list	PE
show ipv6 mld snooping mrouter	Displays the information of multicast router ports	PE
show ipv6 mld snooping statistics	Shows IGMP snooping protocol statistics for the specified interface	PE

ipv6 mld snooping This command enables MLD Snooping globally on the switch. Use the **no** form to disable MLD Snooping.

Syntax

[no] ipv6 mld snooping

Default Setting

Disabled

Command Mode

Global Configuration

Example

The following example enables MLD Snooping:

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

ipv6 mld snooping proxy-reporting This command enables IGMP Snooping with Proxy Reporting. Use the **no** form to restore the default setting.

Syntax

[no] ipv6 mld snooping proxy-reporting

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ When proxy reporting is enabled with this command, reports received from downstream hosts are summarized and used to build internal membership states. Proxy-reporting devices may use the all-zeros IP source address when forwarding any summarized reports upstream. For this reason, IGMP membership reports received by the snooping switch must not be rejected because the source IP address is set to 0.0.0.0.

Example

```
Console(config)#ipv6 mld snooping proxy-reporting
Console(config)#
```

ipv6 mld snooping querier This command allows the switch to act as the querier for MLDv2 snooping. Use the **no** form to disable this feature.

Syntax

[no] ipv6 mld snooping querier

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.
- ◆ An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses its own IPv6 address as the query source address.
- ◆ The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.

Example

```
Console(config)#ipv6 mld snooping querier  
Console(config)#
```

ipv6 mld snooping query-interval This command configures the interval between sending MLD general queries. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping query-interval *interval*

no ipv6 mld snooping query-interval

interval - The interval between sending MLD general queries.
(Range: 60-125 seconds)

Default Setting

125 seconds

Command Mode

Global Configuration

Command Usage

- ◆ This command applies when the switch is serving as the querier.

- ◆ An MLD general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.

Example

```
Console(config)#ipv6 mld snooping query-interval 150
Console(config)#
```

ipv6 mld snooping query-max-response- time

This command configures the maximum response time advertised in MLD general queries. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping query-max-response-time *seconds*

no ipv6 mld snooping query-max-response-time

seconds - The maximum response time allowed for MLD general queries.
(Range: 5-25 seconds)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

This command controls how long the host has to respond to an MLD Query message before the switch deletes the group if it is the last member.

Example

```
Console(config)#ipv6 mld snooping query-max-response-time seconds 15
Console(config)#
```

ipv6 mld snooping robustness

This command configures the MLD Snooping robustness variable. Use the **no** form to restore the default value.

Syntax

ipv6 mld snooping robustness *value*

no ipv6 mld snooping robustness

value - The number of the robustness variable. (Range: 2-10)

Default Setting

2

Command Mode

Global Configuration

Command Usage

A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report.

Example

```
Console(config)#ipv6 mld snooping robustness 2
Console(config)#
```

ipv6 mld snooping router-port- expire-time

This command configures the MLD query timeout. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping router-port-expire-time *time*

no ipv6 mld snooping router-port-expire-time

time - Specifies the timeout of a dynamically learned router port.
(Range: 300-500 seconds)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The router port expire time is the time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired.

Example

```
Console(config)#ipv6 mld snooping router-port-expire-time 300
Console(config)#
```

ipv6 mld snooping unknown-multicast mode

This command sets the action for dealing with unknown multicast packets. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping unknown-multicast mode {flood | to-router-port}

no ipv6 mld snooping unknown-multicast mode

flood - Floods the unknown multicast data packets to all ports.

to-router-port - Forwards the unknown multicast data packets to router ports.

Default Setting

to-router-port

Command Mode

Global Configuration

Command Usage

- ◆ When set to “flood,” any received IPv6 multicast packets that have not been requested by a host are flooded to all ports in the VLAN.
- ◆ When set to “router-port,” any received IPv6 multicast packets that have not been requested by a host are forwarded to ports that are connected to a detected multicast router.

Example

```
Console(config)#ipv6 mld snooping unknown-multicast mode flood
Console(config)#
```

ipv6 mld snooping unsolicited-report- interval

This command specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. Use the **no** form to restore the default value.

Syntax

ipv6 mld snooping unsolicited-report-interval *seconds*

no ipv6 mld snooping unsolicited-report-interval

seconds - The interval at which to issue unsolicited reports.
(Range: 1-65535 seconds)

Default Setting

400 seconds

Command Mode

Global Configuration

Command Usage

- ◆ When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.
- ◆ This command only applies when proxy reporting is enabled (see [page 942](#)).

Example

```
Console(config)#ipv6 mld snooping unsolicited-report-interval 5
Console(config)#
```

ipv6 mld snooping version This command configures the MLD snooping version. Use the **no** form to restore the default.

Syntax

ipv6 mld snooping version {1 | 2}

1 - MLD version 1.

2 - MLD version 2.

Default Setting

Version 2

Command Mode

Global Configuration

Example

```
Console(config)#ipv6 mld snooping version 1
Console(config)#
```

ipv6 mld snooping vlan immediate-leave This command immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* immediate-leave

vlan-id - A VLAN identification number. (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ If MLD immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.
- ◆ If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.

Example

The following shows how to enable MLD immediate leave.

```
Console(config)#ipv6 mld snooping immediate-leave
Console(config)#
```

ipv6 mld snooping This command statically configures an IPv6 multicast router port. Use the **no** form
vlan mrouter to remove the configuration.

Syntax

[no] **ipv6 mld snooping vlan** *vlan-id* **mrouter** *interface*

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

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 1 as a multicast router port within VLAN 1:

```
Console(config)#ipv6 mld snooping vlan 1 mrouter ethernet 1/1
Console(config)#
```

ipv6 mld snooping vlan static

This command adds a port to an IPv6 multicast group. Use the **no** form to remove the port.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* static *ipv6-address* interface

vlan - VLAN ID (Range: 1-4094)

ipv6-address - An IPv6 address of a multicast group. (Format: X:X:X::X)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#ipv6 mld snooping vlan 1 static ff05:0:1:2:3:4:5:6 ethernet
1/6
Console(config)#
```

clear ipv6 mld snooping groups dynamic

This command clears multicast group information dynamically learned through MLD snooping.

Syntax

clear ipv6 mld snooping groups dynamic

Command Mode

Privileged Exec

Command Usage

This command only clears entries learned through MLD snooping. Statically configured multicast addresses are not cleared.

Example

```
Console#clear ipv6 mld snooping groups dynamic
Console#
```

clear ipv6 mld snooping statistics

This command clears MLD snooping statistics.

Syntax

clear ipv6 mld snooping statistics [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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

Command Mode

Privileged Exec

Example

```
Console#clear ipv6 mld snooping statistics
Console#
```

show ipv6 mld snooping

This command shows the current MLD Snooping configuration.

Syntax

show ipv6 mld snooping [**vlan** [*vlan-id*]]

vlan-id - VLAN ID (1-4094)

Command Mode

Privileged Exec

Command Usage

This command displays global and VLAN-specific MLD snooping configuration settings.

Example

The following shows MLD Snooping configuration information

```

Console#show ipv6 mld snooping
Service Status           : Disabled
Proxy Reporting          : Disabled
Querier Status           : Disabled
Robustness               : 2
Query Interval           : 125 sec
Query Max Response Time  : 10 sec
Router Port Expiry Time  : 300 sec
Unsolicited Report Interval : 400 sec
Immediate Leave          : Disabled on all VLAN
Immediate Leave By Host  : Disabled on all VLAN
Unknown Flood Behavior   : To Router Port
MLD Snooping Version     : Version 2

VLAN Group IPv6 Address      Port
-----
1          ff05:0:1:2:3:4:5:6 Eth 1/1

Console#show ipv6 mld snooping vlan
VLAN 1
Immediate Leave           : Disabled
Unknown Flood Behavior    : To Router Port
Console#

```

show ipv6 mld snooping group This command shows known multicast groups, member ports, and the means by which each group was learned.

Syntax

show ipv6 mld snooping group

Command Mode

Privileged Exec

Example

The following shows MLD Snooping group configuration information:

```

Console#show ipv6 mld snooping group

Total Entries 3, limit 255

VLAN Multicast IPv6 Address      Member port Type
-----
1          FF02::01:01:01:01 Eth 1/1    MLD Snooping
1          FF02::01:01:01:02 Eth 1/1    Multicast Data
1          FF02::01:01:01:02 Eth 1/1    User

Console#

```

show ipv6 mld snooping group source-list

This command shows known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.

Syntax

show ipv6 mld snooping group source-list [*ipv6-address* | **vlan** *vlan-id*]

ipv6-address - An IPv6 address of a multicast group. (Format: X:X:X:X::X)

vlan-id - VLAN ID (1-4094)

Command Mode

Privileged Exec

Example

The following shows MLD Snooping group mapping information:

```

Console#show ipv6 mld snooping group source-list

VLAN ID                : 1
Multicast IPv6 Address  : FF02::01:01:01:01
Member Port             : Eth 1/1
Type                    : MLD Snooping
Filter Mode             : Include
(if exclude filter mode)
Filter Timer elapse     : 10 sec.
Request List            : ::01:02:03:04, ::01:02:03:05, ::01:02:03:06,
                        ::01:02:03:07
Exclude List            : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                        ::02:02:03:07
(if include filter mode)
Include List            : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                        ::02:02:03:06

Option:
  Filter Mode: Include, Exclude

Console#

```

show ipv6 mld snooping mrouter

This command shows MLD Snooping multicast router information.

Syntax

show ipv6 mld snooping mrouter vlan *vlan-id*

vlan-id - A VLAN identification number. (Range: 1-4094)

Command Mode

Privileged Exec

Example

```

Console#show ipv6 mld snooping mrouter vlan 1
VLAN Multicast Router Port Type      Expire
-----
1 Eth 1/ 2                      Static
Console#

```

**show ipv6 mld
snooping statistics**

This command shows MLD snooping protocol statistics for the specified interface.

Syntax**show ipv6 mld snooping statistics**

```

{input [interface interface] |
output [interface interface] |
query [vlan vlan-id] |
summary interface interface}

```

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

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

query - Displays IGMP snooping-related statistics.

Default Setting

None

Command Mode

Privileged Exec

Example

The following shows MLD protocol statistics input:

```

Console#show ipv6 mld snooping statistics input interface ethernet 1/1
Input Statistics:
Interface Report    Leave    G Query  G(-S)-S Query Drop    Join Succ Group
-----
Eth 1/ 1           23       11        4           10        5         14        5
Console#

```

MLD Filtering and Throttling

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.

Table 139: MLD Filtering and Throttling Commands

Command	Function	Mode
<code>ipv6 mld filter</code>	Enables MLD filtering and throttling on the switch	GC
<code>ipv6 mld profile</code>	Sets a profile number and enters MLD filter profile configuration mode	GC
<code>permit, deny</code>	Sets a profile access mode to permit or deny	IPC
<code>range</code>	Specifies one or a range of multicast addresses for a profile	IPC
<code>ipv6 mld filter</code>	Assigns an MLD filter profile to an interface	IC
<code>ipv6 mld max-groups</code>	Specifies an M:D throttling number for an interface	IC
<code>ipv6 mld max-groups action</code>	Sets the MLD throttling action for an interface	IC
<code>ipv6 mld query-drop</code>	Drops any received MLD query packets	IC
<code>show ipv6 mld filter</code>	Displays the MLD filtering status	PE
<code>show ipv6 mld profile</code>	Displays MLD profiles and settings	PE
<code>show ipv6 mld query-drop</code>	Shows if the interface is configured to drop MLD query packets	PE
<code>show ipv6 mld throttle interface</code>	Displays the MLD throttling setting for interfaces	PE

ipv6 mld filter This command globally enables MLD filtering and throttling on the switch. Use the **no** form to disable the feature.
(Global Configuration)

Syntax

[no] ipv6 mld filter

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ MLD filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An MLD filter profile can contain one or more, or a range of multicast addresses; but only one profile

can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.

- ◆ MLD filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.
- ◆ The MLD filtering feature operates in the same manner when MVR6 is used to forward multicast traffic.

Example

```
Console(config)#ipv6 mld filter
Console(config)#
```

Related Commands

[show ipv6 mld filter](#)

ipv6 mld profile This command creates an MLD filter profile number and enters MLD profile configuration mode. Use the **no** form to delete a profile number.

Syntax

[no] ipv6 mld profile *profile-number*

profile-number - An MLD filter profile number. (Range: 1-4294967295)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

Example

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#
```

Related Commands

[show ipv6 mld profile](#)

permit, deny This command sets the access mode for an MLD filter profile. Use the **no** form to delete a profile number.

Syntax

{**permit** | **deny**}

Default Setting

deny

Command Mode

MLD Profile Configuration

Command Usage

- ◆ Each profile has only one access mode; either permit or deny.
- ◆ When the access mode is set to permit, MLD join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, MLD join reports are only processed when a multicast group is not in the controlled range.

Example

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#permit
Console(config-mld-profile)#
```

range This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

Syntax

[**no**] **range** *low-ipv6-address* [*high-ipv6-address*]

low-ipv6-address - A valid IPv6 address (X:X:X::X) of a multicast group or start of a group range.

high-ipv6-address - A valid IPv6 address (X:X:X:X::X) for the end of a multicast group range.

Default Setting

None

Command Mode

MLD Profile Configuration

Command Usage

Enter this command multiple times to specify more than one multicast address or address range for a profile.

Example

```
Console(config-mld-profile)#range ff01::0101 ff01::0202
Console(config-mld-profile)#
```

ipv6 mld filter (Interface Configuration) This command assigns an MLD filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

Syntax

[no] ipv6 mld filter *profile-number*

profile-number - An MLD filter profile number. (Range: 1-4294967295)

Default Setting

None

Command Mode

Interface Configuration

Command Usage

- ◆ The MLD filtering profile must first be created with the [ipv6 mld profile](#) command before being able to assign it to an interface.
- ◆ Only one profile can be assigned to an interface.
- ◆ A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld filter 19
Console(config-if)#
```

ipv6 mld max-groups This command configures the maximum number of MLD groups that an interface can join. Use the **no** form to restore the default setting.

Syntax

ipv6 mld max-groups *number*

no ipv6 mld max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 1-255)

Default Setting

255

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.
- ◆ MLD throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.
- ◆ If the maximum number of MLD groups is set to the default value, the running status of MLD throttling will change to false. This means that any configuration for MLD throttling will have no effect until the maximum number of MLD groups is configured to another value.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld max-groups 10
Console(config-if)#
```

ipv6 mld max-groups action

This command sets the MLD throttling action for an interface on the switch.

Syntax

ipv6 mld max-groups action {deny | replace}

deny - The new multicast group join report is dropped.

replace - The new multicast group replaces an existing group.

Default Setting

Deny

Command Mode

Interface Configuration (Ethernet)

Command Usage

When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld max-groups action replace
Console(config-if)#
```

ipv6 mld query-drop This command drops any received MLD query packets. Use the no form to restore the default setting.

Syntax

[no] **ipv6 mld query-drop**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld query-drop
Console(config-if)#
```

show ipv6 mld filter This command displays the global and interface settings for MLD filtering.

Syntax

show ipv6 mld filter [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ipv6 mld filter
  MLD filter Enabled
Console#show ipv6 mld filter interface ethernet 1/3
Ethernet 1/3 information
-----
  MLD Profile 19
  Deny
  Range ff01::101          ff01::faa
Console#
```

show ipv6 mld profile This command displays MLD filtering profiles created on the switch.

Syntax

show ipv6 mld profile [*profile-number*]

profile-number - An existing MLD filter profile number.
(Range: 1-4294967295)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ipv6 mld profile
  MLD Profile 19
  MLD Profile 50
Console#show ipv6 mld profile 19
  MLD Profile 19
  Deny
  Range ff01::101          ff01::faa
Console#
```

show ipv6 mld query-drop This command shows if the specified interface is configured to drop MLD query packets.

Syntax

show ipv6 mld query-drop interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ipv6 mld query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

show ipv6 mld throttle interface This command displays the interface settings for MLD throttling.

Syntax

show ipv6 mld throttle interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays information for all interfaces.

Example

```
Console#show ipv6 mld throttle interface ethernet 1/3
Eth 1/3 Information
  Status                : TRUE
  Action                 : Replace
  Max Multicast Groups   : 10
  Current Multicast Groups : 0

Console#
```

LLDP Commands

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1AB standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Table 140: LLDP Commands

Command	Function	Mode
<code>lldp</code>	Enables LLDP globally on the switch	GC
<code>lldp holdtime-multiplier</code>	Configures the time-to-live (TTL) value sent in LLDP advertisements	GC
<code>lldp med-fast-start-count</code>	Configures how many medFastStart packets are transmitted	GC
<code>lldp notification-interval</code>	Configures the allowed interval for sending SNMP notifications about LLDP changes	GC
<code>lldp refresh-interval</code>	Configures the periodic transmit interval for LLDP advertisements	GC
<code>lldp reinit-delay</code>	Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down	GC
<code>lldp tx-delay</code>	Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables	GC
<code>lldp admin-status</code>	Enables LLDP transmit, receive, or transmit and receive mode on the specified port	IC
<code>lldp basic-tlv management-ip-address</code>	Configures an LLDP-enabled port to advertise the management address for this device	IC
<code>lldp basic-tlv port-description</code>	Configures an LLDP-enabled port to advertise its port description	IC
<code>lldp basic-tlv system-capabilities</code>	Configures an LLDP-enabled port to advertise its system capabilities	IC

Table 140: LLDP Commands (Continued)

Command	Function	Mode
<code>lldp basic-tlv system-description</code>	Configures an LLDP-enabled port to advertise the system description	IC
<code>lldp basic-tlv system-name</code>	Configures an LLDP-enabled port to advertise its system name	IC
<code>lldp dot1-tlv proto-ident*</code>	Configures an LLDP-enabled port to advertise the supported protocols	IC
<code>lldp dot1-tlv proto-vid*</code>	Configures an LLDP-enabled port to advertise port-based protocol related VLAN information	IC
<code>lldp dot1-tlv pvid*</code>	Configures an LLDP-enabled port to advertise its default VLAN ID	IC
<code>lldp dot1-tlv vlan-name*</code>	Configures an LLDP-enabled port to advertise its VLAN name	IC
<code>lldp dot3-tlv link-aggr</code>	Configures an LLDP-enabled port to advertise its link aggregation capabilities	IC
<code>lldp dot3-tlv mac-phy</code>	Configures an LLDP-enabled port to advertise its MAC and physical layer specifications	IC
<code>lldp dot3-tlv max-frame</code>	Configures an LLDP-enabled port to advertise its maximum frame size	IC
<code>lldp med-location civic-addr</code>	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
<code>lldp med-notification</code>	Enables the transmission of SNMP trap notifications about LLDP-MED changes	IC
<code>lldp med-tlv inventory</code>	Configures an LLDP-MED-enabled port to advertise its inventory identification details	IC
<code>lldp med-tlv location</code>	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
<code>lldp med-tlv med-cap</code>	Configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities	IC
<code>lldp med-tlv network-policy</code>	Configures an LLDP-MED-enabled port to advertise its network policy configuration	IC
<code>lldp notification</code>	Enables the transmission of SNMP trap notifications about LLDP changes	IC
<code>show lldp config</code>	Shows LLDP configuration settings for all ports	PE
<code>show lldp info local-device</code>	Shows LLDP global and interface-specific configuration settings for this device	PE
<code>show lldp info remote-device</code>	Shows LLDP global and interface-specific configuration settings for remote devices	PE
<code>show lldp info statistics</code>	Shows statistical counters for all LLDP-enabled interfaces	PE

* Vendor-specific options may or may not be advertised by neighboring devices.

lldp This command enables LLDP globally on the switch. Use the **no** form to disable LLDP.

Syntax

[no] lldp

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#lldp
Console(config)#
```

lldp holdtime-multiplier This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the **no** form to restore the default setting.

Syntax

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

value - Calculates the TTL in seconds based on the following rule:
minimum of ((Transmission Interval * Holdtime Multiplier), or 65536)

(Range: 2 - 10)

Default Setting

Holdtime multiplier: 4

TTL: 4*30 = 120 seconds

Command Mode

Global Configuration

Command Usage

The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

Example

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```


lldp med-fast-start-count This command specifies the amount of MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism. Use the **no** form to restore the default setting.

Syntax

lldp med-fast-start-count *packets*

no lldp med-fast-start-count

seconds - Amount of packets. (Range: 1-10 packets; Default: 4 packets)

Default Setting

4 packets

Command Mode

Global Configuration

Command Usage

This parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

Example

```
Console(config)#lldp med-fast-start-count 6
Console(config)#
```

lldp notification-interval This command configures the allowed interval for sending SNMP notifications about LLDP MIB changes. Use the **no** form to restore the default setting.

Syntax

lldp notification-interval *seconds*

no lldp notification-interval

seconds - Specifies the periodic interval at which SNMP notifications are sent. (Range: 5 - 3600 seconds)

Default Setting

5 seconds

Command Mode

Global Configuration

Command Usage

- ◆ This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.

- ◆ Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of `IldpStatsRemTableLastChangeTime` to detect any `IldpRemTablesChange` notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#lldp notification-interval 30
Console(config)#
```

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 870](#)).

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 864](#) and [“protocol-vlan protocol-group \(Configuring Interfaces\)” on page 871](#).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

lldp dot3-tlv link-agg This command configures an LLDP-enabled port to advertise link aggregation capabilities. Use the **no** form to disable this feature.

Syntax

[no] **lldp dot3-tlv link-agg**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises link aggregation capabilities, aggregation status of the link, and the 802.3 aggregated port identifier if this interface is currently a link aggregation member.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

lldp dot3-tlv mac-phy This command configures an LLDP-enabled port to advertise its MAC and physical layer capabilities. Use the **no** form to disable this feature.

Syntax

[no] **lldp dot3-tlv mac-phy**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises MAC/PHY configuration/status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

lldp dot3-tlv max-frame This command configures an LLDP-enabled port to advertise its maximum frame size. Use the **no** form to disable this feature.

Syntax

[no] **lldp dot3-tlv max-frame**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Refer to [“Frame Size” on page 539](#) for information on configuring the maximum frame size for this switch.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

lldp med-location civic-addr This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to restore the default settings.

Syntax

lldp med-location civic-addr [[**country** *country-code*] | [**what** *device-type*] | [*ca-type* *ca-value*]]

no lldp med-location civic-addr [[**country**] | [**what**] | [*ca-type*]]

country-code – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

device-type – The type of device to which the location applies.

0 – Location of DHCP server.

1 – Location of network element closest to client.

2 – Location of client.

ca-type – A one-octet descriptor of the data civic address value. (Range: 0-255)

ca-value – Description of a location. (Range: 1-32 characters)

Default Setting

Not advertised

No description

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ Use this command without any keywords to advertise location identification details.
- ◆ Use the *ca-type* to advertise the physical location of the device, that is the city, street number, building and room information. The address location is specified as a type and value pair, with the civic address (CA) type being defined in RFC 4776. The following table describes some of the CA type numbers and provides examples.

Table 141: LLDP MED Location CA Types

CA Type	Description	CA Value Example
1	National subdivisions (state, canton, province)	California
2	County, parish	Orange
3	City, township	Irvine
4	City division, borough, city district	West Irvine
5	Neighborhood, block	Riverside

Table 141: LLDP MED Location CA Types (Continued)

CA Type	Description	CA Value Example
6	Group of streets below the neighborhood level	Exchange
18	Street suffix or type	Avenue
19	House number	320
20	House number suffix	A
21	Landmark or vanity address	Tech Center
26	Unit (apartment, suite)	Apt 519
27	Floor	5
28	Room	509B

Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.

- ◆ For the location options defined for *device-type*, normally option **2** is used to specify the location of the client device. In situations where the client device location is not known, **0** and **1** can be used, providing the client device is physically close to the DHCP server or network element.

Example

The following example enables advertising location identification details.

```

Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-location civic-addr
Console(config-if)#lldp med-location civic-addr 1 California
Console(config-if)#lldp med-location civic-addr 2 Orange
Console(config-if)#lldp med-location civic-addr 3 Irvine
Console(config-if)#lldp med-location civic-addr 4 West Irvine
Console(config-if)#lldp med-location civic-addr 6 Exchange
Console(config-if)#lldp med-location civic-addr 18 Avenue
Console(config-if)#lldp med-location civic-addr 19 320
Console(config-if)#lldp med-location civic-addr 27 5
Console(config-if)#lldp med-location civic-addr 28 509B
Console(config-if)#lldp med-location civic-addr country US
Console(config-if)#lldp med-location civic-addr what 2
Console(config-if)#

```

lldp med-notification This command enables the transmission of SNMP trap notifications about LLDP-MED changes. Use the **no** form to disable LLDP-MED notifications.

Syntax

[no] lldp med-notification

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This option sends out SNMP trap notifications to designated target stations at the interval specified by the `lldp notification-interval` command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA 1057), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- ◆ SNMP trap destinations are defined using the `snmp-server host` command.
- ◆ Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-notification
Console(config-if)#
```

lldp med-tlv inventory This command configures an LLDP-MED-enabled port to advertise its inventory identification details. Use the **no** form to disable this feature.

Syntax

[no] **lldp med-tlv inventory**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv inventory
Console(config-if)#
```

lldp med-tlv location This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to disable this feature.

Syntax

[no] lldp med-tlv location

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises location identification details.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv location
Console(config-if)#
```

lldp med-tlv med-cap This command configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities. Use the **no** form to disable this feature.

Syntax

[no] lldp med-tlv med-cap

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv med-cap
Console(config-if)#
```

lldp med-tlv network-policy This command configures an LLDP-MED-enabled port to advertise its network policy configuration. Use the **no** form to disable this feature.

Syntax

[no] **lldp med-tlv network-policy**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv network-policy
Console(config-if)#
```

lldp notification This command enables the transmission of SNMP trap notifications about LLDP changes. Use the **no** form to disable LLDP notifications.

Syntax

[no] **lldp notification**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- ◆ This option sends out SNMP trap notifications to designated target stations at the interval specified by the **lldp notification-interval** command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- ◆ SNMP trap destinations are defined using the **snmp-server host** command.
- ◆ Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should

therefore periodically check the value of `lldpStatsRemTableLastChangeTime` to detect any `lldpRemTablesChange` notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

show lldp config This command shows LLDP configuration settings for all ports.

Syntax

show lldp config [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Command Mode

Privileged Exec

Example

The following example shows all basic LLDP parameters are enabled on Port 1.

```
Console#show lldp config

LLDP Global Configuration

LLDP Enabled                : Yes
LLDP Transmit Interval      : 30 seconds
LLDP Hold Time Multiplier   : 4
LLDP Delay Interval         : 2 seconds
LLDP Re-initialization Delay : 2 seconds
LLDP Notification Interval  : 5 seconds
LLDP MED Fast Start Count   : 4

LLDP Port Configuration
Port      Admin Status Notification Enabled
-----
Eth 1/1   Tx-Rx          True
Eth 1/2   Tx-Rx          True
Eth 1/3   Tx-Rx          True
Eth 1/4   Tx-Rx          True
Eth 1/5   Tx-Rx          True
.
.
.
```



```

Console#show lldp config detail ethernet 1/1
LLDP Port Configuration Detail
  Port : Eth 1/1
  Admin Status : Tx-Rx
  Notification Enabled : True
  Basic TLVs Advertised : port-description
                        system-name
                        system-description
                        system-capabilities
                        management-ip-address
  802.1 specific TLVs Advertised : port-vid
                                vlan-name
                                proto-vlan
                                proto-ident
  802.3 specific TLVs Advertised : mac-phy
                                link-agg
                                max-frame
  MED Notification Status : Enabled
  MED Enabled TLVs Advertised : med-cap
                              network-policy
                              location
                              ext-poe
                              inventory
  MED Location Identification:
  Location Data Format : Civic Address LCI
  Civic Address Status : Enabled
  Country Name : US
  What : 2
  CA-Type : 1
  CA-Value : Alabama
  CA-Type : 2
  CA-Value : Tuscaloosa

Console#

```

show lldp info local-device This command shows LLDP global and interface-specific configuration settings for this device.

Syntax

show lldp info local-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Command Mode

Privileged Exec

Example

```

Console#show lldp info local-device
LLDP Local Global Information
  Chassis Type           : MAC Address
  Chassis ID             : 00-11-3B-D7-A6-84
  System Name            :
  System Description     : SP6528
  System Capabilities Support : Bridge
  System Capabilities Enabled : Bridge
  Management Address     : 192.168.16.28 (IPv4)

LLDP Local Port Information
  Port      Port ID Type      Port ID      Port Description
  -----
  Eth 1/1   MAC Address      00-11-3B-D7-A6-85 Ethernet Port on unit 1, port 1
  Eth 1/2   MAC Address      00-11-3B-D7-A6-86 Ethernet Port on unit 1, port 2
  Eth 1/3   MAC Address      00-11-3B-D7-A6-87 Ethernet Port on unit 1, port 3
  Eth 1/4   MAC Address      00-11-3B-D7-A6-88 Ethernet Port on unit 1, port 4
  Eth 1/5   MAC Address      00-11-3B-D7-A6-89 Ethernet Port on unit 1, port 5
  Eth 1/6   MAC Address      00-11-3B-D7-A6-8A Ethernet Port on unit 1, port 6
  .
  .
Console#show lldp info local-device detail ethernet 1/1
LLDP Local Port Information Detail
  Port           : Eth 1/1
  Port ID Type   : MAC Address
  Port ID        : 00-11-3B-D7-A6-85
  Port Description : Ethernet Port on unit 1, port 1
  MED Capability : LLDP-MED Capabilities
                  Network Policy
                  Location Identification
                  Inventory
Console#

```

show lldp info remote-device This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

Syntax

show lldp info remote-device [**detail** *interface*]

detail - Shows detailed information.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

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

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

Command Mode

Privileged Exec

Example

Note that an IP phone or other end-node device which advertises LLDP-MED capabilities must be connected to the switch for information to be displayed in the “LLDP-MED Capability” and other related fields.

```

Console#show lldp info remote-device
LLDP Remote Devices Information
Interface Chassis ID      Port ID      System Name
-----
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)

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

Command Mode

Privileged Exec

Example

```

Console#show lldp info statistics
LLDP Global Statistics
Neighbor Entries List Last Updated : 485 seconds
New Neighbor Entries Count          : 2
Neighbor Entries Deleted Count      : 1
Neighbor Entries Dropped Count      : 0
Neighbor Entries Ageout Count       : 1

LLDP Port Statistics
Port      NumFramesRecvd NumFramesSent NumFramesDiscarded
-----
Eth 1/1   12             12             0
Eth 1/2   17             17             0
Eth 1/3    0              0              0
Eth 1/4    0              0              0
Eth 1/5    0              0              0
:
Console#show lldp info statistics detail ethernet 1/1
LLDP Port Statistics Detail
Port Name      : Eth 1/1
Frames Discarded : 0
Frames Invalid  : 0
Frames Received : 12
Frames Sent     : 12
TLVs Unrecognized : 0
TLVs Discarded  : 0
Neighbor Ageouts : 1
Console#

```

Domain Name Service Commands

These commands are used to configure Domain Naming System (DNS) services. Entries can be manually configured in the DNS domain name to IP address mapping table, default domain names configured, or one or more name servers specified to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the `ip name-server` command and domain lookup is enabled with the `ip domain-lookup` command.

Table 142: Address Table Commands

Command	Function	Mode
<code>ip domain-list</code>	Defines a list of default domain names for incomplete host names	GC
<code>ip domain-lookup</code>	Enables DNS-based host name-to-address translation	GC
<code>ip domain-name</code>	Defines a default domain name for incomplete host names	GC
<code>ip host</code>	Creates a static IPv4 host name-to-address mapping	GC
<code>ip name-server</code>	Specifies the address of one or more name servers to use for host name-to-address translation	GC
<code>ipv6 host</code>	Creates a static IPv6 host name-to-address mapping	GC
<code>clear dns cache</code>	Clears all entries from the DNS cache	PE
<code>clear host</code>	Deletes entries from the host name-to-address table	PE
<code>show dns</code>	Displays the configuration for DNS services	PE
<code>show dns cache</code>	Displays entries in the DNS cache	PE
<code>show hosts</code>	Displays the static host name-to-address mapping table	PE

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 \(987\)](#)

ip domain-lookup This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

Syntax

[no] ip domain-lookup

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ At least one name server must be specified before DNS can be enabled.

- ◆ If one or more name servers are configured, but DNS is not yet enabled and the switch receives a DHCP packet containing a DNS field with a list of DNS servers, then the switch will automatically enable DNS host name-to-address translation.
- ◆ If all name servers are deleted, DNS will automatically be disabled.

Example

This example enables DNS and then displays the configuration.

```

Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#

```

Related Commands

[ip domain-name \(987\)](#)

[ip name-server \(989\)](#)

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 \(985\)](#)

[ip name-server \(989\)](#)

[ip domain-lookup \(986\)](#)

ip host This command creates a static entry in the DNS table that maps a host name to an IPv4 address. Use the **no** form to remove an entry.

Syntax

[no] ip host *name address*

name - Name of an IPv4 host. (Range: 1-127 characters)

address - Corresponding IPv4 address.

Default Setting

No static entries

Command Mode

Global Configuration

Command Usage

Use the **no ip host** command to clear static entries, or the [clear host](#) command to clear dynamic entries.

Example

This example maps an IPv4 address to a host name.

```

Console(config)#ip host rd5 192.168.1.55
Console(config)#end
Console#show hosts
No.  Flag Type      IP Address          TTL  Domain
---  ---  ---
0    2 Address 192.168.1.55      rd5
Console#

```


ip name-server This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

Syntax

```
[no] ip name-server server-address1 [server-address2 ...  
server-address6]
```

server-address1 - IPv4 or IPv6 address of domain-name server.

server-address2 ... server-address6 - IPv4 or IPv6 address of additional domain-name servers.

Default Setting

None

Command Mode

Global Configuration

Command Usage

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Example

This example adds two domain-name servers to the list and then displays the list.

```
Console(config)#ip name-server 192.168.1.55 10.1.0.55  
Console(config)#end  
Console#show dns  
Domain Lookup Status:  
  DNS disabled  
Default Domain Name:  
  sample.com  
Domain Name List:  
  sample.com.jp  
  sample.com.uk  
Name Server List:  
  192.168.1.55  
  10.1.0.55  
Console#
```

Related Commands

[ip domain-name \(987\)](#)

[ip domain-lookup \(986\)](#)

ipv6 host This command creates a static entry in the DNS table that maps a host name to an IPv6 address. Use the **no** form to remove an entry.

Syntax

[no] ipv6 host name ipv6-address

name - Name of an IPv6 host. (Range: 1-127 characters)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Default Setting

No static entries

Command Mode

Global Configuration

Example

This example maps an IPv6 address to a host name.

```

Console(config)#ipv6 host rd6 2001:0db8:1::12
Console(config)#end
Console#show hosts
No.  Flag Type      IP Address          TTL  Domain
-----
0    2 Address 192.168.1.55          rd5
1    2 Address 2001:DB8:1::12      rd6
Console#

```

clear dns cache This command clears all entries in the DNS cache.

Command Mode

Privileged Exec

Example

```

Console#clear dns cache
Console#show dns cache
No.  Flag Type      IP Address          TTL  Host
-----
Console#

```

clear host This command deletes dynamic entries from the DNS table.

Syntax

clear host {*name* | *}

name - Name of the host. (Range: 1-127 characters)

* - Removes all entries.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Use the **clear host** command to clear dynamic entries, or the **no ip host** command to clear static entries.

Example

This example clears all dynamic entries from the DNS table.

```
Console#clear host *
Console#
```

show dns This command displays the configuration of the DNS service.

Command Mode

Privileged Exec

Example

```
Console#show dns
Domain Lookup Status:
  DNS enabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
  192.168.1.55
  10.1.0.55
Console#
```

show dns cache This command displays entries in the DNS cache.

Command Mode

Privileged Exec

Example

```

Console#show dns cache
No.      Flag    Type    IP Address      TTL    Host
-----
      3      4 Host    209.131.36.158  115    www-real.wa1.b.yahoo.com
      4      4 CNAME   POINTER TO:3    115    www.yahoo.com
      5      4 CNAME   POINTER TO:3    115    www.wa1.b.yahoo.com
Console#

```

Table 143: show dns cache - display description

Field	Description
No.	The entry number for each resource record.
Flag	The flag is always "4" indicating a cache entry and therefore unreliable.
Type	This field includes "Host" which specifies the primary name for the owner, and "CNAME" which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.
IP Address	The IP address associated with this record.
TTL	The time to live reported by the name server.
Host	The host name associated with this record.

show hosts This command displays the static host name-to-address mapping table.

Command Mode

Privileged Exec

Example

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```

Console#show hosts
No.  Flag Type    IP Address      TTL    Host
-----
  0   2 Address 192.168.1.55      rd5
  1   2 Address 2001:DB8:1::12    rd6
  3   4 Address 209.131.36.158    65    www-real.wa1.b.yahoo.com
  4   4 CNAME   POINTER TO:3      65    www.yahoo.com
  5   4 CNAME   POINTER TO:3      65    www.wa1.b.yahoo.com
Console#

```

Table 144: show hosts - display description

Field	Description
No.	The entry number for each resource record.
Flag	The field displays "2" for a static entry, or "4" for a dynamic entry stored in the cache.
Type	This field includes "Address" which specifies the primary name for the owner, and "CNAME" which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.
IP Address	The IP address associated with this record.
TTL	The time to live reported by the name server. This field is always blank for static entries.
Host	The host name associated with this record.

DHCP Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client and relay functions. Any VLAN interface on this switch can be configured to automatically obtain an IP address through DHCP. This switch can also be configured to relay DHCP client configuration requests to a DHCP server on another network.

Table 145: DHCP Commands

Command Group	Function
DHCP Client	Allows interfaces to dynamically acquire IP address information

DHCP Client

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

Table 146: DHCP Client Commands

Command	Function	Mode
<i>DHCP for IPv4</i>		
<code>ip dhcp dynamic-provision</code>	Enables dynamic provision via DHCP	GC
<code>ip dhcp client class-id</code>	Specifies the DHCP client identifier for an interface	IC
<code>ip dhcp restart client</code>	Submits a BOOTP or DHCP client request	PE
<code>show ip dhcp dynamic-provision</code>	Shows the status of dynamic provision via DHCP	PE
<i>DHCP for IPv6</i>		
<code>ipv6 dhcp client rapid-commit vlan</code>	Specifies the Rapid Commit option for DHCPv6 message exchange	GC
<code>ipv6 dhcp restart client vlan</code>	Submits a DHCPv6 client request	PE
<code>show ipv6 dhcp duid</code>	Shows the DHCP Unique Identifier for this switch	PE
<code>show ipv6 dhcp vlan</code>	Shows DHCPv6 information for specified interface	PE

DHCP for IPv4

ip dhcp dynamic-provision This command enables dynamic provisioning via DHCP. Use the **no** form to disable this feature.

Syntax

[no] ip dhcp dynamic-provision

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

DHCPD is the daemon used by Linux to dynamically configure TCP/IP information for client systems. To support DHCP option 66/67, you have to add corresponding statements to the configuration file of DHCPD. Information on how to complete this process are described in [“Downloading a Configuration File and Other Parameters From a DHCP Server” on page 78](#).

The following are some alternative commands which can be added to the DHCPD to complete the dynamic provisioning process.

By default, the parameters for DHCP option 66/67 are not carried by the reply sent from the DHCP server. To ask for a DHCP reply with option 66/67, the client can inform the server that it is interested in option 66/67 by sending a DHCP request that includes a 'parameter request list' option. Besides this, the client can also send a DHCP request that includes a 'vendor class identifier' option to the server so that the DHCP server can identify the device, and determine what information should be given to requesting device.

The following are two additional sample configurations of the dhcpd.conf file for the server version dhcp-3.0.4rc1, you can choose either one of them.

1. Define the conditions in subnet section:

```
shared-network Sample1 {  
    subnet 192.168.1.0 netmask 255.255.255.0 {  
        # option 55  
        option dhcp-parameter-request-list 1,66,67;  
        # option 66  
        option tftp-server-name "192.168.1.1";  
        # option 67  
        option bootfile-name "dhcp_config.cfg";  
    }  
}
```

2. Define the conditions in class section:

```

class "OPT66_67" { # for option 66/67
# option 124
    match if option vendor-class-identifier = "Micronet";
# option 55
    option dhcp-parameter-request-list 1,66,67;
# option 66
    option tftp-server-name "192.168.1.1";
# option 67
    option bootfile-name "dhcp_config.cfg";
}

shared-network Sample2 {
subnet 192.168.1.0 netmask 255.255.255.0 {
    }
    pool {
        allow members of "OPT66_67";
        range 192.168.1.10 192.168.1.20;
    }
}

```

Example

In the following example enables dhcp dynamic provisioning.

```

Console(config)#ip dhcp dynamic provisioning
Console(config)#

```

ip dhcp client class-id This command specifies the DHCP client vendor class identifier for the current interface. Use the **no** form to remove the class identifier from the DHCP packet.

Syntax

ip dhcp client class-id [**text** *text* | **hex** *hex*]

no ip dhcp client class-id

text - A text string. (Range: 1-32 characters)

hex - A hexadecimal value. (Range: 1-64 characters)

Default Setting

Class identifier option enabled, using the model number as the string

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Use this command without any keyword to restore the default setting.

- ◆ This command is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.
- ◆ The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator. Options 60, 66 and 67 statements can be added to the server daemon's configuration file.

Table 147: 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 148: Options 55 and 124 Statements

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

- ◆ The server should reply with Option 66 attributes, including the TFTP server name and boot file name.
- ◆ Note that the vendor class identifier can be formatted in either text or hexadecimal using the **ip dhcp client class-id** command, but the format used by both the client and server must be the same.

Example

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 000011112222
Console(config-if)#
```

Related Commands

[ip dhcp restart client \(998\)](#)

ip dhcp restart client This command submits a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode through the [ip address](#) command.
- ◆ DHCP requires the server to reassign the client's last address if available.
- ◆ If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-E0-00-00-00-01
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.2 Mask: 255.255.255.0
  Proxy ARP is disabled
  DHCP Client Vendor Class ID (text): SP6528
  DHCP Relay Server:
Console#
```

Related Commands

[ip address \(1004\)](#)

show ip dhcp dynamic-provision This command shows the status of dynamic provision via DHCP.

Command Mode

Privileged Exec

Example

```
Console#show ip dhcp dynamic provisioning
Dynamic Provision via DHCP Status: Disabled
Console#
```

DHCP for IPv6

ipv6 dhcp client rapid-commit vlan This command specifies the Rapid Commit option for DHCPv6 message exchange for all DHCPv6 client requests submitted from the specified interface. Use the **no** form to disable this option.

Syntax

[no] ipv6 dhcp client rapid-commit vlan *vlan-id*

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- ◆ DHCPv6 clients can obtain configuration parameters from a server through a normal four-message exchange (solicit, advertise, request, reply), or through a rapid two-message exchange (solicit, reply). The rapid-commit option must be enabled on both client and server for the two-message exchange to be used.
- ◆ This command allows two-message exchange method for prefix delegation. When enabled, DHCPv6 client requests submitted from the specified interface will include the rapid commit option in all solicit messages.
- ◆ If the rapid commit option has been enabled on the switch with this command, and on the DHCPv6 server, message exchange can be reduced from the normal four step process to a two-step exchange of only solicit and reply messages.

Example

```
Console(config)#ipv6 dhcp client rapid-commit vlan 2
Console(config)#
```

ipv6 dhcp restart client vlan This command submits a DHCPv6 client request.

Syntax

ipv6 dhcp restart client vlan *vlan-id*

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ This command starts the DHCPv6 client process if it is not yet running by submitting requests for configuration information through the specified interface(s). When DHCPv6 is restarted, the switch may attempt to acquire an IP address prefix through stateful address auto-configuration. If the router advertisements have the “other stateful configuration” flag set, the switch may also attempt to acquire other non-address configuration information (such as a default gateway or DNS server) when DHCPv6 is restarted.

Prior to submitting a client request to a DHCPv6 server, the switch should be configured with a link-local address using the [ipv6 address autoconfig](#) command. The state of the Managed Address Configuration flag (M flag) and Other Stateful Configuration flag (O flag) received in Router Advertisement messages will determine the information this switch should attempt to acquire from the DHCPv6 server as described below.

- Both M and O flags are set to 1:

DHCPv6 is used for both address and other configuration settings.

This combination is known as DHCPv6 stateful, in which a DHCPv6 server assigns stateful addresses to IPv6 hosts.

- The M flag is set to 0, and the O flag is set to 1:

DHCPv6 is used only for other configuration settings.

Neighboring routers are configured to advertise non-link-local address prefixes from which IPv6 hosts derive stateless addresses.

This combination is known as DHCPv6 stateless, in which a DHCPv6 server does not assign stateful addresses to IPv6 hosts, but does assign stateless configuration settings.

- ◆ DHCPv6 clients build a list of servers by sending a solicit message and collecting advertised message replies. These servers are then ranked based on their advertised preference value. If the client needs to acquire prefixes from servers, only servers that have advertised prefixes are considered.
- ◆ If the rapid commit option has been enabled on the switch using the [ipv6 dhcp client rapid-commit vlan](#) command, and on the DHCPv6 server, message exchange can be reduced from the normal four step process to a two-step exchange of only solicit and reply messages.

Example

The following command submits a client request on VLAN 1.

```
Console#ipv6 dhcp restart client vlan 1
Console#
```

Related Commands

[ipv6 address autoconfig \(1016\)](#)

show ipv6 dhcp duid This command shows the DHCP Unique Identifier for this switch.

Command Mode

Privileged Exec

Command Usage

DHCPv6 clients and servers are identified by a DHCP Unique Identifier (DUID) included in the client identifier and server identifier options. Static or dynamic address prefixes may be assigned by a DHCPv6 server based on the client's DUID.

Example

```
Console#show ipv6 dhcp duid
DHCPv6 Unique Identifier (DUID): 0001-0001-568A0C9D-00E00C0000FD
Console#
```

show ipv6 dhcp vlan This command shows DHCPv6 information for the specified interface(s).

Syntax

show ipv6 dhcp vlan *vlan-list*

vlan-list - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

Command Usage

Each allocation in the DHCPv6 server is identified by a DUID and an IAID. IAID means Interface Association Identifier, and is a binding between the interface and one or more IP addresses.

Command Mode

Privileged Exec

Example

```
Console#show ipv6 dhcp vlan 1
VLAN 1 is in DHCP client mode , No Rapid-Commit
IAID :                                0
```

```
None of known servers now ...
```

```
Console#
```

RELATED COMMANDS

[ipv6 address \(1015\)](#)

IP Interface Commands

An IP Version 4 and Version 6 address may be used for management access to the switch over the network. Both IPv4 or IPv6 addresses can be used simultaneously to access the switch. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a BOOTP or DHCP server when it is powered on. An IPv6 address can either be manually configured or dynamically generated.

An IPv4 address for this switch is obtained via DHCP by default for VLAN 1. You may also need to establish an IPv4 or IPv6 default gateway between this device and management stations that exist on another network segment.

Table 149: 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 150: 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 151: 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 default-gateway</code>	Displays the default gateway configured for this device	PE
<code>show ip interface</code>	Displays the IP settings for this device	PE
<code>show ip traffic</code>	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE
<code>tracert</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 remove an IP address.

Syntax

ip address *{ip-address netmask [secondary]*
[default-gateway ip-address] | bootp | dhcp}

no ip address *[ip-address netmask [secondary] | dhcp]*

ip-address - IP address

netmask - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets. The network mask can be either in the traditional format xxx.xxx.xxx.xxx or use classless format with the range /5 to /32. For example the subnet 255.255.224.0 would be /19.

secondary - Specifies a secondary IP address.

default-gateway - The default gateway. (Refer to the `ip default-gateway` command which provides the same function.)

bootp - Obtains IP address from BOOTP.

dhcp - Obtains IP address from DHCP.

Default Setting

192.168.2.10/24

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ An IP address must be assigned to this device to gain management access over the network or to connect the router to existing IP subnets. A specific IP address can be manually configured, or the router can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format is not accepted by the configuration program.
- ◆ An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router/switch in a network segment uses a secondary address, all other routers/switches in that segment must also use a secondary address from the same network or subnet address space.
- ◆ If **bootp** or **dhcp** options are selected, the system will immediately start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast periodically by the router in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask). If the DHCP/BOOTP server is slow to respond, you may need to use the [ip dhcp restart client](#) command to re-start broadcasting service requests, or reboot the switch.



Note: Each VLAN group can be assigned its own IP interface address. You can manage the switch via any of these IP addresses.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

This example assigns an IP address to VLAN 2 using a classless network mask.

```
Console(config)#interface vlan 2
Console(config-if)#ip address 10.2.2.1/24
Console(config-if)#
```

Related Commands

[ip dhcp restart client \(998\)](#)
[ip default-gateway \(1006\)](#)
[ipv6 address \(1015\)](#)

ip default-gateway This command specifies the default gateway for destinations not found in local routing tables. Use the **no** form to remove a default gateway.

Syntax

ip default-gateway *gateway*

no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No default gateway is established.

Command Mode

Global Configuration

Command Usage

- ◆ The default gateway can also be defined using the following Global configuration command: **ip route 0.0.0.0 0.0.0.0** *gateway-address*.
- ◆ Static routes can also be defined using the [ip route](#) command to ensure that traffic to the designated address or subnet passes through a preferred gateway.
- ◆ A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the router.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address for a default gateway, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 192.168.0.1
Console(config)#
```

Related Commands

[ip address \(1004\)](#)

[ip route \(788\)](#)

[ipv6 default-gateway \(1014\)](#)

show ip default-gateway This command shows the IPv4 default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip default-gateway
IP default gateway 10.1.0.254
Console#
```

Related Commands

[ip default-gateway \(1006\)](#)

[show ipv6 default-gateway \(1023\)](#)

show ip interface This command displays the settings of an IPv4 interface.

Command Mode

Privileged Exec

Example

```
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-E0-00-00-00-01
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.2 Mask: 255.255.255.0
  DHCP Client Vendor Class ID (text): SFP6528
Console#
```

Related Commands

[ip address \(1004\)](#)

[show ipv6 interface \(1023\)](#)

show ip traffic This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

Command Mode

Privileged Exec

Example

```

Console#show ip traffic
IP Statistics:
IP received
    7845 total received
        header errors
        unknown protocols
        address errors
        discards
    7845 delivers
        reassembly request datagrams
        reassembly succeeded
        reassembly failed

IP sent
    forwards datagrams
    9903 requests
        discards
        no routes
        generated fragments
        fragment succeeded
        fragment failed

ICMP Statistics:
ICMP received
    input
    errors
    destination unreachable messages
    time exceeded messages
    parameter problem message
    echo request messages
    echo reply messages
    redirect messages
    timestamp request messages
    timestamp reply messages
    source quench messages
    address mask request messages
    address mask reply messages

ICMP sent
    output
    errors
    destination unreachable messages
    time exceeded messages
    parameter problem message
    echo request messages
    echo reply messages
    redirect messages
    timestamp request messages
    timestamp reply messages
    source quench messages
    address mask request messages
    address mask reply messages

UDP Statistics:
    input
    no port errors
    other errors
    output

TCP Statistics:
    7841 input
  
```

```
          input errors
    9897 output
Console#
```

traceroute This command shows the route packets take to the specified destination.

Syntax

traceroute *host*

host - IP address or alias of the host.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **traceroute** command to determine the path taken to reach a specified destination.
- ◆ A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- ◆ The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the "Request Timed Out" message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.
- ◆ If the target device does not respond or other errors are detected, the switch will indicate this by one of the following messages:
 - * - No Response
 - H - Host Unreachable
 - N - Network Unreachable
 - P - Protocol Unreachable
 - O -Other

Example

```
Console#traceroute 192.168.0.1
Press "ESC" to abort.
Traceroute to 192.168.0.99, 30 hops max, timeout is 3 seconds
Hop Packet 1 Packet 2 Packet 3 IP Address
---
1      20 ms    <10 ms    <10 ms 192.168.0.99

Trace completed.
Console#
```

ping This command sends (IPv4) ICMP echo request packets to another node on the network.

Syntax

ping *host* [**count** *count*] [**size** *size*]

host - IP address or alias of the host.

count - Number of packets to send. (Range: 1-16)

size - Number of bytes in a packet. (Range: 32-512)

The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

Default Setting

count: 5

size: 32 bytes

Command Mode

Normal Exec, Privileged Exec

Command Usage

- ◆ Use the ping command to see if another site on the network can be reached.
- ◆ The following are some results of the **ping** command:
 - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
 - *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.
 - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
 - *Network or host unreachable* - The gateway found no corresponding entry in the route table.

- ◆ When pinging a host name, be sure the DNS server has been defined (page 989) and host name-to-address translation enabled (page 986). If necessary, local devices can also be specified in the DNS static host table (page 988).

Example

```
Console#ping 10.1.0.9
Press ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
    5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
    Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

[interface \(758\)](#)

ARP Configuration This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

Table 152: Address Resolution Protocol Commands

Command	Function	Mode
arp timeout	Sets the time a dynamic entry remains in the ARP cache	GC
clear arp-cache	Deletes all dynamic entries from the ARP cache	PE
show arp	Displays entries in the ARP cache	NE, PE

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)#
```

clear arp-cache This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

Command Mode

Privileged Exec

Example

This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Do you want to continue this operation (y/n)?
Console#
```

show arp This command displays entries in the Address Resolution Protocol (ARP) cache.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- ◆ This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type "other" indicates local addresses for this router.
- ◆ Static entries are only displayed for VLANs that are up. In other words, static entries are only displayed when configured for the IP subnet of a existing VLAN, and that VLAN is linked up.

Example

This example displays all entries in the ARP cache.

```
Console#show arp
ARP Cache Timeout: 1200 (seconds)
```

IP Address	MAC Address	Type	Interface
10.1.0.0	FF-FF-FF-FF-FF-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 153: IPv6 Configuration Commands

Command	Function	Mode
<i>Interface Address Configuration and Utilities</i>		
<code>ipv6 default-gateway</code>	Sets an IPv6 default gateway for traffic with no known next hop	GC
<code>ipv6 address</code>	Configures an IPv6 global unicast address, and enables IPv6 on an interface	IC
<code>ipv6 address autoconfig</code>	Enables automatic configuration of IPv6 addresses on an interface and enables IPv6 on the interface	IC
<code>ipv6 address eui-64</code>	Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface	IC
<code>ipv6 address link-local</code>	Configures an IPv6 link-local address for an interface and enables IPv6 on the interface	IC
<code>ipv6 enable</code>	Enables IPv6 on an interface that has not been configured with an explicit IPv6 address	IC
<code>ipv6 mtu</code>	Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface	IC
<code>show ipv6 default-gateway</code>	Displays the current IPv6 default gateway	PE
<code>show ipv6 interface</code>	Displays the usability and configured settings for IPv6 interfaces	PE
<code>show ipv6 mtu</code>	Displays maximum transmission unit (MTU) information for IPv6 interfaces	PE
<code>show ipv6 traffic</code>	Displays statistics about IPv6 traffic	PE
<code>clear ipv6 traffic</code>	Resets IPv6 traffic counters	PE
<code>ping6</code>	Sends IPv6 ICMP echo request packets to another node on the network	PE

Table 153: IPv6 Configuration Commands (Continued)

Command	Function	Mode
<code>tracert6</code>	Shows the route packets take to the specified host	PE
<i>Neighbor Discovery</i>		
<code>ipv6 nd dad attempts</code>	Configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection	IC
<code>ipv6 nd ns-interval</code>	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface	IC
<code>ipv6 nd reachable-time</code>	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred	IC
<code>clear ipv6 neighbors</code>	Deletes all dynamic entries in the IPv6 neighbor discovery cache	PE
<code>show ipv6 neighbors</code>	Displays information in the IPv6 neighbor discovery cache	PE

Interface Address Configuration and Utilities

ipv6 default-gateway This command sets an IPv6 default gateway to use for destinations with no known next hop. Use the **no** form to remove a previously configured default gateway.

Syntax

ipv6 default-gateway *ipv6-address*

no ipv6 address

ipv6-address - The IPv6 address of the default next hop router to use for destinations with no known next hop.

Default Setting

No default gateway is defined

Command Mode

Global Configuration

Command Usage

- ◆ All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface.
- ◆ An IPv6 default gateway should be defined if the destination has been assigned an IPv6 address that is located in a different IP segment.

- ◆ An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

Example

The following example defines a default gateway for this device:

```
Console(config)#ipv6 default-gateway 2001:1:1:1::1
Console(config)#
```

Related Commands

[show ipv6 default-gateway \(1023\)](#)

[ip default-gateway \(1006\)](#)

ipv6 address This command configures an IPv6 global unicast address and enables IPv6 on an interface. Use the **no** form without any arguments to remove all IPv6 addresses from the interface, or use the **no** form with a specific IPv6 address to remove that address from the interface.

Syntax

[no] ipv6 address *ipv6-address*[/*prefix-length*]

ipv6-address - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ To connect to a larger network with multiple subnets, you must configure a global unicast address. This address can be manually configured with this command, or it can be automatically configured using the [ipv6 address autoconfig](#) command.
- ◆ If a link-local address has not yet been assigned to this interface, this command will assign the specified static global unicast address and also dynamically generate a link-local unicast address for the interface. (The link-local address is

made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)

- ◆ If a duplicate address is detected, a warning message is sent to the console.

Example

This example specifies a full IPv6 address and prefix length.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:1:1:1::1/64
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
    fe80::ce37:abff:fed7:a684%1/64
Global unicast address(es):
    2001:1:1:1::1/64, subnet is 2001:1:1:1::/64
Joined group address(es):
    ff02::1:ff00:1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands

[ipv6 address eui-64 \(1018\)](#)
[ipv6 address autoconfig \(1016\)](#)
[show ipv6 interface \(1023\)](#)
[ip address \(1004\)](#)

ipv6 address autoconfig This command enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 on the interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages; the host portion is based on the modified EUI-64 form of the interface identifier (i.e., the switch's MAC address). Use the **no** form to remove the address generated by this command.

Syntax

[no] ipv6 address autoconfig

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address (if a global prefix is included in received router advertisements) and a link local address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)
- ◆ If a duplicate address is detected, a warning message is sent to the console.
- ◆ When DHCPv6 is restarted, the switch may attempt to acquire an IP address prefix through stateful address autoconfiguration. If the router advertisements have the "other stateful configuration" flag set, the switch may also attempt to acquire other non-address configuration information (such as a default gateway) from a DHCPv6 server when DHCPv6 is restarted.

Example

This example assigns a dynamic global unicast address of to the switch.

```
Console(config-if)#ipv6 address autoconfig
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
    fe80::ce37:abff:fed7:a684%1/64
Global unicast address(es):
    2001:1:1:1::1/64, subnet is 2001:1:1:1::/64
Joined group address(es):
    ff02::1:ff00:1
    ff02::1:ffd7:a684
    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 \(1015\)](#)
[show ipv6 interface \(1023\)](#)

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 2001:0:1:1::1/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
    fe80::ce37:abff:fed7:a684%1/64
Global unicast address(es):
    2001:0:1:1:ce37:abff:fed7:a684/64, subnet is 2001:0:1:1::/64[EUI][EUI]
    2001:1:1:1::1/64, subnet is 2001:1:1:1::/64
Joined group address(es):
    ff02::1:ff00:1
    ff02::1:ffd7:a684
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#

```

Related Commands

[ipv6 address autoconfig \(1016\)](#)

[show ipv6 interface \(1023\)](#)

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::c0a8:6779 link-local
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
  fe80::c0a8:6779%1/64
Global unicast address(es):
  2001:0:1:1:ce37:abff:fed7:a684/64, subnet is 2001:0:1:1::/64[EUI][EUI]
  2001:1:1:1::1/64, subnet is 2001:1:1:1::/64
Joined group address(es):
  ff02::1:ffa8:6779
  ff02::1:ff00:1
  ff02::1:ffd7:a684
```



```
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
```

```
Console#
```

Related Commands

[ipv6 enable \(1021\)](#)

[show ipv6 interface \(1023\)](#)

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 1018](#)). 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::c0a8:6779%1/64
Global unicast address(es):
    2001:0:1:1:ce37:abff:fed7:a684/64, subnet is 2001:0:1:1::/64[EUI][EUI]
    2001:1:1:1::1/64, subnet is 2001:1:1:1::/64
Joined group address(es):
    ff02::1:ffa8:6779
    ff02::1:ff00:1
    ff02::1:ffd7:a684
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#
```

Related Commands

[ipv6 address link-local \(1020\)](#)

[show ipv6 interface \(1023\)](#)

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 \(1026\)](#)
[jumbo frame \(539\)](#)

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 2001:1:1:1::1

Console#
```

show ipv6 interface

This command displays the usability and configured settings for IPv6 interfaces.

Syntax

show ipv6 interface [**brief** [**vlan** *vlan-id* [*ipv6-prefix/prefix-length*]]]

brief - Displays a brief summary of IPv6 operational status and the addresses configured for each interface.

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

ipv6-prefix - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Command Mode

Privileged Exec

Example

This example displays all the IPv6 addresses configured for the switch.

```

Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
    fe80::c0a8:6779%1/64
Global unicast address(es):
    2001:0:1:1:ce37:abff:fed7:a684/64, subnet is 2001:0:1:1::/64[EUI][EUI]
    2001:1:1:1::1/64, subnet is 2001:1:1:1::/64
Joined group address(es):
    ff02::1:ffa8:6779
    ff02::1:ff00:1
    ff02::1:ffd7:a684
    ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#

```

Table 154: show ipv6 interface - display description

Field	Description
VLAN	A VLAN is marked "up" if the switch can send and receive packets on this interface, "down" if a line signal is not present, or "administratively down" if the interface has been disabled by the administrator.
IPv6	IPv6 is marked "enable" if the switch can send and receive IP traffic on this interface, "disable" if the switch cannot send and receive IP traffic on this interface, or "stalled" if a duplicate link-local address is detected on the interface.
Link-local address	Shows the link-local address assigned to this interface
Global unicast address(es)	Shows the global unicast address(es) assigned to this interface

Table 154: show ipv6 interface - display description (Continued)

Field	Description
Joined group address(es)	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. 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, FE80::C0A8:6779/64 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.
ND DAD	Indicates whether (neighbor discovery) duplicate address detection is enabled.
number of DAD attempts	The number of consecutive neighbor solicitation messages sent on the interface during duplicate address detection.
ND retransmit interval	The interval between IPv6 neighbor solicitation retransmissions sent on an interface during duplicate address detection.
ND advertised retransmit interval	The retransmit interval is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.
ND reachable time	The amount of time a remote IPv6 node is considered reachable after a reachability confirmation event has occurred
ND advertised reachable time	The reachable time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.
ND advertised router lifetime	The length of time during which the prefix is valid for on-link determination.

This example displays a brief summary of IPv6 addresses configured on the switch.

```

Console#show ipv6 interface brief
Interface      Status      IPv6      IPv6 Address
-----
VLAN 1         Up          Up        2001:0:1:1:ce37:abff:fed7:a684/64
VLAN 1         Up          Up        2001:1:1:1::1/64
VLAN 1         Up          Up        fe80::c0a8:6779/64
Console#

```

Related Commands

[show ip interface \(1007\)](#)

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
Console#
```

Table 155: show ipv6 mtu - display description*

Field	Description
MTU	Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path.
Since	Time since an ICMP packet-too-big message was received from this destination.
Destination Address	Address which sent an ICMP packet-too-big message.

* No information is displayed if an IPv6 address has not been assigned to the switch.

show ipv6 traffic This command displays statistics about IPv6 traffic passing through this switch.

Command Mode

Privileged Exec

Example

The following example shows statistics for all IPv6 unicast and multicast traffic, as well as ICMP, UDP and TCP statistics:

```
Console#show ipv6 traffic
IPv6 Statistics:
IPv6 received
    3 total received
    header errors
    too big errors
    no routes
    address errors
    unknown protocols
    truncated packets
    discards
    delivers
    reassembly request datagrams
    reassembly succeeded
    reassembly failed
IPv6 sent
    forwards datagrams
```

```

6 requests
  discards
  no routes
  generated fragments
  fragment succeeded
  fragment failed

ICMPv6 Statistics:
ICMPv6 received
  input
  errors
  destination unreachable messages
  packet too big messages
  time exceeded messages
  parameter problem message
  echo request messages
  echo reply messages
  router solicit messages
  router advertisement messages
  neighbor solicit messages
  neighbor advertisement messages
  redirect messages
  group membership query messages
  group membership response messages
  group membership reduction messages

ICMPv6 sent
  6 output
    destination unreachable messages
    packet too big messages
    time exceeded messages
    parameter problem message
    echo request messages
    echo reply messages
  3 router solicit messages
  router advertisement messages
  3 neighbor solicit messages
  neighbor advertisement messages
  redirect messages
  group membership query messages
  group membership response messages
  group membership reduction messages

UDP Statistics:
  input
  no port errors
  other errors
  output

Console#

```

Table 156: 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.

Table 156: show ipv6 traffic - display description (Continued)

Field	Description
no routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
address errors	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
unknown protocols	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
truncated packets	The number of input datagrams discarded because datagram frame didn't carry enough data.
discards	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
delivers	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
reassembly request datagrams	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
reassembly succeeded	The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
reassembly failed	The number of failures detected by the IPv6 re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
<i>IPv6 sent</i>	
forwards datagrams	The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.
requests	The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in 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.

Table 156: show ipv6 traffic - display description (Continued)

Field	Description
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 ipv6IfcmlnErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
errors	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
destination unreachable messages	The number of ICMP Destination Unreachable messages received by the interface.
packet too big messages	The number of ICMP Packet Too Big messages received by the interface.
time exceeded messages	The number of ICMP Time Exceeded messages received by the interface.
parameter problem message	The number of ICMP Parameter Problem messages received by the interface.
echo request messages	The number of ICMP Echo (request) messages received by the interface.
echo reply messages	The number of ICMP Echo Reply messages received by the interface.
router solicit messages	The number of ICMP Router Solicit messages received by the interface.
router advertisement messages	The number of ICMP Router Advertisement messages received by the interface.
neighbor solicit messages	The number of ICMP Neighbor Solicit messages received by the interface.
neighbor advertisement messages	The number of ICMP Neighbor Advertisement messages received by the interface.
redirect messages	The number of Redirect messages received by the interface.
group membership query messages	The number of ICMPv6 Group Membership Query messages received by the interface.
group membership response messages	The number of ICMPv6 Group Membership Response messages received by the interface.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages received by the interface.
multicast listener discovery version 2 reports	The number of MLDv2 reports received by the interface.

Table 156: show ipv6 traffic - display description (Continued)

Field	Description
<i>ICMPv6 sent</i>	
output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
destination unreachable messages	The number of ICMP Destination Unreachable messages sent by the interface.
packet too big messages	The number of ICMP Packet Too Big messages sent by the interface.
time exceeded messages	The number of ICMP Time Exceeded messages sent by the interface.
parameter problem message	The number of ICMP Parameter Problem messages sent by the interface.
echo request messages	The number of ICMP Echo (request) messages sent by the interface.
echo reply messages	The number of ICMP Echo Reply messages sent by the interface.
router solicit messages	The number of ICMP Router Solicitation messages sent by the interface.
router advertisement messages	The number of ICMP Router Advertisement messages sent by the interface.
neighbor solicit messages	The number of ICMP Neighbor Solicit messages sent by the interface.
neighbor advertisement messages	The number of ICMP Router Advertisement messages sent by the interface.
redirect messages	The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
group membership query messages	The number of ICMPv6 Group Membership Query messages sent by the interface.
group membership response messages	The number of ICMPv6 Group Membership Response messages sent.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages sent.
multicast listener discovery version 2 reports	The number of MLDv2 reports sent by the interface.
<i>UDP Statistics</i>	
input	The total number of UDP datagrams delivered to UDP users.
no port errors	The total number of received UDP datagrams for which there was no application at the destination port.
other errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
output	The total number of UDP datagrams sent from this entity.

clear ipv6 traffic This command resets IPv6 traffic counters.

Command Mode
Privileged Exec

Command Usage

This command resets all of the counters displayed by the [show ipv6 traffic](#) command.

Example

```
Console#clear ipv6 traffic
Console#
```

ping6 This command sends (IPv6) ICMP echo request packets to another node on the network.

Syntax

ping6 {*ipv6-address* | *host-name*} [**count** *count*] [**size** *size*]

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

host-name - A host name string which can be resolved into an IPv6 address through a domain name server.

count - Number of packets to send. (Range: 1-16)

size - Number of bytes in a packet. (Range: 0-1500 bytes)

The actual packet size will be eight bytes larger than the size specified because the router adds header information.

Default Setting

count: 5

size: 32 bytes

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **ping6** command to see if another site on the network can be reached, or to evaluate delays over the path.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::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 986](#)). If necessary, local devices can also be specified in the DNS static host table (see [page 988](#)).

- ◆ When using ping6 with a host name, the switch first attempts to resolve the alias into an IPv6 address before trying to resolve it into an IPv4 address.

Example

```

Console#ping6 fe80::c0a8:6779%1
Press "ESC" to abort.
Ping to fe80::c0a8:6779%1, by 5 0-byte payload ICMP packets, timeout is 3
seconds
response time: 0 ms      [fe80::c0a8:6779%1]      seq_no: 1
response time: 0 ms      [fe80::c0a8:6779%1]      seq_no: 2
response time: 0 ms      [fe80::c0a8:6779%1]      seq_no: 3
response time: 0 ms      [fe80::c0a8:6779%1]      seq_no: 4
response time: 0 ms      [fe80::c0a8:6779%1]      seq_no: 5
Ping statistics for fe80::c0a8:6779%1:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms
Console#

```

traceroute6 This command shows the route packets take to the specified destination.

Syntax

traceroute6 {*ipv6-address* | *host-name*} [**max-failures** *failure-count*]

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

host-name - A host name string which can be resolved into an IPv6 address through a domain name server.

failure-count - The maximum number of failures before which the trace route is terminated. (Range: 1-255)

Default Setting

Maximum failures: 5

Command Mode

Privileged Exec

Command Usage

- ◆ Use the **traceroute6** command to determine the path taken to reach a specified destination.
- ◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::C0A8:6779%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::c0a8:6779%1
Press "ESC" to abort.
Traceroute to fe80::c0a8:6779%1, 30 hops max, timeout is 3 seconds, 5 max
failu.

Hop  Packet 1  Packet 2  Packet 3  IPv6 Address
-----
1      <10 ms   <10 ms   <10 ms   fe80::c0a8:6779%1

Trace completed.
Console#

```

Neighbor Discovery

ipv6 nd dad attempts This command configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. Use the **no** form to restore the default setting.

Syntax

ipv6 nd dad attempts *count*

no ipv6 nd dad attempts

count - The number of neighbor solicitation messages sent to determine whether or not a duplicate address exists on this interface. (Range: 0-600)

Default Setting

3

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ Configuring a value of 0 disables duplicate address detection.

- ◆ Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
- ◆ Duplicate address detection is stopped on any interface that has been suspended (see the [vlan](#) command). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
- ◆ An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface’s link-local address, the other IPv6 addresses remain in a “tentative” state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- ◆ If a duplicate address is detected, it is set to “duplicate” state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in “duplicate” state.
- ◆ If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

Example

The following configures five neighbor solicitation attempts for addresses configured on VLAN 1. The [show ipv6 interface](#) command indicates that the duplicate address detection process is still on-going.

```

Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
    fe80::200:e8ff:fe90:0/64
Global unicast address(es):
    2009:db9:2229::79, subnet is 2009:db9:2229:0::/64
Joined group address(es):
    ff01::1/16
    ff02::1/16
    ff02::1:ff00:79/104
    ff02::1:ff90:0/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
Console#

```

Related Commands[ipv6 nd ns-interval \(1035\)](#)[show ipv6 neighbors \(1037\)](#)

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::c0a8:6779%1/64
Global unicast address(es):
  2001:0:1:1:ce37:abff:fed7:a684/64, subnet is 2001:0:1:1::/64[EUI][EUI]
  2001:1:1:1:1/64, subnet is 2001:1:1:1::/64
Joined group address(es):
  ff02::1:ffa8:6779
```

```
ff02::1:ff00:1
ff02::1:ffd7:a684
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 30000 milliseconds
ND advertised retransmit interval is 30000 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 \(533\)](#)

ipv6 nd reachable-time This command configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. Use the **no** form to restore the default setting.

Syntax

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

milliseconds - The time that a node can be considered reachable after receiving confirmation of reachability. (Range: 0-3600000)

Default Setting

30000 milliseconds is used for neighbor discovery operations

0 milliseconds is advertised in router advertisements

Command Mode

Interface Configuration (VLAN)

Command Usage

- ◆ The time limit configured by this parameter allows the router to detect unavailable neighbors. During the neighbor discover process, an IPv6 node will multicast neighbor solicitation messages to search for neighbor nodes. For a neighbor node to be considered reachable, it must respond to the neighbor soliciting node with a neighbor advertisement message to become a confirmed neighbor, after which the reachable timer will be considered in effect for subsequent unicast IPv6 layer communications.
- ◆ 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)#ipv6 nd reachable-time 1000
Console(config)#
```

clear ipv6 neighbors This command deletes all dynamic entries in the IPv6 neighbor discovery cache.

Command Mode

Privileged Exec

Example

The following deletes all dynamic entries in the IPv6 neighbor cache:

```
Console#clear ipv6 neighbors
Console#
```

show ipv6 neighbors This command displays information in the IPv6 neighbor discovery cache.

Syntax

show ipv6 neighbors [**vlan** *vlan-id* | *ipv6-address*]

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

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Default Setting

All IPv6 neighbor discovery cache entries are displayed.

Command Mode

Privileged Exec

Example

The following shows all known IPv6 neighbors for this switch:

```
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,
       P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address                               Age  Link-layer Addr  State Interface
-----
```

```
FE80::2E0:CFF:FE9C:CA10          4      00-E0-0C-9C-CA-10 R      1
Console#
```

Table 157: show ipv6 neighbors - display description

Field	Description
IPv6 Address	IPv6 address of neighbor
Age	The time since the address was verified as reachable (in seconds). A static entry is indicated by the value "Permanent."
Link-layer Addr	Physical layer MAC address.
State	The following states are used for dynamic entries: I1 (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message. I2 (Invalid) - An invalidated mapping. Setting the state to invalid dis-associates the interface identified with this entry from the indicated mapping (RFC 4293). R (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets. S (Stale) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent. 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. P1 (Probe) - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received. U (Unknown) - Unknown state. The following states are used for static entries: I1 (Incomplete)-The interface for this entry is down. R (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache. P2 (Permanent) - Indicates a static entry.
VLAN	VLAN interface from which the address was reached.

Related Commands

[show mac-address-table \(823\)](#)

Section IV

Appendices

This section provides additional information and includes these items:

- ◆ [“Software Specifications” on page 1040](#)
- ◆ [“Troubleshooting” on page 1044](#)
- ◆ [“License Information” on page 1046](#)



Software Specifications

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/LHX/ZX: 1000 Mbps 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)

VLAN Support Up to 4094 groups; port-based, protocol-based, tagged (802.1Q), voice VLANs, MAC-based

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 DiffServ²¹ supports class maps, policy maps, and service policies

Multicast Filtering IGMP Snooping (Layer 2 IPv4)
MLD Snooping (Layer 2 IPv6)

IP Routing ARP, CIDR (Classless Inter-Domain Routing)

Additional Features BOOTP Client
DHCP Client, Option 82,
LLDP (Link Layer Discover Protocol)
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 or TFTP in-band, or XModem out-of-band

SNMP Management access via MIB database
Trap management to specified hosts

RMON Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

²¹. Only supported for IPv4.

Standards

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
ARP (RFC 826)
DHCP Client (RFC 2131)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
IGMP Proxy (RFC 4541)
IPv4 IGMP (RFC 3228)
MLD Snooping (RFC 4541)
NTP (RFC 1305)
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)
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 MIB (RFC 2011)
IP Forwarding Table MIB (RFC 2096)
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)
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 158: Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, web browser, or SNMP software	◆ 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	◆ 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	◆ 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	◆ Contact your local distributor.

Using System Logs

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Set up your terminal emulation software so that it can capture all console output to a file. Then enter the “show tech-support” command to record all system settings in this file.
9. Contact your distributor’s service engineer, and send a detailed description of the problem, along with the file used to record your system settings.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
:
```



License Information

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

The GNU General Public License

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a). Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

- 5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
- 7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
- 8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Glossary

ACL Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

ARP Address Resolution Protocol converts between IP addresses and MAC (hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CoS Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DHCP Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP Option 82 A relay option for sending information about the requesting client (or an intermediate relay agent) in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information can be used by DHCP servers to assign fixed IP addresses, or set other services or policies for clients.

DHCP Snooping A technique used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

- DiffServ** Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.
- DNS** Domain Name Service. A system used for translating host names for network nodes into IP addresses.
- DSCP** Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.
- EAPOL** Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.
- EUI** Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.
- GARP** Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.
- GMRP** Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.
- GVRP** GARP VLAN Registration Protocol. Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

- ICMP** Internet Control Message Protocol is a network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.
- IEEE 802.1D** Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.
- IEEE 802.1Q** VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.
- IEEE 802.1p** An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.
- IEEE 802.1s** An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.
- IEEE 802.1w** An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)
- IEEE 802.1X** Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.
- IEEE 802.3ac** Defines frame extensions for VLAN tagging.
- IEEE 802.3x** Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)
- IGMP** Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.
- IGMP Proxy** Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in a simple tree that uses IGMP Proxy.

IGMP Query On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP Snooping Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

In-Band Management Management of the network from a station attached directly to the network.

IP Multicast Filtering A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

LACP Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Layer 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3 Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation *See Port Trunk.*

LLDP Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

MD5 MD5 Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MRD Multicast Router Discovery is a A protocol used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled devices to determine where to send multicast source and group membership messages.

MSTP Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

Multicast Switching A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

NTP Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Out-of-Band Management Management of the network from a station not attached to the network.

Port Authentication *See IEEE 802.1X.*

Port Mirroring A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

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.

CLI Command List

A

aaa accounting commands 639
aaa accounting dot1x 640
aaa accounting exec 641
aaa accounting update 642
aaa authorization commands 642
aaa authorization exec 643
aaa group server 644
absolute 588
access-list arp 752
access-list ip 734
access-list ipv6 740
access-list mac 747
accounting commands 646
accounting dot1x 645
accounting exec 646
arp timeout 1011
authentication enable 628
authentication login 629
authorization commands 647
authorization exec 648

B

boot system 541

C

calendar set 586
capabilities 759
channel-group 789
class 898
class-map 894
clear access-list hardware counters 755
clear arp-cache 1012
clear collision-mac-address-table 822
clear counters 765
clear dns cache 990
clear host 991
clear ip dhcp snooping binding 707
clear ip dhcp snooping database flash 707
clear ip igmp snooping groups dynamic 924
clear ip igmp snooping statistics 924
clear ip source-guard binding blocked 714
clear ipv6 mld snooping groups dynamic 949
clear ipv6 mld snooping statistics 950
clear ipv6 neighbors 1037
clear ipv6 traffic 1030
clear log 567
clear mac-address-table dynamic 822

clear network-access 693
clock summer-time (date) 581
clock summer-time (predefined) 583
clock summer-time (recurring) 584
clock timezone 585
configure 522
copy 542

D

databits 554
delete 545
delete public-key 662
description 895
description 760
dir 546
disable 523
disconnect 561
dos-protection smurf 725
dos-protection tcp-null-scan 726
dos-protection tcp-syn-fin-scan 726
dos-protection tcp-xmas-scan 727
dot1x default 667
dot1x identity profile 675
dot1x intrusion-action 668
dot1x max-reauth-req 669
dot1x max-req 670
dot1x max-start 676
dot1x operation-mode 670
dot1x pae supplicant 676
dot1x port-control 671
dot1x re-authenticate 674
dot1x re-authentication 672
dot1x system-auth-control 668
dot1x timeout auth-period 677
dot1x timeout held-period 677
dot1x timeout quiet-period 672
dot1x timeout re-authperiod 673
dot1x timeout start-period 678
dot1x timeout supp-timeout 673
dot1x timeout tx-period 674

E

enable 520
enable password 624
end 524
exec-timeout 554
exit 524

F

flowcontrol 761

G

garp timer 857

H

history 762

hostname 527

I

interface 758

interface vlan 862

ip access-group 738

ip address 1004

ip arp inspection 717

ip arp inspection filter 718

ip arp inspection limit 722

ip arp inspection log-buffer logs 719

ip arp inspection trust 722

ip arp inspection validate 720

ip arp inspection vlan 721

ip default-gateway 1006

ip dhcp client class-id 996

ip dhcp dynamic-provision 995

ip dhcp restart client 998

ip dhcp snooping 697

ip dhcp snooping max-number 705

ip dhcp snooping database flash 707

ip dhcp snooping information option 699

ip dhcp snooping information option circuit-id 704

ip dhcp snooping information option encode no-subtype 700

ip dhcp snooping information policy 702

ip dhcp snooping trust 706

ip dhcp snooping verify mac-address 702

ip dhcp snooping vlan 703

ip domain-list 985

ip domain-lookup 986

ip domain-name 987

ip host 988

ip http authentication 651

ip http port 651

ip http secure-port 652

ip http secure-server 653

ip http server 652

ip igmp filter (Global Configuration) 932

ip igmp filter (Interface Configuration) 934

ip igmp max-groups 935

ip igmp max-groups action 935

ip igmp profile 932

ip igmp query-drop 936

ip igmp snooping 908

ip igmp snooping priority 909

ip igmp snooping proxy-reporting 909

ip igmp snooping querier 910

ip igmp snooping router-alert-option-check 911

ip igmp snooping router-port-expire-time 911

ip igmp snooping tcn-flood 912

ip igmp snooping tcn-query-solicit 913

ip igmp snooping unregistered-data-flood 914

ip igmp snooping unsolicited-report-interval 914

ip igmp snooping version 915

ip igmp snooping version-exclusive 916

ip igmp snooping vlan general-query-suppression 916

ip igmp snooping vlan immediate-leave 917

ip igmp snooping vlan last-memb-query-count 918

ip igmp snooping vlan last-memb-query-intvl 919

ip igmp snooping vlan mrd 919

ip igmp snooping vlan mrouter 930

ip igmp snooping vlan proxy-address 920

ip igmp snooping vlan query-interval 922

ip igmp snooping vlan query-resp-intvl 922

ip igmp snooping vlan static 923

ip multicast-data-drop 936

ip name-server 989

ip source-guard 711

ip source-guard binding 709

ip source-guard max-binding 713

ip source-guard mode 714

ip ssh authentication-retries 660

ip ssh crypto host-key generate 663

ip ssh crypto zeroize 664

ip ssh save host-key 664

ip ssh server 660

ip ssh server-key size 661

ip ssh timeout 662

ip telnet max-sessions 655

ip telnet port 655

ip telnet server 656

ip tftp retry 550

ip tftp timeout 551

ipv6 access-group 745

ipv6 address 1015

ipv6 address autoconfig 1016

ipv6 address eui-64 1018

ipv6 address link-local 1020

ipv6 default-gateway 1014

ipv6 dhcp client rapid-commit vlan 999

ipv6 dhcp restart client vlan 999

ipv6 enable 1021

ipv6 host 990

ipv6 mld filter (Global Configuration) 954

ipv6 mld filter (Interface Configuration) 957

ipv6 mld max-groups 957

ipv6 mld max-groups action 958

ipv6 mld profile 955

ipv6 mld query-drop 959

ipv6 mld snooping 942

ipv6 mld snooping proxy-reporting 942

ipv6 mld snooping querier 943

ipv6 mld snooping query-interval 943

ipv6 mld snooping query-max-response-time 944

ipv6 mld snooping robustness 944

ipv6 mld snooping router-port-expire-time 945
 ipv6 mld snooping unknown-multicast mode 946
 ipv6 mld snooping unsolicited-report-interval 946
 ipv6 mld snooping version 947
 ipv6 mld snooping vlan immediate-leave 947
 ipv6 mld snooping vlan mrouter 948
 ipv6 mld snooping vlan static 949
 ipv6 mtu 1022
 ipv6 nd dad attempts 1033
 ipv6 nd ns-interval 1035
 ipv6 nd reachable-time 1036

J

jumbo frame 539

L

lacp 790
 lacp admin-key (Ethernet Interface) 791
 lacp admin-key (Port Channel) 794
 lacp port-priority 792
 lacp system-priority 793
 lacp timeout 795
 line 553
 lldp 964
 lldp admin-status 968
 lldp basic-tlv management-ip-address 968
 lldp basic-tlv port-description 969
 lldp basic-tlv system-capabilities 969
 lldp basic-tlv system-description 970
 lldp basic-tlv system-name 970
 lldp dot1-tlv proto-ident 971
 lldp dot1-tlv proto-vid 971
 lldp dot1-tlv pvid 972
 lldp dot1-tlv vlan-name 972
 lldp dot3-tlv link-aggr 973
 lldp dot3-tlv mac-phy 973
 lldp dot3-tlv max-frame 974
 lldp holdtime-multiplier 964
 lldp med-fast-start-count 965
 lldp med-location civic-addr 975
 lldp med-notification 976
 lldp med-tlv inventory 977
 lldp med-tlv location 978
 lldp med-tlv med-cap 978
 lldp med-tlv network-policy 979
 lldp notification 979
 lldp notification-interval 965
 lldp refresh-interval 966
 lldp reinit-delay 966
 lldp tx-delay 967
 logging command 563
 logging facility 564
 logging history 564
 logging host 565
 logging on 566
 logging sendmail 571
 logging sendmail destination-email 571

logging sendmail host 572
 logging sendmail level 572
 logging sendmail source-email 573
 logging trap 567
 login 555
 loopback detection trap 817
 loopback-detection 815
 loopback-detection action 815
 loopback-detection recover-time 816
 loopback-detection release 818
 loopback-detection transmit-interval 817

M

mac access-group 750
 mac-address-table aging-time 820
 mac-address-table static 821
 mac-learning 685
 management 681
 match 896
 max-hops 836
 media-type 762
 memory 612
 mst priority 836
 mst vlan 837

N

name 838
 negotiation 763
 network-access aging 690
 network-access dynamic-vlan 692
 network-access guest-vlan 693
 network-access mac-filter 691
 nlm 609
 no rspan session 808
 ntp authenticate 578
 ntp authentication-key 578
 ntp client 579
 ntp server 580

P

parity 556
 password 557
 password-thresh 557
 periodic 589
 permit, deny 933
 permit, deny 956
 permit, deny (ARP ACL) 753
 permit, deny (Extended IPv4 ACL) 736
 permit, deny (Extended IPv6 ACL) 742
 permit, deny (MAC ACL) 747
 permit, deny (Standard IP ACL) 735
 permit, deny (Standard IPv6 ACL) 741
 ping 1010
 ping6 1031
 police rate 899
 policy-map 897

port channel load-balance 787
 port monitor 800
 port security 686
 power-save 784
 privilege 627
 process cpu 613
 process cpu guard 614
 prompt 518
 protocol-vlan protocol-group (Configuring Groups)
 871
 protocol-vlan protocol-group (Configuring Interfaces)
 871

Q

qos map cos-dscp 886
 qos map dscp-mutation 888
 qos map trust-mode 889
 queue mode 882
 queue weight 883
 quit 521

R

radius-server acct-port 630
 radius-server auth-port 631
 radius-server host 631
 radius-server key 632
 radius-server retransmit 633
 radius-server timeout 633
 range 933
 range 956
 rate-limit 811
 reload (Global Configuration) 519
 reload (Privileged Exec) 523
 rename 897
 revision 838
 rmon alarm 617
 rmon collection history 619
 rmon collection rmon1 620
 rmon event 618
 rspan destination 806
 rspan remote vlan 807
 rspan source 805

S

server 645
 service-policy 903
 set cos 900
 set ip dscp 901
 set phb 902
 show access-group 755
 show access-list 756
 show access-list arp 754
 show access-list tcam-utilization 528
 show accounting 648
 show arp 1012
 show authorization 649

show bridge-ext 858
 show cable-diagnostics 783
 show calendar 587
 show class-map 903
 show collision-mac-address-table 822
 show dns 991
 show dns cache 992
 show dos-protection 727
 show dot1x 678
 show garp timer 859
 show history 521
 show hosts 992
 show interfaces brief 766
 show interfaces counters 767
 show interfaces history 770
 show interfaces protocol-vlan protocol-group 873
 show interfaces status 772
 show interfaces switchport 773
 show interfaces transceiver 780
 show interfaces transceiver-threshold 781
 show ip access-group 739
 show ip access-list 739
 show ip arp inspection configuration 723
 show ip arp inspection interface 723
 show ip arp inspection log 724
 show ip arp inspection statistics 724
 show ip arp inspection vlan 724
 show ip default-gateway 1007
 show ip dhcp dynamic-provision 998
 show ip dhcp snooping 708
 show ip dhcp snooping binding 708
 show ip igmp filter 937
 show ip igmp profile 938
 show ip igmp query-drop 938
 show ip igmp snooping 925
 show ip igmp snooping group 926
 show ip igmp snooping mrouter 927
 show ip igmp snooping statistics 927
 show ip igmp throttle interface 939
 show ip interface 1007
 show ip multicast-data-drop 940
 show ip source-guard 715
 show ip source-guard binding 715
 show ip ssh 665
 show ip telnet 657
 show ip tftp 551
 show ip traffic 1008
 show ipv6 access-group 745
 show ipv6 access-list 746
 show ipv6 default-gateway 1023
 show ipv6 dhcp duid 1001
 show ipv6 dhcp vlan 1001
 show ipv6 interface 1023
 show ipv6 mld filter 959
 show ipv6 mld profile 960
 show ipv6 mld query-drop 960
 show ipv6 mld snooping group 951
 show ipv6 mld snooping group source-list 952
 show ipv6 mld snooping mrouter 952

show ipv6 mld snooping statistics 953
show ipv6 mld throttle interface 961
show ipv6 mld snooping 950
show ipv6 mtu 1026
show ipv6 neighbors 1037
show ipv6 traffic 1026
show lacp 796
show line 562
show lldp config 980
show lldp info local-device 981
show lldp info remote-device 982
show lldp info statistics 984
show log 568
show logging 569
show logging sendmail 574
show loopback-detection 818
show mac access-group 751
show mac access-list 751
show mac-address-table 823
show mac-address-table aging-time 824
show mac-address-table count 824
show management 682
show memory 529
show network-access 694
show network-access mac-address-table 695
show network-access mac-filter 696
show nlm oper-status 612
show ntp 581
show policy-map 904
show policy-map interface 905
show port monitor 802
show port security 688
show port-channel load-balance 799
show power-save 785
show privilege 627
show process cpu 530
show process cpu guard 530
show process cpu task 531
show protocol-vlan protocol-group 872
show public-key 665
show qos map cos-dscp 890
show qos map dscp-mutation 891
show qos map trust-mode 891
show queue mode 885
show queue weight 885
show radius-server 634
show reload 524
show rmon alarms 621
show rmon events 621
show rmon history 622
show rmon statistics 622
show rspan 809
show running-config 533
show snmp 595
show snmp engine-id 606
show snmp group 607
show snmp notify-filter 612
show snmp user 608
show snmp view 609
show snmp-server enable port-traps 600
show snmp 577
show spanning-tree 852
show spanning-tree mst configuration 854
show spanning-tree tc-prop 854
show ssh 666
show startup-config 534
show system 535
show tacacs-server 637
show tech-support 536
show time-range 590
show traffic-segmentation 732
show upgrade 550
show users 537
show version 537
show vlan 869
show voice vlan 880
show watchdog 538
shutdown 764
silent-time 558
snmp-server 593
snmp-server community 593
snmp-server contact 594
snmp-server enable port-traps link-up-down 599
snmp-server enable port-traps mac-notification 600
snmp-server enable traps 596
snmp-server engine-id 601
snmp-server group 602
snmp-server host 597
snmp-server location 595
snmp-server notify-filter 610
snmp-server user 603
snmp-server view 605
snmp client 575
snmp poll 576
snmp server 576
spanning-tree 827
spanning-tree bpdu-filter 839
spanning-tree bpdu-guard 840
spanning-tree cisco-prestandard 828
spanning-tree cost 841
spanning-tree edge-port 842
spanning-tree forward-time 828
spanning-tree hello-time 829
spanning-tree link-type 843
spanning-tree loopback-detection 843
spanning-tree loopback-detection action 844
spanning-tree loopback-detection release 851
spanning-tree loopback-detection release-mode 845
spanning-tree loopback-detection trap 846
spanning-tree max-age 830
spanning-tree mode 830
spanning-tree mst configuration 832
spanning-tree mst cost 846
spanning-tree mst port-priority 847
spanning-tree pathcost method 832
spanning-tree port-bpdu-flooding 848
spanning-tree port-priority 848
spanning-tree priority 833

spanning-tree protocol-migration 852
spanning-tree root-guard 849
spanning-tree spanning-disabled 850
spanning-tree system-bpdu-flooding 834
spanning-tree tc-prop 834
spanning-tree tc-prop-stop 850
spanning-tree transmission-limit 835
speed 559
speed-duplex 764
stopbits 559
switchport acceptable-frame-types 863
switchport allowed vlan 864
switchport forbidden vlan 858
switchport ingress-filtering 865
switchport mode 866
switchport native vlan 867
switchport packet-rate 812
switchport priority default 884
switchport voice vlan 877
switchport voice vlan priority 878
switchport voice vlan rule 878
switchport voice vlan security 879

T

tacacs-server host 635
tacacs-server key 635
tacacs-server port 636
tacacs-server retransmit 636
tacacs-server timeout 637
telnet (client) 656
terminal 561
test cable-diagnostics 782
timeout login response 560
time-range 587
traceroute 1009
traceroute6 1032
traffic-segmentation 728
traffic-segmentation session 729
traffic-segmentation uplink/downlink 730
traffic-segmentation uplink-to-uplink 731
transceiver-monitor 774
transceiver-threshold current 775
transceiver-threshold rx-power 776
transceiver-threshold temperature 777
transceiver-threshold tx-power 778
transceiver-threshold voltage 779
transceiver-threshold-auto 775

U

upgrade opcode auto 547
upgrade opcode path 549
upgrade opcode reload 550
username 625

V

vlan 861

vlan database 860
vlan-trunking 867
voice vlan 874
voice vlan aging 875
voice vlan mac-address 876

W

watchdog software 538
whichboot 547

Index

Numerics

802.1X

- authenticator, configuring 332, 668–674
- global settings 331, 667–668
- port authentication 329, 666, 668
- port authentication accounting 269, 270, 645
- supplicant, configuring 675–678

A

AAA

- accounting 802.1X port settings 269, 270, 645
- accounting exec command privileges 269, 276, 641, 646, 647
- accounting exec settings 270, 276, 646
- accounting summary 271, 648
- accounting update 269, 642
- accounting, configuring 269, 638
- authentication, authorization, and accounting 262
- authorization & accounting 638
- authorization exec settings 276, 643
- authorization method 276, 643
- authorization settings 275, 643
- authorization summary 648
- RADIUS group settings 270, 644
- TACACS+ group settings 270, 644

acceptable frame type 187, 863

Access Control List *See* ACL

ACL 299, 733

- ARP 302, 313, 752
- binding to a port 315
- IPv4 Extended 302, 305, 733, 736
- IPv4 Standard 302, 304, 733, 735
- IPv6 Extended 302, 309, 740, 742
- IPv6 Standard 302, 307, 740, 741
- MAC 302, 311, 746
- time range 421, 587

Address Resolution Protocol *See* ARP

address table 197, 820

- aging time 201, 820
- aging time, displaying 201, 824
- aging time, setting 201, 820

administrative users, displaying 537

ARP ACL 313, 718

ARP configuration 1011

ARP description 467

ARP inspection 317, 716

ACL filter 320, 718

additional validation criteria 319, 720

ARP ACL 321, 752

enabling globally 319, 717

enabling per VLAN 721

trusted ports 322, 722

ARP statistics 1008

ATC 581

authentication

MAC address authentication 281, 690

MAC, configuring ports 284, 690

network access 281, 690

public key 294, 659

B

BOOTP 484, 1004

BPDU 207

filter 220, 839

flooding when STA disabled on VLAN 211, 848

flooding when STA globally disabled 211, 834

ignoring superior BPDUs 219, 849

selecting protocol based on message format 220, 852

shut down port on receipt 220, 840

bridge extension capabilities, displaying 107, 858

broadcast storm, threshold 231, 232, 812

C

cable diagnostics 782

canonical format indicator 242

class map

description 895

DiffServ 245, 894

Class of Service *See* CoS

CLI

command modes 512

showing commands 510

command line interface *See* CLI

committed information rate, QoS policy 250, 899

community string 69, 396, 593

configuration file, DHCP download reference 78

configuration files, restoring defaults 108, 540

configuration settings

restoring 73, 110, 111, 540, 542

saving 73, 110, 540, 542

configuration settings, automatic installation 78
 console port, required connections 61
 CoS 233, 889
 configuring 233, 881
 default mapping to internal values 241, 887
 enabling 238, 889
 layer 3/4 priorities 237, 886
 priorities, mapping to internal values 241, 886
 queue mode 234, 882
 queue weights, assigning 235, 883
 CoS/CFI to PHB/drop precedence 241, 886
 CPU
 status 130, 530
 tasks, showing 531
 utilization, setting trap 613
 utilization, showing 130, 530

D

dashboard 85
 Daylight Savings Time *See* summer time
 default IPv4 gateway, configuration 483, 1006
 default IPv6 gateway, configuration 488, 1014
 default priority, ingress port 233, 884
 default settings, system 57
 DHCP 475, 484, 1004
 class identifier 477, 996
 client 484, 994, 1004
 client identifier 476, 477, 996
 dynamic configuration 67
 dynamic provision 481
 option 82 information 339, 480
 relay service 477
 relay service, enabling 480
 DHCP snooping
 information option, circuit ID 343, 704
 information option, remote ID 340
 subtype field 700
 DHCPv4 snooping 337, 696
 enabling 340, 697
 global configuration 340, 697
 information option 340, 699
 information option policy 340, 702
 information option, enabling 340, 699
 information option, remote ID 699
 policy selection 340, 702
 specifying trusted interfaces 342, 706
 sub-length field 700
 sub-option format 700
 sub-type and sub-length, disabling 700
 subtype field 700
 verifying MAC addresses 340, 702
 VLAN configuration 342, 703
 DHCPv6 restart 491
 Differentiated Code Point Service *See* DSCP

Differentiated Services *See* DiffServ
 DiffServ 244, 893
 binding policy to interface 253, 903
 class map 245, 894, 898
 class map, description 895
 classifying QoS traffic 245, 896
 committed information rate 899
 configuring 244, 893
 description 895
 metering, configuring 249
 policy map 249, 897
 policy map, description 246, 895
 QoS policy 249, 897
 service policy 253, 903
 setting CoS for matching packets 250, 900
 setting IP DSCP for matching packets 901
 setting PHB for matching packets 250, 902

DNS

default domain name 469, 987
 displaying the cache 474, 992
 domain name list 469, 988, 990
 enabling lookup 469, 986
 name server list 469, 989
 static entries, IPv4 473, 988
 static entries, IPv6 990

Domain Name Service *See* DNS

DoS protection 725

downloading software 108, 542
 automatically 113, 547
 using FTP or TFTP 113
 using TFTP 542

drop precedence

 CoS priority mapping 242, 886
 DSCP ingress map 240, 888

DSA encryption 296, 297, 663

DSCP 237, 889

 enabling 238, 889
 ingress map, drop precedence 240, 888
 mapping to internal values 239, 888

DSCP to PHB/drop precedence 240, 888

dynamic addresses

 clearing 203, 822
 displaying 201, 823

Dynamic Host Configuration Protocol *See* DHCP

dynamic QoS assignment 282

dynamic VLAN assignment 281, 284, 692

E

edge port, STA 219, 222, 842

encryption

 DSA 296, 297, 663
 RSA 296, 297, 663

engine ID 384, 385, 601

event logging 354, 563

exec command privileges, accounting 269, 276, 641, 646, 647

exec settings

accounting 270, 646
authorization 276, 643

F

firmware

displaying version 105, 537
upgrading 108, 542
upgrading automatically 113, 547
upgrading with FTP or TFTP 113, 547
version, displaying 105, 537

G

gateway, IPv4 default 483, 1006
gateway, IPv6 default 488, 1014
general security measures 261, 684

H

hardware version, displaying 105, 537
HTTP, web server 652
HTTPS 289, 290, 653
configuring 289, 652, 653
replacing SSL certificate 290, 542
secure-site certificate 290, 542
HTTPS, secure server 289, 653

I

IEEE 802.1D 206, 830
IEEE 802.1s 206, 830
IEEE 802.1w 206, 830
IEEE 802.1X 329, 666, 668
IGMP
filter profiles, binding to interface 934
filter profiles, configuration 451, 453, 932
filter, interface configuration 934–935
filter, parameters 451, 453, 932–935
filtering & throttling 450, 931
filtering & throttling, creating profile 451
filtering & throttling, enabling 450, 932
filtering & throttling, interface configuration 453, 934–936
filtering & throttling, status 450, 932
filtering, configuring profile 933
filtering, creating profile 932
filtering, group range 933
filtering, interface settings 934–935
groups, displaying 437, 926
Layer 2 428, 906
query 430, 910

query, enabling 910
snooping 428, 906
snooping & query, parameters 430, 906
snooping, configuring 430, 906
snooping, enabling 908
snooping, immediate leave 440, 917

IGMP services, displaying 445

IGMP snooping

configuring 438, 906
enabling per interface 438, 439, 908
forwarding entries 445, 926
immediate leave, status 440, 917
interface attached to multicast router 436, 927, 930
last leave 429
last member query count 918
last member query interval 442, 919
proxy address 442
proxy query address 920
proxy query interval 922
proxy query response interval 922
proxy reporting 441, 909, 942
querier timeout 433, 911
querier, enabling 910
query interval 441
query response interval 442
query suppression 429
router port expire time 433, 911
static host interface 429, 923
static multicast routing 434, 930
static port assignment 436, 923
static router interface 429, 930
static router port, configuring 434, 930
statistics, displaying 446, 927, 953
TCN flood 431, 912
unregistered data flooding 432, 914
version exclusive 432, 916
version for interface, setting 441, 915
version, setting 433, 915
with proxy reporting 429, 909, 942

immediate leave, IGMP snooping 440, 917

immediate leave, MLD snooping 457, 947

importing user public keys 297, 542, 545

ingress filtering 187, 865

IP address

BOOTP/DHCP 484
setting 483

IP address, setting 1003

IP filter, for management access 325, 681

IP source guard

ACL table, learning mode 348
configuring static entries 349, 709
learning mode, ACL table or MAC table 348
MAC table, learning mode 348
setting filter criteria 347, 711

- setting maximum bindings 348, 713, 714
- IP statistics 498, 1008
- IPv4 address
 - BOOTP/DHCP 484, 998, 1004
 - dynamic configuration 67
 - manual configuration 64
 - setting 64, 483, 1004
- IPv6
 - displaying neighbors 497, 1037
 - duplicate address detection 497, 1033
 - enabling 490, 1021
 - MTU 490, 1022
 - neighbor reachable time 1036
 - neighbor solicitation interval 1035
- IPv6 address
 - dynamic configuration (global unicast) 494, 1016
 - dynamic configuration (link-local) 68, 490, 1021
 - EUI format 494, 1018
 - EUI-64 setting 494, 1018
 - explicit configuration 490, 1021
 - global unicast 494, 1015
 - link-local 495, 1017
 - manual configuration (global unicast) 65, 494, 1015
 - manual configuration (link-local) 65, 495, 1020
 - setting 64, 487, 1015

J

- jumbo frame 106, 539

K

- key
 - private 292, 657
 - public 292, 657
 - user public, importing 297, 542, 545
- key pair
 - host 292, 657
 - host, generating 296, 663

L

- LACP
 - configuration 157, 786
 - group attributes, configuring 161, 794
 - group members, configuring 159, 790
 - load balancing 167
 - local parameters 164, 796
 - partner parameters 166, 796
 - protocol message statistics 163, 796
 - protocol parameters 159, 786
 - timeout, for LACPDU 158, 795
- last member query count, IGMP snooping 918
- last member query interval, IGMP snooping 442, 919
- license information 1046

- Link Layer Discovery Protocol - Media Endpoint Discovery
- See LLDP-MED

- Link Layer Discovery Protocol See LLDP

- link type, STA 218, 222, 843

- LLDP 359, 962
 - device statistics details, displaying 381, 984
 - device statistics, displaying 379, 984
 - display device information 371, 982
 - displaying remote information 371, 982
 - interface attributes, configuring 361, 968–979
 - local device information, displaying 981
 - message attributes 361, 962
 - message statistics 379, 984
 - remote information, displaying 378, 379, 982
 - remote port information, displaying 371, 982
 - timing attributes, configuring 359, 964–967
 - TLV 359, 362
 - TLV, 802.1 971–972
 - TLV, 802.3 973–??
 - TLV, basic 968–970
 - TLV, management address 362, 968
 - TLV, port description 362, 969
 - TLV, system capabilities 362, 969
 - TLV, system description 362, 970
 - TLV, system name 362, 970

- LLDP-MED 359, 962
 - notification, status 361, 976
 - TLV 363, 962
 - TLV, extended PoE 363
 - TLV, inventory 363, 977
 - TLV, location 363, 975, 978
 - TLV, MED capabilities 363, 978
 - TLV, network policy 364, 979
 - TLV, PoE 363

- local engine ID 384, 601

- logging
 - messages, displaying 355, 568
 - syslog traps 356, 567
 - to syslog servers 357, 565

- log-in, web interface 85

- logon authentication 279, 623
 - encryption keys 266, 632, 635
 - RADIUS client 265, 630
 - RADIUS server 265, 630
 - sequence 263, 628, 629
 - settings 264, 266, 629
 - TACACS+ client 264, 634
 - TACACS+ server 264, 634

- loopback detection
 - non-STA 814
 - STA 208, 843

M

- MAC address authentication 281, 690
 - ports, configuring 284, 690
- MAC address, mirroring 800
- main menu, web interface 89
- management access, filtering per address 325, 681
- management access, IP filter 325, 681
- Management Information Bases (MIBs) 1042
- matching class settings, classifying QoS traffic 246, 896
- media-type 762
- memory
 - status 132, 529
 - utilization, showing 132, 529
- memory utilization, setting trap 612
- mirror port
 - configuring 171, 800
 - configuring local traffic 171, 800
 - configuring remote traffic 172, 803
- MLD
 - filter profiles, configuration 955
 - filtering & throttling 954
 - filtering & throttling, configuring profile 956
 - filtering & throttling, creating profile 955
 - filtering & throttling, enabling 954
 - filtering & throttling, interface configuration 957–958
 - filtering & throttling, status 954
- MLD snooping 455, 940
 - configuring 455, 941
 - enabling 455, 942
 - groups, displaying 461, 462
 - immediate leave 457, 947
 - immediate leave, status 457, 947
 - interface attached to multicast router 458, 459
 - multicast static router port 458, 948
 - querier 455, 943
 - querier, enabling 455, 943
 - query interval 456, 943
 - query, maximum response time 456, 944
 - robustness value 456, 944
 - static port assignment 460, 949
 - static router port 458, 948
 - unknown multicast, handling 456, 946
 - version 456, 947
- MSTP 224, 830
 - global settings, configuring 210, 224, 826
 - global settings, displaying 215, 853
 - interface settings, configuring 216, 228, 827, 839–850
 - interface settings, displaying 229, 852
 - path cost 228, 846
- MTU for IPv6 490, 1022
- multicast filtering 427, 906
 - enabling IGMP snooping 439, 908
 - enabling IGMP snooping per interface 438, 908

- enabling MLD snooping 455, 942
 - router configuration 434, 930
- multicast groups 437, 445, 461, 926
 - displaying 437, 445, 461
 - static 436, 437, 460, 461, 923, 926
- Multicast Listener Discovery *See* MLD snooping
- multicast router discovery 438, 919
- multicast router port, displaying 435, 459, 927
- multicast services
 - configuring 436, 460, 923
 - displaying 437, 461, 926
- multicast static router port 434, 930
 - configuring 434, 930
 - configuring for MLD snooping 458, 948
- multicast storm, threshold 232, 812
- multicast, filtering and throttling 450, 932, 954

N

- network access
 - authentication 281, 690
 - dynamic VLAN assignment 284, 692
 - MAC address filter 285, 691
 - port configuration 284
 - secure MAC information 287, 695, 696
- NTP
 - authentication keys, specifying 122, 578
 - client, enabling 119, 579
 - setting the system clock 120
 - specifying servers 120, 580
- NTP, setting the system clock 578–581

P

- password, line 557
- passwords 62, 279, 624
 - administrator setting 279, 625
- path cost 222, 841
 - method 212, 832
 - STA 222, 832, 841
- per-hop behavior, DSCP ingress map 239, 888
- PoE time range 421
- policing traffic, QoS policy 249, 250
- policy map
 - description 895
 - DiffServ 249, 897
- port authentication 329, 666, 668
- port priority
 - configuring 233, 881
 - default ingress 233, 884
 - STA 217, 848
- port security, configuring 327, 685
- port, statistics 142, 767
- ports
 - autonegotiation 138, 763

- broadcast storm threshold 231, 232, 812
- capabilities 138, 759
- configuring 137, 757
- duplex mode 139, 764
- flow control 139, 761
- forced selection of media type 762
- forced selection on combo ports 762
- mirroring 171, 800
- mirroring local traffic 171, 800
- mirroring remote traffic 172, 803
- multicast storm threshold 232, 812
- speed 139, 764
- statistics 142, 767
- transceiver threshold, auto-set 152
- transceiver threshold, trap 152
- unknown unicast storm threshold 232, 812
- power savings
 - configuring 169, 784
 - enabling per port 169, 784
- priority, default port ingress 233, 884
- private key 292, 657
- privilege level, defining per command 627
- problems, troubleshooting 1044
- protocol migration 220, 852
- protocol VLANs 190, 870
 - configuring 191, 871
 - interface configuration 192, 871
 - system configuration 191, 871
- proxy address, IGMP snooping 442
- proxy query address, IGMP snooping 920
- proxy query interval, IGMP snooping 922
- proxy query response interval, IGMP snooping 922
- proxy reporting, IGMP snooping 441, 909, 942
- public key 292, 657
- PVID, port native VLAN 187, 867

Q

- QoS 244, 893
 - configuration guidelines 894
 - configuring 244, 893
 - CoS/CFI to PHB/drop precedence 241, 886
 - DSCP to PHB/drop precedence 239, 888
 - matching class settings 246, 896
 - selecting DSCP, CoS 238, 889
- QoS policy
 - policing flow 249, 250
- QoS policy, committed information rate 250, 899
- Quality of Service *See* QoS
- query interval, IGMP snooping 441
- query response interval, IGMP snooping 442
- queue weight, assigning to CoS 235, 883

R

- RADIUS
 - logon authentication 265, 630
 - settings 265, 630
- rate limit
 - port 230, 811
 - setting 230, 810
- remote engine ID 384, 601
- remote logging 356, 567
- Remote Monitoring *See* RMON
- rename, DiffServ 897
- restarting the system 133, 519, 523
 - at scheduled times 133, 519
 - showing restart time 136, 524
- RMON 410, 616
 - alarm, displaying settings 413, 621
 - alarm, setting thresholds 411, 617
 - commands 616
 - event settings, displaying 415, 621
 - response to alarm setting 413, 618
 - statistics history, collection 415, 619
 - statistics history, displaying 417, 622
 - statistics, collection 418, 620
 - statistics, displaying 419, 622
- RSA encryption 296, 297, 663
- RSTP 206, 830
 - global settings, configuring 210, 830
 - global settings, displaying 215, 852
 - interface settings, configuring 216, 839–850
 - interface settings, displaying 221, 852
- running configuration files, displaying 533

S

- secure shell 292, 657
 - configuration 292, 658
- security, general measures 261, 684
- serial port, configuring 126, 552
- Simple Mail Transfer Protocol *See* SMTP
- Simple Network Management Protocol *See* SNMP
- SMTP
 - event handling 357, 570
 - sending log events 357, 570
- SNMP 381, 591
 - community string 396, 593
 - enabling traps 402, 596
 - enabling traps, mac-address changes 204, 600
 - filtering IP addresses 325, 681
 - global settings, configuring 383, 593–605
 - mac address traps 596, 600
 - trap manager 402, 597
 - users, configuring 397, 399
- SNMPv3 384–404, 601–603
 - engine ID 384, 385, 601

- engine identifier, local 384, 601
 - engine identifier, remote 384, 385, 601
 - groups 389, 602
 - local users, configuring 397, 603
 - remote users, configuring 399, 603
 - user configuration 397, 399, 603
 - views 387, 605
 - SNTP
 - setting the system clock 118, 575–577
 - specifying servers 120, 576
 - software
 - displaying version 105, 537
 - downloading 108, 542
 - version, displaying 105, 537
 - Spanning Tree Protocol *See* STA
 - specifications, software 1040
 - SSH 292, 657
 - authentication retries 295, 660
 - configuring 292, 658
 - downloading public keys for clients 297, 542, 545
 - generating host key pair 296, 663
 - server, configuring 294, 660
 - timeout 295, 662
 - SSL, replacing certificate 290
 - STA 206, 826
 - BPDU auto recovery 220
 - BPDU filter 220, 839
 - BPDU flooding 211, 217, 848
 - BPDU shutdown 220, 840
 - cisco-prestandard, setting compatibility 828
 - detecting loopbacks 208, 843
 - edge port 219, 222, 842
 - global settings, configuring 210, 827–835
 - global settings, displaying 215, 852
 - interface settings, configuring 216, 839–850
 - interface settings, displaying 221, 853
 - link type 218, 222, 843
 - loopback detection 208, 843
 - MSTP interface settings, configuring 228, 836–838
 - MSTP path cost 228, 846
 - path cost 222, 832, 841
 - path cost method 212, 832
 - port priority 217, 848
 - port/trunk loopback detection 208, 843
 - protocol migration 220, 852
 - transmission limit 212, 835
 - standards, IEEE 1042
 - startup files
 - creating 108, 542
 - displaying 108, 534, 547
 - setting 108, 541
 - static addresses, setting 199, 821
 - statistics
 - ARP 1008
 - history for port 146
 - history for trunk 146
 - ICMP 1008
 - IP 1008
 - TCP 1008
 - UDP 1008
 - statistics, port 142, 767
 - STP 210, 830
 - Also see* STA
 - summary, accounting 271, 648
 - summer time, setting 124, 581–584
 - switch settings
 - restoring 110, 540
 - saving 110, 540
 - system clock
 - setting 117, 574
 - setting manually 117, 586
 - setting the time zone 123, 585
 - setting with NTP 120, 578–581
 - setting with SNTP 118, 575–577
 - summer time 124, 581–584
 - system clock, setting 80
 - system logs 566
 - system software, downloading from server 108, 542
- ## T
- TACACS+
 - logon authentication 264, 634
 - settings 266, 634
 - TCN
 - flood 431, 912
 - general query solicitation 431, 913
 - Telnet
 - configuring 128, 654
 - server, enabling 128, 656
 - terminal, configuration settings 561
 - TFTP
 - retry count 550
 - timeout 551
 - time range, ACL 421, 587
 - time range, PoE 421
 - time zone, setting 123, 585
 - time, setting 117, 574
 - traffic segmentation 177, 727
 - assigning ports 177, 730
 - enabling 177, 728
 - sessions, assigning ports 179, 730
 - sessions, creating 178, 729
 - transceiver data, displaying 150
 - transceiver thresholds
 - configuring 151
 - displaying 151, 781
 - trap manager 70, 402, 597
 - troubleshooting 1044, 1046

- trunk
 - configuration 153, 786
 - LACP 157, 786, 790
 - load balancing 787
 - static 155, 789
- tunneling unknown VLANs, VLAN trunking 867
- Type Length Value
 - See LLDP TLV

U

- unknown unicast storm, threshold 232, 812
- unregistered data flooding, IGMP snooping 432, 914
- upgrading software 108, 542, 547
- user account 279, 624, 625
- user password 279, 624, 625

V

- VLAN trunking 867
- VLANs 181–194, 856–880
 - acceptable frame type 187, 863
 - adding static members 186, 864
 - basic information, displaying 858
 - creating 184, 861
 - description 181
 - displaying port members 869
 - displaying port members by interface 189
 - displaying port members by interface range 190
 - displaying port members by VLAN index 188
 - dynamic assignment 284, 692
 - egress mode 186, 866
 - ingress filtering 187, 865
 - interface configuration 186, 863–867
 - MAC-based 194
 - mirroring 800
 - port members, displaying 869
 - protocol 190, 870
 - protocol, configuring 191, 871
 - protocol, configuring groups 191, 871
 - protocol, interface configuration 192, 871
 - protocol, system configuration 191, 871
 - PVID 187, 867
 - tunneling unknown groups 867
 - voice 255, 874
- voice VLANs 255, 874
 - detecting VoIP devices 256, 874
 - enabling for ports 259, 877–878
 - identifying client devices 257, 876
- VoIP traffic 255, 874
 - ports, configuring 258, 877–878
 - telephony OUI, configuring 257, 876
 - voice VLAN, configuring 256, 874
- VoIP, detecting devices 259, 878

W

- web interface
 - access requirements 84
 - configuration buttons 87
 - home page 87
 - menu list 89
 - panel display 88

