



ECS5510-48S  
48-Port 10G Ethernet  
Top-of-Rack Switch

Management Guide



## **ECS5510-48S 10G ETHERNET TOP-OF-RACK SWITCH**

*Layer 2 Managed Switch,  
with 48 10GBASE SFP+ Slots,  
One Power Supply Unit,  
and one Fan Tray Module*



# ABOUT THIS GUIDE

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

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

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



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

---



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

---



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

---

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

*The Installation Guide*

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

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

**MAY 2011 REVISION**

This is the first version of this guide. This guide is valid for software release v2.0.0.23.

# CONTENTS

<b>ABOUT THIS GUIDE</b>	<b>5</b>
<b>CONTENTS</b>	<b>6</b>
<b>FIGURES</b>	<b>33</b>
<b>TABLES</b>	<b>41</b>

---

<b>SECTION I</b>	<b>GETTING STARTED</b>	<b>43</b>
<b>1</b>	<b>INTRODUCTION</b>	<b>45</b>
	Key Features	45
	Description of Software Features	46
	Configuration Backup and Restore	46
	Authentication	46
	Access Control Lists	47
	Port Configuration	47
	Rate Limiting	47
	Port Mirroring	47
	Port Trunking	47
	Storm Control	47
	Static Addresses	47
	IP Address Filtering	48
	IEEE 802.1D Bridge	48
	Store-and-Forward Switching	48
	Spanning Tree Algorithm	48
	Virtual LANs	49
	Traffic Prioritization	49
	Quality of Service	49
	Multicast Filtering	49
	Basic System Defaults	50

<b>2</b>	<b>INITIAL SWITCH CONFIGURATION</b>	<b>51</b>
	Connecting to the Switch	51
	Configuration Options	51
	Required Connections	52
	Remote Connections	53
	Console Connection	53
	Setting Passwords	54
	Setting an IPv4 Address	54
	Manual Configuration	55
	Dynamic Configuration	55
<hr/>		
<b>SECTION II</b>	<b>WEB CONFIGURATION</b>	<b>57</b>
<b>3</b>	<b>USING THE WEB INTERFACE</b>	<b>59</b>
	Connecting to the Web Interface	59
	Navigating the Web Browser Interface	60
	Home Page	60
	Configuration Options	61
	Panel Display	61
	Main Menu	62
<b>4</b>	<b>MONITORING SYSTEM STATUS</b>	<b>67</b>
	Displaying the System Settings	68
	Viewing Ethernet Interface	69
	Viewing Etherlike Statistics	70
	Managing RMON Statistics	72
	Viewing RMON Statistics	72
	Configuring RMON History	74
	Viewing the RMON History Table	76
	Defining RMON Events Control	78
	Viewing the RMON Events Logs	80
	Defining RMON Alarms	80
	Monitoring the Health	83
	Viewing Memory Logs	83
	RAM Memory	84
	Flash Memory	84

<b>5 ADMINISTRATION</b>	<b>87</b>
Defining Users	87
Managing the Time Settings	89
System Time Options	89
Configuring System Time	90
Adding an SNTP Server	92
Defining SNTP Authentication	96
Managing System Logs	97
Setting System Log Settings	98
Setting Remote Logging Settings	99
Managing System Files	101
Upgrading/Backing Up Firmware	103
Selecting the Active Image	105
Saving a Configuration	106
Copying/Saving Configuration Files	108
Setting DHCP Auto Configuration	109
Rebooting the Switch	111
Managing Device Diagnostics	112
Displaying Optical Module Status	112
Viewing CPU Utilization	113
Configuring LLDP	114
Setting LLDP Properties	115
Editing LLDP Port Settings	117
LLDP MED Protocol	119
Setting LLDP MED Network Policy	120
Configuring LLDP MED Port Settings	122
Displaying LLDP Neighbors Information	124
Accessing LLDP Statistics	129
LLDP Overloading	130
Displaying LLDP MED Port Status Details	132
Displaying LLDP MED Port Status Table	136
Configuring sFlow	137
sFlow Overview	137
Configuring sFlow Receiver Settings	138
Configuring sFlow Interface Settings	139
Viewing sFlow Statistics	140

<b>6 CONFIGURING PORTS &amp; VLANS</b>	<b>141</b>
Configuring Ports	141
Port Management Workflow	141
Setting the Basic Port Configuration	142
Configuring Link Aggregation	144
Static and Dynamic LAG Workflow	145
Defining LAG Management	146
Defining Member Ports in a LAG	147
Configuring LAG Settings	148
Configuring LACP	149
Setting Port LACP Parameter Settings	150
Configuring VLANs	151
Creating VLANs	153
Configuring VLAN Interface Settings	154
Defining VLAN Membership	156
Configuring Port to VLAN	157
Viewing VLAN Membership	158
Configuring Port and VLAN Mirroring	159
Defining GVRP Settings	161
Managing VLAN Groups	162
Assigning MAC-Based Groups	163
Assigning Subnet-Based Groups	164
Assigning Protocol-Based Groups	165
Mapping VLAN Group to VLAN	166
<b>7 CONFIGURING THE SPANNING TREE PROTOCOL</b>	<b>169</b>
STP Flavors	169
Configuring STP Global Settings	170
Defining STP Interface Settings	172
Configuring RSTP Settings	175
Multiple Spanning Tree Protocol Overview	177
Defining MSTP Properties	178
Mapping VLANs to an MST Instance	179
Defining MST Instance Settings	181
Defining MSTP Interface Settings	182
<b>8 MANAGING MAC ADDRESS TABLES</b>	<b>187</b>
Configuring Static MAC Addresses	187

Dynamic MAC Addresses	189
Configuring Dynamic MAC Address Parameters	189
Querying Dynamic Addresses	189
<b>9 CONFIGURING MULTICAST FORWARDING</b>	<b>191</b>
Multicast Forwarding	191
Typical Multicast Setup	192
Multicast Operation	192
Multicast Registration	193
Multicast Address Properties	193
Defining Multicast Properties	194
Adding MAC Group Address	196
Adding IP Multicast Group Address	198
Configuring IGMP Snooping	200
Configuring MLD Snooping	203
Viewing IGMP/MLD IP Multicast Groups	207
Defining Multicast Router Ports	208
Defining Forward All Multicast	209
Defining Unregistered Multicast Settings	211
<b>10 CONFIGURING IP INFORMATION</b>	<b>213</b>
Management and IP Interfaces	213
IP Addressing	213
Defining an IPv4 Interface	214
Defining IPv6 Global Configuration	216
Defining an IPv6 Interface	217
Defining IPv6 Addresses	219
Viewing the IPv6 Default Router List	220
Configuring IPv6 Tunnels	222
Defining IPv6 Neighbors Information	224
Viewing IPv6 Route Tables	226
Defining IPv4 Static Routing	227
Configuring ARP	228
Defining UDP Relay	230
Domain Name Systems	231
Defining DNS Servers	231
Mapping DNS Hosts	233

<b>11 CONFIGURING SECURITY</b>	<b>237</b>
Configuring TACACS+	238
Configuring Default TACACS+ Parameters	238
Adding a TACACS+ Server	239
Configuring RADIUS Parameters	241
Configuring Management Access Authentication	244
Defining Access Profiles	245
Displaying, Adding, or Activating an Access Profile	246
Defining Profile Rules	249
Defining Storm Control	252
Configuring Port Security	254
Configuring 802.1X	256
802.1X Parameters Workflow	259
Defining 802.1X Properties	259
Defining 802.1X Port Authentication	261
Defining Host and Session Authentication	265
Defining DHCP Snooping	268
Defining DHCP Snooping Properties	268
Defining DHCP Snooping on VLANs	269
Defining Trusted Interfaces	270
Binding Addresses to the DHCP Snooping Database	271
Defining Dynamic ARP Inspection	273
Defining ARP Inspection Properties	274
Defining ARP Inspection Trusted Interfaces	275
Defining ARP Inspection List	277
Assigning ARP Inspection VLAN Settings	278
<b>12 DEFINING ACCESS CONTROL</b>	<b>281</b>
Access Control Lists Overview	281
Defining MAC-based ACLs	283
Adding Rules to a MAC-based ACL	284
Defining IPv4-based ACLs	286
Defining an IPv4-based ACL	287
Adding Rules (ACEs) to an IPv4-Based ACL	287
Defining IPv6-based ACLs	291
Defining an IPv6-based ACL	291
Defining a Rule (ACE) for an IPv6-based ACL	292

Defining ACL Binding	295
<b>13 CONFIGURING QUALITY OF SERVICE</b>	<b>299</b>
QoS Features and Components	299
Configuring QoS	301
Displaying QoS Properties	301
Configuring QoS Queues	303
Mapping CoS/802.1p to a Queue	305
Mapping DSCP to Queue	306
Configuring Bandwidth	307
QoS Basic Mode	309
Configuring Global Settings	309
Interface QoS Settings	311
QoS Advanced Mode	312
Configuring Global Settings	313
Configuring Out-of-Profile DSCP Remarking	315
Defining Class Mapping	316
QoS Policers	318
Defining Aggregate Policers	319
Configuring a Policy	320
Configuring Policy Class Maps	321
Policy Binding	323
<b>14 CONFIGURING DCE</b>	<b>325</b>
Fiber Channel over Ethernet Initialization Protocol (FIP) Snooping	325
FIP MAC Address Filtering	327
FIP Tunnels	328
Cut-Through	330
Limitations and Interactions with Other Features	330
Configuring Cut-Through	330
Quantized Congestion Notification (QCN)	332
Queue Configuration	332
CN Tag Recognition	333
Limitations and Interactions with Other Features	333
Configuring QCN	333
Priority-based Flow Control (PFC)	335
Priority to Queue Mapping	336
PFC Priority Operational State	336

Buffers Allocation	337
PFC and QoS	337
Limitation in Regard to QoS	338
Remapping	338
ISCSI with PFC	339
Voice VLAN	340
PFC and Shaper Coexistence	340
Performance	340
Cascade ports	340
PFC and LAGs	341
Coexistence with Link Level FC (802.3x)	341
Configuring PFC	341
Configuring ETS	342
Data Center Discovery and Capability Exchange Protocol (DCBX)	343
Configuring DCBX Through the GUI	343
<b>15 CONFIGURING SNMP</b>	<b>347</b>
SNMP Versions and Workflow	347
SNMP v1 and v2	347
SNMP v3	348
SNMP Workflow	348
Supported MIBs	349
Model OID	350
SNMP Engine ID	350
Configuring SNMP Views	351
Managing SNMP Users	353
Creating SNMP Groups	356
Defining SNMP Communities	358
Defining Trap Settings	360
Defining Notification Recipients	361
Defining SNMPv1,2 Notification Recipients	361
Defining SNMPv3 Notification Recipients	363
Configuring SNMP Notification Filters	365

---

<b>SECTION III</b>	<b>COMMAND LINE INTERFACE</b>	<b>367</b>
<b>16</b>	<b>USING THE CLI INTERFACE</b>	<b>369</b>
	CLI Command Modes	369
	User EXEC Mode	369
	Privileged EXEC Mode	370
	Global Configuration Mode	370
	Interface Configuration Modes	370
	Starting the CLI	371
	CLI Command Conventions	372
	Entering Commands	372
	Terminal Command Buffer	373
	Negating the Effect of Commands	373
	Command Completion	373
	Keyboard Shortcuts	374
<b>17</b>	<b>USER INTERFACE COMMANDS</b>	<b>375</b>
	enable	375
	disable	375
	login	376
	configure	376
	exit (Configuration)	377
	exit (EXEC)	377
	end	377
	help	378
	history	378
	history size	379
	terminal history	380
	terminal history size	380
	terminal datadump	381
	debug-mode	382
	show history	382
	show privilege	383
	do	383
	banner exec	384
	banner login	385

banner motd	386
exec-banner	388
login-banner	388
motd-banner	389
show banner	389
<b>18 SYSTEM MANAGEMENT COMMANDS</b>	<b>391</b>
ping	391
traceroute	393
telnet	396
resume	398
hostname	399
reload	399
service cpu-utilization	400
show cpu utilization	400
clear cpu counters	401
service cpu-counters	401
show cpu counters	402
show users	402
show sessions	403
show system	404
show version	404
system resources routing	405
show system resources routings	405
show system tcam utilization	406
show system defaults	406
show tech-support	408
show system id	410
<b>19 CLOCK COMMANDS</b>	<b>411</b>
clock set	411
clock source	411
clock timezone	412
clock summer-time	413
sntp authentication-key	414
sntp authenticate	415
sntp trusted-key	416
sntp client poll timer	416

snmp broadcast client enable	417
snmp anycast client enable	417
snmp client enable	418
snmp client enable (Interface)	419
snmp unicast client enable	419
snmp unicast client poll	420
snmp server	420
snmp port	422
show clock	423
show snmp configuration	424
show snmp status	424
<b>20 CONFIGURATION AND IMAGE FILE COMMANDS</b>	<b>426</b>
copy	426
delete	429
dir	430
more	430
rename	431
boot system	432
show running-config	433
show startup-config	433
show bootvar	434
<b>21 AUTO-UPDATE AND AUTO-CONFIGURATION</b>	<b>435</b>
boot host auto-config	435
show boot	435
ip dhcp tftp-server ip addr	437
ip dhcp tftp-server file	438
show ip dhcp tftp-server	438
<b>22 MANAGEMENT ACL COMMANDS</b>	<b>439</b>
management access-list	439
permit (Management)	440
deny (Management)	441
management access-class	442
show management access-list	442
show management access-class	443

<b>23 NETWORK MANAGEMENT PROTOCOL (SNMP) COMMANDS</b>	<b>444</b>
snmp-server	444
snmp-server community	444
snmp-server view	446
snmp-server group	447
snmp-server user	449
snmp-server filter	450
snmp-server host	451
snmp-server engineID local	453
snmp-server enable traps	454
snmp-server trap authentication	455
snmp-server contact	455
snmp-server location	456
snmp-server set	456
show snmp	457
show snmp engineID	458
show snmp views	458
show snmp groups	459
show snmp filters	460
show snmp users	460
<b>24 RSA AND CERTIFICATE COMMANDS</b>	<b>462</b>
crypto key generate dsa	462
crypto key generate rsa	462
show crypto key mypubkey	463
crypto certificate generate	464
crypto certificate request	465
crypto certificate import	466
crypto certificate export pkcs12	467
crypto certificate import pkcs12	468
show crypto certificate mycertificate	469
<b>25 WEB SERVER COMMANDS</b>	<b>471</b>
ip http server	471
ip http port	471
ip http timeout-policy	472
ip http secure-server	473
ip http secure-port	473

ip https certificate	474
show ip http	474
show ip https	475
<b>26 TELNET, SECURE SHELL (SSH), AND SECURE LOGIN (SLOGIN) COMMANDS</b>	<b>476</b>
ip telnet server	476
ip ssh port	476
ip ssh server	477
ip ssh pubkey-auth	477
crypto key pubkey-chain ssh	478
user-key	479
key-string	479
show ip ssh	481
show crypto key pubkey-chain ssh	481
<b>27 LINE COMMANDS</b>	<b>483</b>
line	483
speed	483
autobaud	484
exec-timeout	485
show line	485
<b>28 AAA COMMANDS</b>	<b>487</b>
aaa authentication login	487
aaa authentication enable	488
login authentication	490
enable authentication	490
ip http authentication	491
show authentication methods	492
password	493
enable password	493
username	494
show user accounts	494
aaa accounting login	495
aaa accounting dot1x	496
show accounting	498
passwords strength minimum character-classes	498
passwords strength max-limit repeated-characters	499

<b>29 RADIUS COMMANDS</b>	<b>500</b>
radius-server host	500
radius-server key	502
radius-server retransmit	503
radius-server source-ip	503
radius-server source-ipv6	504
radius-server timeout	505
radius-server deadtime	505
show radius-servers	506
<b>30 TACACS+ COMMANDS</b>	<b>507</b>
tacacs-server host	507
tacacs-server key	508
tacacs-server timeout	509
tacacs-server source-ip	509
show tacacs	510
<b>31 SYSLOG COMMANDS</b>	<b>512</b>
logging on	512
Logging host	512
logging console	514
logging buffered	514
clear logging	515
logging file	515
clear logging file	516
aaa logging	516
file-system logging	517
management logging	517
show logging	518
show logging file	519
show syslog-servers	520
<b>32 REMOTE NETWORK MONITORING (RMON) COMMANDS</b>	<b>521</b>
show rmon statistics	521
rmon collection stats	522
show rmon collection stats	523
show rmon history	524
rmon alarm	526

show rmon alarm-table	528
show rmon alarm	528
rmon event	530
show rmon events	531
show rmon log	531
rmon table-size	532
<b>33 802.1X COMMANDS</b>	<b>534</b>
aaa authentication dot1x	534
dot1x system-auth-control	535
dot1x port-control	535
dot1x reauthentication	536
dot1x timeout reauth-period	537
dot1x re-authenticate	537
dot1x timeout quiet-period	538
dot1x timeout tx-period	539
dot1x max-req	539
dot1x timeout supp-timeout	540
dot1x timeout server-timeout	541
show dot1x	542
show dot1x users	544
show dot1x statistics	545
dot1x auth-not-req	546
dot1x host-mode	546
dot1x violation-mode	547
dot1x guest-vlan	548
dot1x guest-vlan timeout	549
dot1x guest-vlan enable	550
dot1x mac-authentication	550
dot1x radius-attributes vlan	551
show dot1x advanced	552
<b>34 ETHERNET CONFIGURATION COMMANDS</b>	<b>553</b>
interface	553
interface range	553
shutdown	553
description	554
speed	555

flowcontrol	555
port jumbo-frame	556
clear counters	556
set interface active	557
errdisable recovery cause	558
errdisable recovery interval	559
show interfaces configuration	559
show interfaces status	560
show interfaces advertise	560
show interfaces description	561
show interfaces counters	562
show port jumbo-frame	563
show errdisable recovery	564
show errdisable interfaces	564
storm-control broadcast enable	565
storm-control broadcast level kbps	566
storm-control include-multicast	566
show storm-control	567
<b>35 PHY DIAGNOSTICS COMMANDS</b>	<b>568</b>
show fiber-ports optical-transceiver	568
<b>36 PORT CHANNEL COMMANDS</b>	<b>570</b>
channel-group	570
port-channel load-balance	571
show interfaces port-channel	571
<b>37 ADDRESS TABLE COMMANDS</b>	<b>573</b>
bridge multicast filtering	573
bridge multicast mode	573
bridge multicast address	575
bridge multicast forbidden address	576
bridge multicast forbidden ip-address	577
bridge multicast source group	578
bridge multicast forbidden source group	579
bridge multicast ipv6 mode	580
bridge multicast ipv6 forbidden ip-address	581
bridge multicast ipv6 source group	582

bridge multicast ipv6 forbidden source group	583
bridge multicast unregistered	584
bridge multicast forward-all	585
bridge multicast forbidden forward-all	586
mac address-table static	587
clear mac address-table	588
mac address-table aging-time	588
port security	589
port security mode	589
port security max	590
port security routed secure-address	591
show mac address-table	591
show mac address-table count	592
show bridge multicast mode	593
show bridge multicast address-table	593
show bridge multicast address-table static	596
show bridge multicast filtering	598
show bridge multicast unregistered	598
show ports security	599
show ports security addresses	600
<b>38 PORT MONITOR COMMANDS</b>	<b>601</b>
port monitor	601
show ports monitor	603
port monitor mode	603
<b>39 sFLOW COMMANDS</b>	<b>605</b>
sflow receiver	605
sflow flow-sampling	606
sflow counters-sampling	606
clear sflow statistics	607
show sflow configuration	607
show sflow statistics	608
<b>40 LINK LAYER DISCOVERY PROTOCOL (LLDP) COMMANDS</b>	<b>609</b>
lldp run	609
lldp transmit	609
lldp receive	610

lldp timer	611
lldp hold-multiplier	611
lldp reinit	612
lldp tx-delay	612
lldp optional-tlv	613
lldp management-address	614
lldp notifications	615
lldp notifications interval	615
lldp optional-tlv 802.1	616
lldp med enable	617
lldp med notifications topology-change	617
lldp med fast-start repeat-count	618
lldp med network-policy (global)	618
lldp med network-policy (interface)	619
clear lldp table	620
lldp med location	620
show lldp configuration	621
show lldp med configuration	623
show lldp local tlvs-overloading	624
show lldp local	624
show lldp neighbors	626
show lldp statistics	629
<b>41 SPANNING-TREE COMMANDS</b>	<b>631</b>
spanning-tree	631
spanning-tree mode	631
spanning-tree forward-time	632
spanning-tree hello-time	633
spanning-tree max-age	634
spanning-tree priority	634
spanning-tree disable	635
spanning-tree cost	636
spanning-tree port-priority	636
spanning-tree portfast	637
spanning-tree link-type	638
spanning-tree pathcost method	638
spanning-tree bpdu (Global)	639

spanning-tree bpdu (Interface)	640
spanning-tree guard root	641
spanning-tree bpduguard	642
clear spanning-tree detected-protocols	642
spanning-tree mst priority	643
spanning-tree mst max-hops	644
spanning-tree mst port-priority	644
spanning-tree mst cost	645
spanning-tree mst configuration	646
instance (MST)	646
name (MST)	647
revision (MST)	647
show (MST)	648
exit (MST)	649
abort (MST)	649
show spanning-tree	649
show spanning-tree bpdu	658
spanning-tree loopback-guard	659
<b>42 VIRTUAL LOCAL AREA NETWORK (VLAN) COMMANDS</b>	<b>661</b>
vlan database	661
vlan	661
interface vlan	662
interface range vlan	662
name	663
switchport protected-port	664
switchport community	664
show interfaces protected-ports	665
switchport	665
switchport mode	666
switchport access vlan	667
switchport trunk allowed vlan	667
switchport trunk native vlan	668
switchport general allowed vlan	669
switchport general pvid	670
switchport general ingress-filtering disable	670
switchport general acceptable-frame-type	671

map protocol protocols-group	672
switchport general map protocols-group vlan	673
map mac macs-group	673
switchport general map macs-group vlan	674
map subnet subnets-group	675
switchport general map subnets-group vlan	675
show vlan	676
show vlan protocols-groups	677
show vlan macs-groups	677
show vlan subnets-groups	678
show interfaces switchport	678
<b>43 VIRTUAL LOCAL AREA NETWORK (VLAN) NON-ISCLI COMMANDS</b>	<b>681</b>
switchport forbidden default-vlan	681
switchport forbidden vlan	681
switchport default-vlan tagged	682
show interfaces switchport	683
<b>44 IGMP SNOOPING COMMANDS</b>	<b>686</b>
ip igmp snooping (Global)	686
ip igmp snooping vlan	686
ip igmp snooping mrouter	687
ip igmp snooping mrouter interface	688
ip igmp snooping forbidden mrouter interface	688
ip igmp snooping static	689
ip igmp snooping querier	690
ip igmp snooping querier address	691
ip igmp snooping querier version	691
ip igmp robustness	692
ip igmp query-interval	692
ip igmp query-max-response-time	693
ip igmp last-member-query-count	694
ip igmp last-member-query-interval	694
ip igmp snooping vlan immediate-leave	695
show ip igmp snooping mrouter	695
show ip igmp snooping interface	696
show ip igmp snooping groups	697

<b>45 IPv6 MLD Snooping Commands</b>	<b>698</b>
ipv6 mld snooping (Global)	698
ipv6 mld snooping vlan	698
ipv6 mld robustness	699
ipv6 mld snooping mrouter	699
ipv6 mld snooping mrouter interface	700
ipv6 mld snooping forbidden mrouter interface	701
ipv6 mld snooping static	702
ipv6 mld query-interval	702
ipv6 mld query-max-response-time	703
ipv6 mld last-member-query-count	704
ipv6 mld last-member-query-interval	704
ipv6 mld snooping vlan immediate-leave	705
show ipv6 mld snooping mrouter	705
show ipv6 mld snooping interface	706
show ipv6 mld snooping groups	706
<b>46 Link Aggregation Control Protocol (LACP) Commands</b>	<b>709</b>
lacp system-priority	709
lacp port-priority	709
lacp timeout	710
show lacp	710
show lacp port-channel	712
<b>47 GARP VLAN Registration Protocol (GVRP) Commands</b>	<b>713</b>
gvrp enable (Global)	713
gvrp enable (Interface)	713
garp timer	714
gvrp vlan-creation-forbid	715
gvrp registration-forbid	716
clear gvrp statistics	716
show gvrp configuration	717
show gvrp statistics	717
show gvrp error-statistics	718
<b>48 DHCP Snooping and ARP Inspection Commands</b>	<b>720</b>
ip dhcp snooping	720
ip dhcp snooping vlan	720

ip dhcp snooping trust	721
ip dhcp snooping information option allowed-untrusted	722
ip dhcp snooping verify	722
ip dhcp snooping database	723
ip dhcp snooping database update-freq	723
ip dhcp snooping binding	724
clear ip dhcp snooping database	725
show ip dhcp snooping	725
show ip dhcp snooping binding	726
ip source-guard	727
ip arp inspection	728
ip arp inspection vlan	728
ip arp inspection trust	729
ip arp inspection validate	730
ip arp inspection list create	730
ip mac	731
ip arp inspection list assign	732
ip arp inspection logging interval	732
show ip arp inspection	733
show ip arp inspection list	733
show ip arp inspection statistics	734
clear ip arp inspection statistics	734
ip dhcp information option	735
show ip dhcp information option	735
<b>49 IP ADDRESSING COMMANDS</b>	<b>737</b>
ip address	737
ip address dhcp	738
renew dhcp	739
ip default-gateway	740
show ip interface	741
arp	741
arp timeout (Global)	742
arp timeout	743
clear arp-cache	743
show arp	744
show arp configuration	744

ip helper-address	745
show ip helper-address	746
ip domain lookup	747
ip domain name	747
ip name-server	748
ip host	749
clear host	750
clear host dhcp	750
show hosts	751
<b>50 IPv6 ADDRESSING COMMANDS</b>	<b>753</b>
ipv6 enable	753
ipv6 address autoconfig	754
ipv6 icmp error-interval	754
show ipv6 icmp error-interval	755
ipv6 address	756
ipv6 address link-local	757
ipv6 unreachable	758
ipv6 default-gateway	758
show ipv6 interface	759
show IPv6 route	760
ipv6 nd dad attempts	761
ipv6 host	762
ipv6 neighbor	763
ipv6 set mtu	764
ipv6 mld version	765
ipv6 mld join-group	765
show ipv6 neighbors	766
clear ipv6 neighbors	767
<b>51 IP ROUTING PROTOCOL-INDEPENDENT COMMANDS</b>	<b>769</b>
ip route	769
ip routing	770
show ip route	770
<b>52 TUNNEL COMMANDS</b>	<b>772</b>
interface tunnel	772
tunnel mode ipv6ip	772

tunnel isatap router	773
tunnel source	774
tunnel isatap query-interval	775
tunnel isatap solicitation-interval	775
tunnel isatap robustness	776
show ipv6 tunnel	777
<b>53 ACL COMMANDS</b>	<b>778</b>
ip access-list extended	778
permit ( IP )	778
deny ( IP )	781
ipv6 access-list	783
permit ( IPv6 )	784
deny ( IPv6 )	786
mac access-list	788
permit ( MAC )	789
service-acl	790
show access-lists	791
show interfaces access-lists	792
clear access-lists counters	792
show interfaces access-lists counters	792
<b>54 QUALITY OF SERVICE (QoS) COMMANDS</b>	<b>794</b>
qos	794
qos advanced-mode trust	795
show qos	795
class-map	796
show class-map	797
match	798
policy-map	798
class	799
show policy-map	800
trust	801
set	802
police	803
service-policy	804
qos aggregate-policer	805
show qos aggregate-policer	806

police aggregate	806
wrr-queue cos-map	807
wrr-queue bandwidth	808
priority-queue out num-of-queues	809
traffic-shape	810
traffic-shape queue	810
rate-limit (Ethernet)	811
rate-limit (VLAN)	812
qos wrr-queue wrtd	813
show qos interface	813
wrr-queue	815
qos wrr-queue threshold	816
qos map policed-dscp	817
qos map dscp-queue	817
qos map dscp-dp	818
qos trust (Global)	819
qos trust (Interface)	820
qos cos	820
qos dscp-mutation	821
qos map dscp-mutation	821
show qos map	822
clear qos statistics	824
qos statistics policer	824
qos statistics aggregate-policer	825
qos statistics queues	825
show qos statistics	826
<b>55 DATA CENTER ETHERNET COMMANDS</b>	<b>829</b>
dce priority-flow-control enable (Global)	829
dce priority-flow-control priority enable	829
dce priority-flow-control enable (interface)	830
show dce priority-flow-control	831
dce qcn enable (global)	831
dce qcn priority enable	832
dce qcn cnm priority	833
dce qcn cp enable	833
dce qcn cp set-point	834

dce qcn cp feedback-weight	834
dce qcn cp min-sample-base	835
show dce qcn	835
dce dcbx enable	837
dce dcbx advertise priority-groups	837
dce dcbx advertise priority-flow-control	838
dce dcbx advertise application-protocol	838
dce application-protocol enable	839
dce application-protocol map	839
show dce dcbx	840
wrr-queue bandwidth (ETS)	842
show dce ets	843
dce cut-through enable (global)	844
dce cut-through enable (interface)	844
dce cut-through priority enable	845
dce cut-through untagged enable	845
dce cut-through packet-length	846
show dce cut-through	847
dce fip-snooping enable (Global)	847
dce fip-snooping enable (Interface)	848
dce fip-snooping fcf-address-filtering enable	849
dce fip-snooping fcf-address-filtering list	849
dce fip-snooping tunnel	850
clear dce fip-snooping tunnel	850
show dce fip-snooping configuration	851
show dce fip-snooping tunnels	851

---

<b>SECTION IV</b>	<b>APPENDICES</b>	<b>853</b>
	<b>A TROUBLESHOOTING</b>	<b>855</b>
	Problems Accessing the Management Interface	855
	Using System Logs	856
	<b>INDEX</b>	<b>857</b>



# FIGURES

Figure 1: Home Page	60
Figure 2: Front Panel Indicators	61
Figure 3: System Settings Page	68
Figure 4: Interface Page	69
Figure 5: Etherlike Page	71
Figure 6: Statistics Page	73
Figure 7: History Control Table Page	75
Figure 8: Add RMON History Page	76
Figure 9: History Table Page	77
Figure 10: Events Page	78
Figure 11: Add RMON Events Page	79
Figure 12: Event Log Table Page	80
Figure 13: Alarms Page	81
Figure 14: Add RMON Alarm Page	81
Figure 15: Health Page	83
Figure 16: RAM Memory Page	84
Figure 17: Flash Memory Page	85
Figure 18: User Accounts Page	88
Figure 19: Add/Edit User Account Page	88
Figure 20: System Time Page	91
Figure 21: SNTP Settings Page	93
Figure 22: Add SNTP Server Page	94
Figure 23: SNTP Authentication Page	96
Figure 24: Add SNTP Authentication Page	97
Figure 25: Log Settings Page	99
Figure 26: Remote Log Server Page	100
Figure 27: Add Remote Log Server Page	100
Figure 28: Upgrade/Backup Firmware Page	104
Figure 29: Active Image Page	106
Figure 30: Save Configuration Page	107
Figure 31: Copy/Save Configuration Page	109

Figure 32: DHCP Auto Configuration Page	110
Figure 33: Reboot Page	111
Figure 34: Optical Module Status Page	113
Figure 35: CPU Utilization Page	114
Figure 36: Properties Page	116
Figure 37: Port Settings Page	117
Figure 38: Edit LLDP Port Settings Page	118
Figure 39: LLDP MED Network Policy Page	121
Figure 40: Add LLDP MED Network Policy Page	121
Figure 41: LLDP MED Port Settings Page	122
Figure 42: Edit LLDP MED Port Settings Page	123
Figure 43: LLDP Neighbors Information Page	124
Figure 44: Neighbors Information Page	125
Figure 45: LLDP Statistics Page	129
Figure 46: LLDP Overloading Page	130
Figure 47: LLDP Overloading Details	131
Figure 48: LLDP MED Port Status Details Page	133
Figure 49: LLDP MED Port StatusTable Page	136
Figure 50: sFlow Receivers Settings Page	138
Figure 51: sFlow Interface Settings Page	139
Figure 52: sFlow Statistics Page	140
Figure 53: Port Settings Page	142
Figure 54: Edit Port Settings Page	143
Figure 55: LAG Management Page	146
Figure 56: Edit LAG Membership Page	147
Figure 57: LAG Settings Page	148
Figure 58: Edit LAG Settings Page	148
Figure 59: LACP Page	150
Figure 60: Edit LACP Page	151
Figure 61: Create VLAN Page	153
Figure 62: Add/Edit VLAN Page	154
Figure 63: Interface Settings Page	155
Figure 64: Edit Interface Setting Page	155
Figure 65: Port to VLAN Page	157
Figure 66: Port VLAN Membership Page	158
Figure 67: Port and VLAN Mirroring Page	160

Figure 68: Add Port/VLAN Mirroring Page	160
Figure 69: GVRP Settings Page	161
Figure 70: Edit GVRP Setting Page	162
Figure 71: MAC-Based Groups Page	163
Figure 72: Add MAC-Based Group Page	163
Figure 73: Subnet-Based Groups Page	164
Figure 74: Add Subnet-Based Group Page	165
Figure 75: Protocol-Based Groups Page	165
Figure 76: Add Protocol-Based Group Page	166
Figure 77: Mapping Group to VLAN Page	166
Figure 78: Add Mapping Group to VLAN Page	167
Figure 79: STP Global Settings Page	170
Figure 80: STP Interface Settings Page	172
Figure 81: Edit Interface Settings Page	173
Figure 82: RSTP Interface Settings Page	175
Figure 83: Edit Rapid Spanning Tree Page	176
Figure 84: MSTP Properties Page	179
Figure 85: VLAN to MST Instance Page	180
Figure 86: Edit MST to VLAN Page	180
Figure 87: MST Instance Settings Page	181
Figure 88: MST Interface Settings Page	182
Figure 89: Edit Interface Settings Page	183
Figure 90: Static Addresses Page	188
Figure 91: Add Static Address Page	188
Figure 92: Dynamic Addresses Setting Page	189
Figure 93: Dynamic Addresses Page	190
Figure 94: Properties Page	195
Figure 95: MAC Group Address Page	196
Figure 96: Add MAC Group Address Page	197
Figure 97: MAC Group Address Settings Page	197
Figure 98: IP Multicast Group Address Page	198
Figure 99: IP Multicast Group Address Details Page	199
Figure 100: IP Multicast Interface Settings Page	200
Figure 101: IGMP Snooping Page	201
Figure 102: Edit IGMP Snooping Page	202
Figure 103: MLD Snooping Page	205

Figure 104: Edit MLD Snooping Page	205
Figure 105: IGMP/MLD IP Multicast Group Page	207
Figure 106: Multicast Router Port Page	208
Figure 107: Forward All Page	210
Figure 108: Unregistered Multicast Page	211
Figure 109: Edit Unregistered Multicast Page	212
Figure 110: IPv4 Interface Page	215
Figure 111: Add IPv4 Interface Page	216
Figure 112: IPv6 Global Configuration Page	217
Figure 113: IPv6 Interfaces Page	217
Figure 114: Add IPv6 Interface Page	218
Figure 115: IPv6 Address Page	219
Figure 116: Add IPv6 Address Page	219
Figure 117: IPv6 Default Router List Page	221
Figure 118: Add Default Router Page	222
Figure 119: IPv6 Tunnel Page	223
Figure 120: IPv6 Neighbors Page	224
Figure 121: Add IPv6 Neighbors Page	225
Figure 122: IPv6 Routes Table Page	226
Figure 123: IPv4 Static Routes	227
Figure 124: Add IPv4 Static Routes	227
Figure 125: ARP Table Page	229
Figure 126: Add ARP Page	230
Figure 127: UDP Relay Page	231
Figure 128: Add UDP Relay Page	231
Figure 129: DNS Servers Page	232
Figure 130: Add DNS Server Page	233
Figure 131: Host Mapping Page	234
Figure 132: Add Host Mapping Page	234
Figure 133: TACACS+ Page	239
Figure 134: Add TACACS+ Server Page	240
Figure 135: RADIUS Page	241
Figure 136: Add RADIUS Server Page	242
Figure 137: Management Access Authentication Page	244
Figure 138: Access Profiles Page	247
Figure 139: Caution Message	247

Figure 140: Add Access Profile Page	248
Figure 141: Profiles Rules Page	250
Figure 142: Add Profile Rule Page	250
Figure 143: Storm Control Page	252
Figure 144: Edit Storm Control Page	253
Figure 145: Port Security Page	255
Figure 146: Edit Port Security Interface Settings Page	255
Figure 147: Properties Page	260
Figure 148: Edit VLAN Authentication Page	261
Figure 149: Port Authentication Page	262
Figure 150: Edit Port Authentication Page	262
Figure 151: Host and Session Authentication Page	266
Figure 152: Edit Host and Session Authentication Page	267
Figure 153: Properties Page	268
Figure 154: VLAN Settings Page	270
Figure 155: Trusted Interfaces Page	270
Figure 156: Edit Trusted Interface Page	271
Figure 157: Binding Database Page	271
Figure 158: Add Binding Database Page	273
Figure 159: ARP Inspection Properties Page	275
Figure 160: ARP Inspection Trusted Interfaces Page	276
Figure 161: Edit Trusted Interfaces Page	276
Figure 162: ARP Inspection List Page	277
Figure 163: Add ARP List Page	277
Figure 164: ARP Inspection VLAN Settings Page	278
Figure 165: Add VLAN Settings Page	279
Figure 166: MAC-Based ACL Page	283
Figure 167: Add MAC-Based ACL Page	284
Figure 168: MAC-Based ACE Page	284
Figure 169: Add MAC-Based ACE Page	285
Figure 170: IPv4-Based ACL Page	287
Figure 171: Add IPv4-Based ACL Page	287
Figure 172: IPv4-Based ACE Page	287
Figure 173: Add IPv4-Based ACE Page	288
Figure 174: IPv6-Based ACL Page	292
Figure 175: Add IPv6-based ACL Page	292

Figure 176: IPv6-Based ACE Page	292
Figure 177: Add IPv6-Based ACE Page	293
Figure 178: ACL Binding Page	296
Figure 179: Edit ACL Binding Page	296
Figure 180: QoS Properties Page	302
Figure 181: Edit Interface CoS Configuration Page	302
Figure 182: Queue Page	304
Figure 183: CoS/802.1p to Queue Page	306
Figure 184: DSCP to Queue Page	307
Figure 185: Bandwidth Page	308
Figure 186: Edit Bandwidth Page	308
Figure 187: Global Settings Page	310
Figure 188: Edit QoS Interface Settings Page	311
Figure 189: Advanced Global Settings Page	314
Figure 190: DSCP Remarking Page	316
Figure 191: Class Mapping Page	317
Figure 192: Add Class Mapping Page	317
Figure 193: Aggregate Policer Page	319
Figure 194: Add Aggregate Policer Page	319
Figure 195: Policy Table Page	321
Figure 196: Add Policy Table Page	321
Figure 197: Policy Class Maps Page	321
Figure 198: Add Policy Class Map Page	322
Figure 199: Policy Binding Page	324
Figure 200: FIP Snooping Page	326
Figure 201: Edit FIP Snooping Interface Settings Page	326
Figure 202: FCF Mac Address Filtering Page	327
Figure 203: Add FCF MAC Address Filter Page	327
Figure 204: FIP Snooping Tunnel Setting Table Page	329
Figure 205: Add Static FIP Snooping Tunnel Page	329
Figure 206: Cut-through Page	331
Figure 207: Edit Interface Setting Page	332
Figure 208: QCN Page	334
Figure 209: Edit Quantized Congestion Notification Page	335
Figure 210: Difference Between IEEE 802.3x PAUSE and PFC Frames	336
Figure 211: PFC Page	341

Figure 212: Edit Priority-based Flow Control Page	342
Figure 213: ETS Page	342
Figure 214: DCBX Page	343
Figure 215: Edit Port Settings Page	344
Figure 216: Application to Priority Mapping Table Page	344
Figure 217: Add Application to Priority Mapping Page	345
Figure 218: Engine ID Page	351
Figure 219: SNMP Views Page	352
Figure 220: Add View Page	352
Figure 221: SNMP Users Page	354
Figure 222: Add User Page	354
Figure 223: Groups Page	356
Figure 224: Add Group Page	357
Figure 225: Communities Page	358
Figure 226: Add SNMP Community Page	359
Figure 227: Trap Settings Page	360
Figure 228: SNMPv1,2 Notification Recipient Page	361
Figure 229: Add SNMP Notification Recipient Page	362
Figure 230: SNMPv3 Notification Recipient Page	363
Figure 231: Add SNMP Notification Recipient Page	363
Figure 232: Notification Filter Page	365
Figure 233: Add Notification Filter Page	365



# TABLES

Table 1: Key Features	45
Table 2: Basic System Defaults	50
Table 3: Web Page Configuration Buttons	61
Table 4: Switch Main Menu	62
Table 5: Default Mapping Queues	305
Table 6: CLI Conventions	372
Table 7: Keyboard Keys	374
Table 8: Troubleshooting Chart	855



# 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 45](#)
- ◆ ["Initial Switch Configuration" on page 51](#)



This switch provides a broad range of features for Layer 2 switching. 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 HTTP/TFTP server
Authentication	Console, Telnet, web – user name/password, RADIUS, TACACS+ Port – IEEE 802.1X, MAC-based authentication 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) Network Access – MAC Address Authentication Port Authentication – IEEE 802.1X Port Security – MAC address filtering
Access Control Lists	Supports IPv4, IPv6, and MAC ACLs, 512 rules per system
DHCP	Client
DNS	Client
Port Configuration	Speed and duplex mode and flow control
Port Trunking	Supports up to 8 trunks – static or dynamic trunking (LACP)
Port Mirroring	One or more source ports to one analysis port
Congestion Control	Rate Limiting Throttling for broadcast, multicast, unknown unicast storms
Address Table	32K MAC addresses in the forwarding table, 1K static MAC addresses, 256 L2 multicast groups
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)

**Table 1: Key Features** (Continued)

Feature	Description
Virtual LANs	Up to 256 using IEEE 802.1Q, port-based, protocol-based, subnet-based VLANs
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, 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/MLD snooping, query, and profile filtering
Data Center Ethernet	Supports FIP Snooping, cut-through switching, QCN, PFC, ETS, and DCBX

## 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 or unknown unicast traffic storms from engulfing the network. Port-based, protocol-based and subnet-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 HTTP/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 verifies the client's right to access the network via an authentication 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 IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, next header type, or flow label), 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 802.3-2005).

**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, VLAN or packets with a specified MAC address 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 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.

**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 8K 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 32 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 802.1D-2004) – 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 802.1D-2004) – 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 256 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.
- ◆ Use protocol VLANs to restrict traffic to specified interfaces based on protocol type. Mac-based and subnet-based VLANs are also supported.

**TRAFFIC PRIORITIZATION** This switch prioritizes each packet based on the required level of service, using four priority queues with strict or Weighted Round Robin 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 DSCP field in the IP frame. 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.

**MULTICAST FILTERING** Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration for IPv4 traffic.

## BASIC SYSTEM DEFAULTS

The following table lists some of the basic system defaults.

**Table 2: Basic System Defaults**

Function	Parameter	Default
Console Port Connection	Baud Rate	115200 bps
	Data bits	8
	Stop bits	1
	Parity	None
	Local Console Timeout	10 minutes
Authentication	Privileged Exec User Name	admin
	Privileged Exec Password	<i>None</i>
IP Settings	IP Address	<i>None</i>
	Subnet Mask	<i>None</i>
	Default Gateway	<i>None</i>
	DHCP Client	Enabled
Virtual LANs	Default VLAN	1
	PVID	1
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Disabled
	HTTP Secure Server Port	443
SNMP	SNMP Agent	Enabled
	Community Strings	<i>None</i>

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 (Groups 1, 2, 3, 9) 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 IP address for this switch is obtained via DHCP by default. To change this address, see "[Setting an IPv4 Address.](#)"

---

### 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 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0 or above. 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 or Secure Shell (SSH) 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 management functions such as those shown below:

- ◆ Set user names and passwords
- ◆ Set an IP interface
- ◆ 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 256 IEEE 802.1Q VLANs
- ◆ Enable GVRP automatic VLAN registration
- ◆ 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

**REQUIRED CONNECTIONS**

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

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

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

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
  - Select the appropriate serial port (COM port 1 or COM port 2).
  - Set the baud rate to 115200 bps.

- Set the data format to 8 data bits, 1 stop bit, and no parity.
- Set flow control to none.
- Set the emulation mode to VT100.
- When using HyperTerminal, select Terminal keys, not Windows keys.



---

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

---

For a description of how to use the CLI, see ["Using the CLI Interface" on page 369.](#)

## REMOTE CONNECTIONS

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

The IP address for this switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP, see ["Setting an IPv4 Address" on page 54.](#)



---

**NOTE:** This switch supports four concurrent Telnet or SSH sessions.

---

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The command-line interface can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 5.0 or above, Netscape 6.2 or above, or Mozilla Firefox 2.0 or above), or from a network computer using SNMP network management software.

---

## CONSOLE CONNECTION

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

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name for the Privileged Exec level. To log into the CLI at the Privileged Exec level using the default user name, 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.” (There is no default password.)
3. 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 a new password for the default user name using the “username” command, record it and put it in a safe place.

Passwords can consist of up to 159 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 “admin” to access the Privileged Exec level.
2. Type “configure” and press <Enter>.
3. Type “username admin password *password*,” for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
User Name:admin

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

---

## SETTING AN IPV4 ADDRESS

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

- ◆ **Manual** — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.
- ◆ **Dynamic** — The switch can send IP configuration requests to a DHCP address allocation server on the network.

**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 IP 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 IP address for this switch is obtained via DHCP by default.

To assign an IP 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
```

**DYNAMIC  
CONFIGURATION****Obtaining an IPv4 Address**

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

Note that the "renew dhcp" command can be used to start broadcasting service requests for any VLAN configured to obtain address assignments through 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 "dhcp" option is saved to the startup-config file, then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with 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, type "ip address dhcp" and press <Enter>.
3. Type "end" to return to the Privileged Exec mode. Press <Enter>.
4. Wait a few minutes, and then check the IP configuration settings by typing the "show ip interface" command. Press <Enter>.
5. Then save your configuration changes by typing "copy running-config startup-config." Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#copy running-config startup-config
Overwrite file [startup-config] ?[Yes/press any key for no]...01-Jan-2010
06:13:19 %COPY-I-FILECPY: Files Copy - source URL running-config
destination URL flash://startup-config
01-Jan-2010 06:13:29 %COPY-N-TRAP: The copy operation was completed
successfully
Copy succeeded
```

# 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 59](#)
- ◆ ["Monitoring System Status" on page 67](#)
- ◆ ["Administration" on page 87](#)
- ◆ ["Configuring Ports & VLANs" on page 141](#)
- ◆ ["Configuring the Spanning Tree Protocol" on page 169](#)
- ◆ ["Managing MAC Address Tables" on page 187](#)
- ◆ ["Configuring Multicast Forwarding" on page 191](#)
- ◆ ["Configuring IP Information" on page 213](#)
- ◆ ["Configuring Security" on page 237](#)
- ◆ ["Defining Access Control" on page 281](#)
- ◆ ["Configuring Quality of Service" on page 299](#)
- ◆ ["Configuring DCE" on page 325](#)
- ◆ ["Configuring SNMP" on page 347](#)



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 5.0 or above, Netscape 6.2 or above, or Mozilla Firefox 2.0.0.0 or above).



---

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

---

---

## CONNECTING TO THE WEB INTERFACE

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

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See ["Setting an IPv4 Address."](#))
2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See ["Setting Passwords."](#))
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 Edge Port) to improve the switch's response time to management commands issued through the web interface. See ["Defining STP Interface Settings."](#)

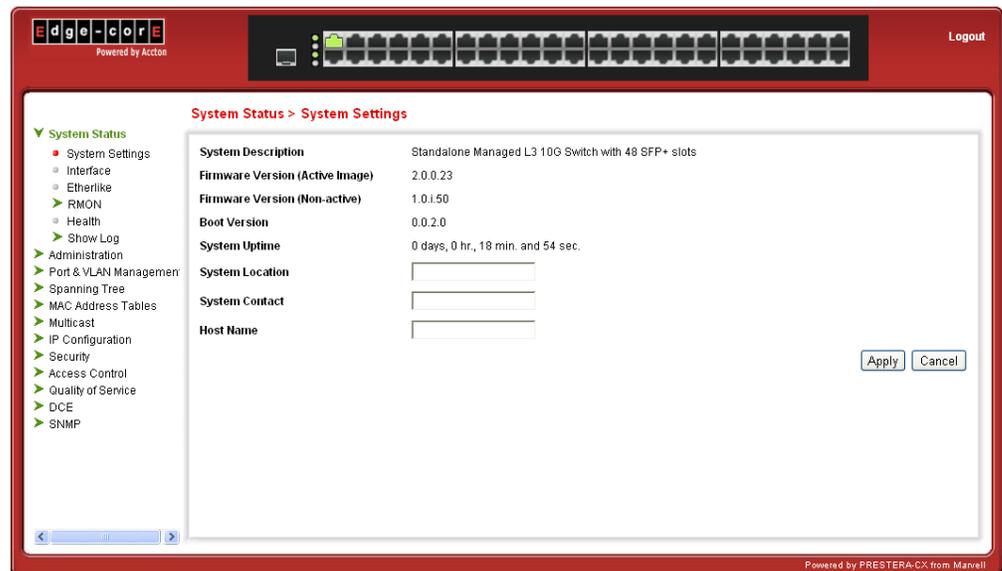
---

## NAVIGATING THE WEB BROWSER INTERFACE

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

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

**Figure 1: Home Page**



**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 3: 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."
Help	Links directly to web help.



**NOTE:** To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

**NOTE:** When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

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

**Figure 2: Front Panel Indicators**



**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 4: Switch Main Menu**

Menu	Description	Page
<b>System Status</b>		
System Settings	Provides basic system description, including contact information	68
Interface	Displays Ethernet interface statistics	69
Etherlike	Displays Etherlike MIB information	70
RMON	Displays RMON statistics	72
Health	Displays the switch fan status and temperature	83
Show Log	Displays system logs	83
<b>Administration</b>		
User Accounts	Manages access user names and passwords	87
Time Settings		
System Time	Configures the current time, time zone, DST, and time source	89
SNTP Settings	Configures SNTP server settings	92
SNTP Authentication	Configures authentication keys for SNTP servers	96
System Log		
Log Settings	Configures system log severity levels	98
Remote Log Servers	Configures remote Syslog server settings	99
File Management		
Upgrade/Backup Firmware	Uploads or backs up operation code files	103
Active Image	Sets the operation code to boot the switch	105
Save Configuration	Backs up and restores switch configuration files	106
Copy/Save Configuration	Saves or copies the switch running configuration to a file	108
DHCP Auto Configuration	Configures automatic configuration from a DHCP server	109
Reboot	Restarts the switch software	111
Diagnostics		
Optical Module Status	Displays information on installed transceivers	112
CPU Utilization	Monitors CPU resource utilization	113
LLDP		
Properties	Configures LLDP general parameters	115
Port Settings	Configures LLDP settings for port interfaces	117
LLDP MED Network Policy	Configures LLDP support for media devices	119
LLDP MED Port Settings	Configures LLDP media TLVs to be advertised on ports	120
Neighbors Information	Displays LLDP information from neighboring devices	124
LLDP Statistics	Displays LLDP statistics per port	129

**Table 4: Switch Main Menu (Continued)**

Menu	Description	Page
LLDP Overloading	Displays LLDP TLV statistics	130
LLDP MED Port Status Details	Displays LLDP MED	132
LLDP MED Port Status	Displays LLDP global information	136
sFlow		
sFlow Receivers Settings	Sets sFlow receiver IP addresses	138
sFlow Interface Settings	Configures sFlow receiver port settings	139
sFlow Statistics	Displays sFlow statistics	140
<b>Port &amp; VLAN Management</b>		
Port Settings	Configures global and per-port interface settings	141
Link Aggregation		
LAG Management	Displays LAG global and port settings	146
LAG Settings	Configures settings for specific LAGs	148
LACP	Configures Link Aggregation Control Protocol settings	149
VLAN Settings		
Create VLAN	Displays and configures VLANs	153
Interface Settings	Configures VLAN parameters for interfaces	154
Port to VLAN	Displays port membership of VLANs	157
Port VLAN Membership	Displays the VLAN membership of ports	158
Port and VLAN Mirroring	Configures mirroring for ports and VLANs	159
GVRP Settings	Configures Generic VLAN Registration Protocol settings	161
VLAN Groups		
MAC-Based Groups	Configures VLANs based on MAC addresses	163
Subnet-Based Groups	Configures VLANs based on IP subnets	164
Protocol-Based Groups	Configures VLANs based on traffic types	165
Mapping Groups to VLANs	Maps MAC- and protocol-based groups to VLANs	166
<b>Spanning Tree</b>		
STP Global Settings	Configures Spanning Tree global settings	170
STP Interface Settings	Configures Spanning Tree port settings	172
RSTP Interface Settings	Configures Rapid Spanning Tree port settings	175
MSTP Properties	Configures Multiple Spanning Tree global settings	178
VLAN to MST Instance	Maps VLANs to MST instances	179
MST Instance Settings	Configures and displays settings per MST instance	181
MSTP Interface Settings	Configures port MST settings for all instances	182
<b>MAC Address Tables</b>		
Static Addresses	Displays and configures static MAC addresses	187
Dynamic Address Settings	Configures the aging time for the MAC address table	189

**Table 4: Switch Main Menu** (Continued)

<b>Menu</b>	<b>Description</b>	<b>Page</b>
Dynamic Addresses	Displays dynamically-learned MAC addresses	189
<b>Multicast</b>		
Properties	Configures bridge multicast filtering settings	194
MAC Group Address	Displays and configures multicast VLAN or MAC-based groups	196
IP Multicast Group Address	Displays and configures IP-based multicast groups	198
IGMP Snooping	Enables IPv4 IGMP Snooping	200
MLD Snooping	Enables IPv6 MLD Snooping	203
IGMP/MLD IP Multicast Group	Displays multicast groups learned from IGMP/MLD snooping	207
Multicast Router Port	Displays and configures ports connected to multicast routers	208
Forward All	Configures ports to receive all multicast streams in a VLAN	209
Unregistered Multicast	Configures the forwarding of unknown multicast frames	211
<b>IP Configuration</b>		
Management and IP Interface		
IPv4 Interface	Configures IPv4 interfaces	214
IPv6 Global Configuration	Configures IPv6 global parameters	216
IPv6 Interfaces	Configures IPv6 interfaces	217
IPv6 Addresses	Assigns IPv6 addresses to interfaces	219
IPv6 Default Router List	Displays and configures IPv6 router addresses	220
IPv6 Tunnel	Configures ISATAP tunnel parameters	222
IPv6 Neighbors	Displays IPv6 neighbors on IPv6 interfaces	224
IPv6 Routes	Displays and configures IPv6 routes table	226
IPv4 Static Routes	Displays and configures IPv4 static routes	227
ARP	Configures Address Resolution Protocol settings	228
UDP Relay	Configures IPv4 UDP relaying	230
Domain Name System		
DNS Servers	Configures DNS servers	231
Host Mapping	Configures static mapping of DNS names to IP addresses	233
<b>Security</b>		
TACACS+	Configures TACACS+ authentication servers	238
RADIUS	Configures RADIUS authentication servers	241
Management Access Authentication	Defines management access authentication methods	244
Mgmt Access Method		
Access Profiles	Configures access profiles	246
Profile Rules	Configures access rules for profiles	249
Storm Control	Configures broadcast, multicast, unknown unicast storm control	252
Port Security	Configures MAC-based port security	254

**Table 4: Switch Main Menu** (Continued)

Menu	Description	Page
802.1X		
Properties	Configures 802.1X port access control global parameters	259
Port Authentication	Configures 802.1X parameters for ports	261
Host and Session Authentication	Configures 802.1X port mode	265
DHCP Snooping		
Properties	Configures DHCP Snooping general parameters	268
VLAN Settings	Enables DHCP Snooping on specified VLANs	269
Trusted Interfaces	Configures DHCP trusted interfaces	270
Binding Database	Adds static IP addresses to the DHCP Snooping database	271
ARP Inspection		
Properties	Configures global Dynamic ARP Inspection parameters	274
Trusted Interfaces	Defines trusted and untrusted ARP Inspection interfaces	275
ARP Inspection List	Creates static ARP binding lists	277
VLAN Settings	Enables ARP Inspection on VLANs	278
<b>Access Control</b>		
MAC-Based ACL	Configures MAC-based access control lists	283
MAC-Based ACE	Adds rules to a MAC-based ACL	284
IPv4 Based ACL	Configures IPv4-based access control lists	286
IPv4 Based ACE	Adds rules to an IPv4-based ACL	287
IPv6 Based ACL	Configures IPv6-based access control lists	291
IPv6 Based ACE	Adds rules to an IPv6-based ACL	292
ACL Binding	Binds ACLs to interfaces	295
<b>Quality of Service</b>		
General		
QoS Properties	Sets the QoS mode for the system and CoS priorities	301
Queue	Sets the queue method and WRR values	303
CoS/802.1p to Queue	Maps CoS values to egress queues	305
DSCP to Queue	Maps DSCP values to egress queues	306
Bandwidth	Limits the bandwidth of ingress interfaces	307
QoS Basic Mode		
Global Settings	Defines the switch trust configuration for QoS Basic Mode	309
QoS Advanced Mode		
Global Settings	Defines the switch trust configuration for QoS Advanced Mode	313
DSCP Remarking	Changes DSCP tags for incoming traffic switched between trusted QoS domains	315
Class Mapping	Configures class mapping to ACLs	316
Aggregate Policer	Applies QoS to one or more class maps	319

**Table 4: Switch Main Menu** (Continued)

<b>Menu</b>	<b>Description</b>	<b>Page</b>
Policy Table	Configures advanced QoS policies	<a href="#">320</a>
Policy Class Maps	Adds class maps to policies	<a href="#">321</a>
Policy Binding	Binds policy profiles to interfaces	<a href="#">323</a>
<b>DCE</b>		
FIP Snooping	Configures FCoE Initialization Protocol settings	<a href="#">325</a>
Cut-through	Configures cut-through forwarding on the switch	<a href="#">330</a>
QCN	Configures Quantized Congestion Notification settings	<a href="#">332</a>
PFC	Configures Priority-based Flow Control settings	<a href="#">335</a>
ETS	Configures Enhanced Transmission Selection settings	<a href="#">342</a>
DCBX	Configures Data Center Bridging Exchange protocol settings	<a href="#">343</a>
<b>SNMP</b>		
Engine ID	Defines the SNMPv3 Engine ID	<a href="#">350</a>
Views	Configures SNMPv3 views	<a href="#">351</a>
Users	Configures SNMPv3 users	<a href="#">353</a>
Groups	Configures SNMPv3 user groups	<a href="#">356</a>
Communities	Configures SNMPv1/2 communities	<a href="#">358</a>
Trap Settings	Configures SNMP trap recipients	<a href="#">360</a>
Notification Recipient SNMPv1,2	Configures recipients of SNMPv1/2 traps/notifications	<a href="#">361</a>
Notification Recipient SNMPv3	Configures recipients of SNMPv3 notifications	<a href="#">363</a>
Notification Filter	Configures SNMP notification filters	<a href="#">365</a>

This chapter describes how to view system information and configure various options on the switch.

It includes the following topics:

- ◆ [Displaying the System Settings](#)
- ◆ [Viewing Ethernet Interface](#)
- ◆ [Viewing Etherlike Statistics](#)
- ◆ [Managing RMON Statistics](#)
- ◆ [Monitoring the Health](#)
- ◆ [Viewing Memory Logs](#)

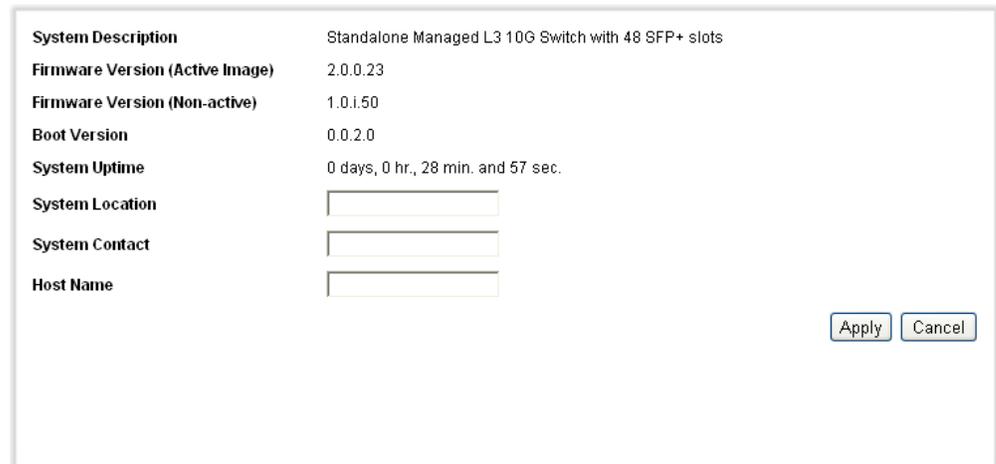
## DISPLAYING THE SYSTEM SETTINGS

The [System Settings Page](#) displays system information.

To view system information:

- ◆ Click **System Status** > **System Settings**. The [System Settings Page](#) is displayed.

**Figure 3: System Settings Page**



The screenshot shows a table of system information with the following data:

System Description	Standalone Managed L3 10G Switch with 48 SFP+ slots
Firmware Version (Active Image)	2.0.0.23
Firmware Version (Non-active)	1.0.1.50
Boot Version	0.0.2.0
System Uptime	0 days, 0 hr., 28 min. and 57 sec.
System Location	<input type="text"/>
System Contact	<input type="text"/>
Host Name	<input type="text"/>

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

The System Settings page displays the following information.

- ◆ **System Description**—A description of the system.
- ◆ **Firmware Version (Active Image)**—Firmware version number of the active image.
- ◆ **Firmware MD5 Checksum (Active Image)**—MD5 checksum of the active image.
- ◆ **Boot Version**—Boot version number.
- ◆ **System Uptime**—Time that has elapsed since the last reboot.
- ◆ **System Location**—Physical location of the switch. Click **Edit** to go the [System Settings Page](#) to enter this value.
- ◆ **System Contact**—Name of a contact person. Click **Edit** to go the [System Settings Page](#) to enter this value.
- ◆ **Host Name**—Name of the switch. Click **Edit** to go the [System Settings Page](#) to enter this value. By default, the switch hostname is composed of the word *switch* concatenated with the three least significant bytes of the switch MAC address (the six furthest right hexadecimal digits).

## VIEWING ETHERNET INTERFACE

The *Interface Page* displays traffic statistics per port. The refresh rate of the information can be selected.

This page is useful for analyzing the amount of traffic that is both sent and received and its dispersion (Unicast, Multicast, and Broadcast).

To display Ethernet statistics:

1. Click **System Status** > **Interface**. The *Interface Page* opens.

**Figure 4: Interface Page**

The screenshot shows the 'Interface Page' configuration and statistics. At the top, there are two radio buttons: 'Port' (selected) and 'LAG'. The 'Port' dropdown is set to 'te0/1' and the 'LAG' dropdown is set to '1'. Below this is the 'Refresh Rate' dropdown, which is set to 'No refresh'. The page is divided into two main sections: 'Receive Statistics' and 'Transmit Statistics'. Each section contains a table of statistics with values of 0.

Receive Statistics	
Total Bytes (Octets)	0
Unicast Packets	0
Multicast Packets	0
Broadcast Packets	0
Packets with Errors	0

Transmit Statistics	
Total Bytes (Octets)	0
Unicast Packets	0
Multicast Packets	0
Broadcast Packets	0
Packets with Errors	0

2. Enter the parameters.

- ◆ **Interface**—Select the type of interface and specific interface for which Ethernet statistics are to be displayed.
- ◆ **Refresh Rate**—Select the time period that passes before the interface Ethernet statistics are refreshed. The available options are:
  - *No Refresh*—Statistics are not refreshed.
  - *15 Sec*—Statistics are refreshed every 15 seconds.
  - *30 Sec*—Statistics are refreshed every 30 seconds.
  - *60 Sec*—Statistics are refreshed every 60 seconds.

The **Receive Statistics** area displays information about incoming packets.

- ◆ **Total Bytes (Octets)**—Octets received, including bad packets and FCS octets, but excluding framing bits.
- ◆ **Unicast Packets**—Good Unicast packets received.

- ◆ **Multicast Packets**—Good Multicast packets received.
- ◆ **Broadcast Packets**—Good Broadcast packets received.
- ◆ **Packets with Errors**—Packets with errors received.

The **Transmit Statistics** area displays information about outgoing packets.

- ◆ **Total Bytes (Octets)**—Octets transmitted, including bad packets and FCS octets, but excluding framing bits.
- ◆ **Unicast Packets**—Good Unicast packets transmitted.
- ◆ **Multicast Packets**—Good Multicast packets transmitted.
- ◆ **Broadcast Packets**—Good Broadcast packets transmitted.

#### TO CLEAR STATISTICS COUNTERS:

- ◆ Click **Clear Interface Counters** to clear counters for the interface displayed.
- ◆ Click **Clear All Interface Counters** to clear counters for all interfaces.

---

## VIEWING ETHERLIKE STATISTICS

The *Etherlike Page* displays statistics per port according to the Etherlike MIB standard definition. The refresh rate of the information can be selected. This page provides more detailed information regarding errors in the physical layer (Layer 1), which might disrupt traffic.

To view Etherlike Statistics:

1. Click **System Status > Etherlike**. The *Etherlike Page* opens.

**Figure 5: Etherlike Page**

The screenshot shows a web interface for monitoring system status. At the top, there are two dropdown menus: 'Port' set to 'te0/1' and 'LAG' set to '1'. Below these is a 'Refresh Rate' dropdown menu set to 'No refresh'. A horizontal line separates the configuration from the statistics. The statistics are listed in a table-like format:

Frame Check Sequence (FCS) Errors	0
Single Collision Frames	
Late Collisions	
Excessive Collisions	0
Oversize Packets	0
Internal MAC Receive Errors	0
Pause Frames Received	0
Pause Frames Transmitted	0

At the bottom of the statistics section, there are two buttons: 'Clear Interface Counters' and 'Clear All Interfaces Counters'.

2. Enter the parameters.

- ◆ **Interface**—Select the type of interface and specific interface for which Ethernet statistics are to be displayed.
- ◆ **Refresh Rate**—Select the amount of time that passes before the Etherlike statistics are refreshed.

The fields are displayed for the selected interface.

- ◆ **Frame Check Sequence (FCS) Errors**—Received frames that failed the CRC (cyclic redundancy checks).
- ◆ **Single Collision Frames**—Number of frames involved in a single collision, but were successfully transmitted.
- ◆ **Late Collisions**—Collisions that have been detected after the first 512 bits of data.
- ◆ **Excessive Collisions**—Number of transmissions due to excessive collisions.
- ◆ **Oversize Packets**—Packets greater than 1518 octets received.
- ◆ **Internal MAC Receive Errors**—Frames rejected because of receiver errors.
- ◆ **Received Pause Frames**—Received flow control pause frames.
- ◆ **Transmitted Pause Frames**—Flow control pause frames transmitted from the selected interface.

#### TO CLEAR STATISTICS COUNTERS:

- ◆ Click **Clear Interface Counters** to clear the selected interface's Etherlike statistics counters.
- ◆ Click **Clear All Interface Counters** to clear the Etherlike statistics counters of all interfaces.

---

## MANAGING RMON STATISTICS

RMON (Remote Networking Monitoring) enables an SNMP agent in the switch to proactively monitor traffic statistics over a given period and send traps to an SNMP manager. The local SNMP agent compares actual, real-time counters against predefined thresholds and generates alarms, without the need for polling by a central SNMP management platform. This is an effective mechanism for proactive management, provided that you have right thresholds set relative to your network's base line.

RMON decreases the traffic between the manager and the switch because the SNMP manager does not have to frequently poll the switch for information, and enables the manager to get timely status reports because the switch reports events as they occur.

With this feature, you can perform the following actions:

- ◆ View statistics (counter values) as they are currently, meaning since the last time they were cleared. You can also collect the values of these counters over a period of time, and then view the table of collected data, where each collected set is a single line of the *History* tab.
- ◆ Define interesting changes in counter values, such as "reached a certain number of late collisions" (defines the alarm), and then define what action to perform when this event occurs (log, trap, or log and trap).

### VIEWING RMON STATISTICS

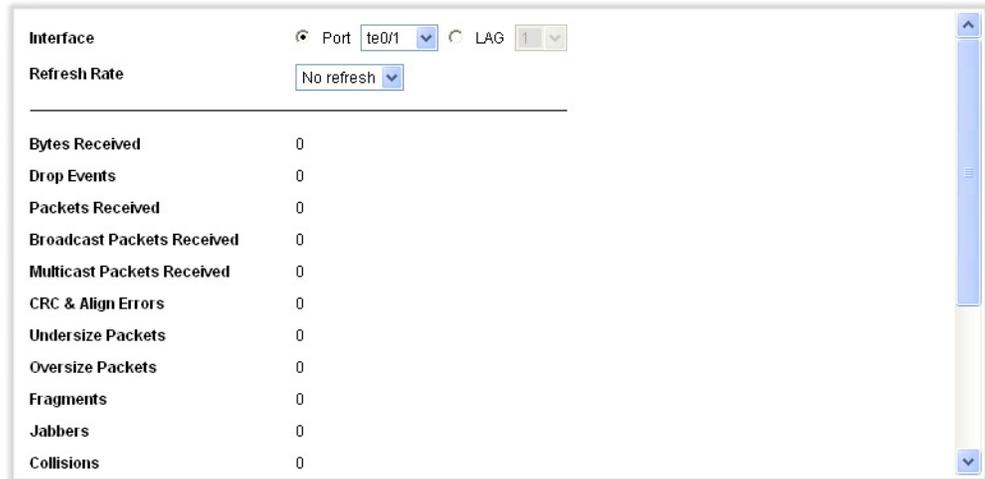
The [Statistics Page](#) displays detailed information regarding packet sizes and some information regarding physical layer errors. The information shown is according to the RMON standard. An oversized packet is defined as an Ethernet frame with the following criteria:

- ◆ Packet length is greater than MRU byte size
- ◆ Collision event has not been detected
- ◆ Late collision event has not been detected
- ◆ Rx error event has not been detected
- ◆ Packet has a valid CRC

To view the RMON statistics:

1. Click **System Status > RMON > Statistics**. The *Statistics Page* opens.

**Figure 6: Statistics Page**



2. Select the **Interface** for which Ethernet statistics are to be displayed.
3. Select the **Refresh Rate**, the time period that passes before the interface statistics are refreshed.

The following statistics are displayed for the selected interface.:

- ◆ **Bytes Received**—Number of octets received, including bad packets and FCS octets, but excluding framing bits.
- ◆ **Drop Events**—Number of packets that were dropped.
- ◆ **Packets Received**—Number of packets received, including bad packets, Multicast, and Broadcast packets.
- ◆ **Broadcast Packets Received**—Number of good Broadcast packets received. This number does not include Multicast packets.
- ◆ **Multicast Packets Received**—Number of good Multicast packets received.
- ◆ **CRC & Align Errors**—Number of CRC and Align errors that have occurred.
- ◆ **Undersize Packets**—Number of undersized packets (less than 64 octets) received.
- ◆ **Oversize Packets**—Number of oversized packets (over 1518 octets) received.
- ◆ **Fragments**—Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.

- ◆ **Jabbers**—Total number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria:
  - Packet data length is greater than MRU
  - Packet has an invalid CRC
  - Rx Error Event has not been detected
- ◆ **Collisions**—Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.
- ◆ **Frames of 64 Bytes**—Number of frames, containing 64 bytes that were received.
- ◆ **Frames of 65 to 127 Bytes**—Number of frames, containing 65-127 bytes that were received.
- ◆ **Frames of 128 to 255 Bytes**—Number of frames, containing 128-255 bytes that were received.
- ◆ **Frames of 256 to 511 Bytes**—Number of frames, containing 256-511 bytes that were received.
- ◆ **Frames of 512 to 1023 Bytes**—Number of frames, containing 512-1023 bytes that were received.
- ◆ **Frames greater than 1024 Bytes**—Number of frames, containing 1024-1518 bytes, and Jumbo Frames, that were received.

**To CLEAR STATISTICS COUNTERS:**

- ◆ Click **Clear Interface Counters** to clear the selected interface's RMON statistics counters.
- ◆ Click **Clear All Interface Counters** to clear the RMON statistics counters of all interfaces.

**CONFIGURING RMON HISTORY**

The [History Control Table Page](#) provides the ability to collect a log of statistics on a port.

You can configure the sampling frequency, amount of samples to store and the port from where to gather the data. After the data is sampled and stored, it is displayed in the [History Table Page](#) that can be viewed by clicking **History Table**.

To define RMON samples:

1. Click **System Status > RMON > History**. *History Control Table Page* opens.

**Figure 7: History Control Table Page**

The screenshot shows a web interface titled "History Control Table". It features a table with the following columns: History Entry No., Source Interface, Max No. of Samples to Keep, Sampling Interval, Owner, and Current Number of Samples. The table is currently empty, displaying the text "Table is empty". Below the table, there are three buttons: "Add...", "Edit...", and "Delete". At the bottom right of the interface, there is a button labeled "History Table".

This page displays the following fields:

- ◆ **History Entry No.**—Number of the history table entry.
- ◆ **Source Interface**—ID of the interface from which the history samples were captured.
- ◆ **Max. No. of Samples to Keep**—Maximum number of samples to be stored in this portion of the History table.
- ◆ **Sampling Interval**—Time period in seconds that samples were collected from the ports. The field range is 1-3600.
- ◆ **Owner**—RMON station or user that requested the RMON information. The field range is 0-20 characters.
- ◆ **Current Number of Samples**—RMON is allowed by standard to not grant all requested samples, but rather to limit the number of samples per request. Therefore, this field represents the sample number actually granted to the request that is equal or less than the requested value.

2. Click **Add**. *Add RMON History Page* opens.

Figure 8: Add RMON History Page

New History Entry	1
Source Interface	<input checked="" type="radio"/> Port <input type="text" value="te0/1"/> <input type="radio"/> LAG <input type="text" value="1"/>
Max No. of Samples to Keep *	<input type="text" value="50"/> (1 - 50, Default: 50)
Sampling Interval *	<input type="text" value="1800"/> sec. (1 - 3600, Default: 1800)
Owner	<input type="text"/>

3. Enter the parameters.
  - ◆ **New History Entry**—Displays the number of the new table entry.
  - ◆ **Source Interface**—Select the port/LAG from where the history samples are to be taken.
  - ◆ **Max No. of Samples to Keep**—Enter the number of samples to store.
  - ◆ **Sampling Interval**—Enter the time in seconds that samples were collected from the ports. The field range is 1-3600.
  - ◆ **Owner**—Enter the RMON station or user that requested the RMON information.
4. Click **Apply**. The entry is added to *History Control Table Page*, and the Running Configuration file is updated.

### VIEWING THE RMON HISTORY TABLE

The *History Table Page* displays interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample.

To view RMON history:

1. Click **System Status > RMON > History**. The *History Table Page* opens.
2. Click **History Table**. *History Table Page* opens.

Figure 9: History Table Page

The screenshot shows a web interface titled "History Table". At the top, there is a search bar with "History Entry No." and a "Query" button, and a "Clear Filter" button. Below this is a table with the following columns: History Entry No., Owner, Sample No., Drop Events, Bytes Received, Packets Received, Broadcast Packets, Multicast Packets, CRC Align Errors, Undersize Packets, Oversize Packets, Fragments, Jabbers, Collisions, and Utilization. The table body is empty, with the text "Table is empty" centered below the header. A "History Control Table" button is located at the bottom right of the table area.

3. From the **History Entry No.** list, select the entry number to display the samples associated with that history entry.

The fields are displayed for the selected sample.

- ◆ **Owner**—History table entry owner.
- ◆ **Sample No.**—Statistics were taken from this sample.
- ◆ **Drop Events**—Dropped packets due to lack of network resources during the sampling interval. This may not represent the exact number of dropped packets, but rather the number of times dropped packets were detected.
- ◆ **Bytes Received**—Octets received that including bad packets and FCS octets, but excluding framing bits.
- ◆ **Packets Received**—Packets received, including bad packets, Multicast, and Broadcast packets.
- ◆ **Broadcast Packets**—Good Broadcast packets received. This number does not include Multicast packets.
- ◆ **Multicast Packets**—Good Multicast packets received.
- ◆ **CRC Align Errors**—CRC and Align errors that have occurred.
- ◆ **Undersize Packets**—Undersized packets (less than 64 octets) received.
- ◆ **Oversize Packets**—Oversized packets (over 1518 octets) received.
- ◆ **Fragments**—Fragments (packets with less than 64 octets) received, excluding framing bits, but including FCS octets).
- ◆ **Jabbers**—Total number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that

had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number.

- ◆ **Collisions**—Collisions received.
- ◆ **Utilization**—Percentage of current interface traffic compared to maximum traffic that the interface can handle.

**DEFINING RMON  
EVENTS CONTROL**

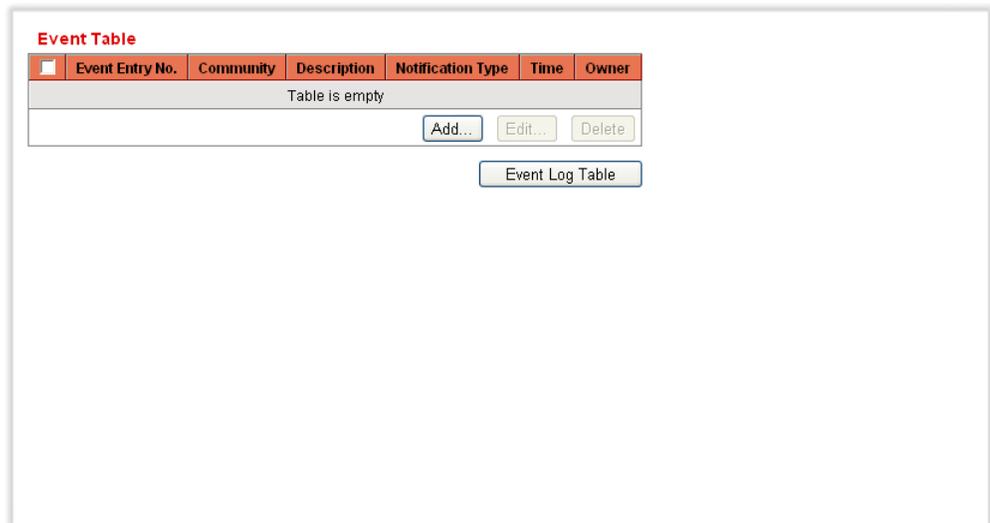
The [Events Page](#) provides the ability to configure events that are *actions* performed when an alarm is generated (alarms are defined in the [Alarms Page](#)). An event can be any combination of logs/traps.

If the action is includes logging then the events are logged in the [Event Log Table Page](#).

To view RMON events:

1. Click **System Status > RMON > Events**. The [Events Page](#) opens.

**Figure 10: Events Page**



This page displays previously-defined events.

2. Click **Add**. The [Add RMON Events Page](#) opens.

Figure 11: Add RMON Events Page

Event Entry	1
Community	<input type="text" value="Default Community"/>
Description	<input type="text" value="Default Description"/>
Notification Type	<input type="text" value="None"/>
Owner	<input type="text"/>

3. Enter the parameters.

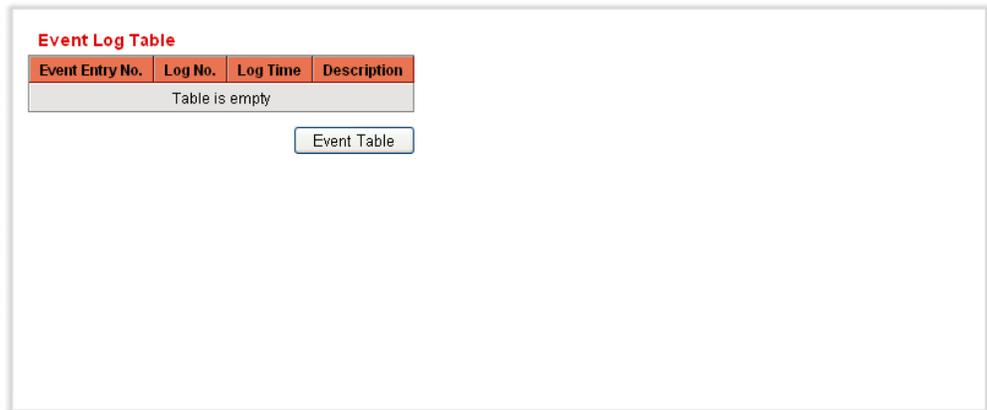
- ◆ **Event Entry**—Displays the event entry index number for the new entry.
  - ◆ **Community**—Enter the SNMP community string to be included when traps are sent (optional).
  - ◆ **Description**—Enter a name for the event. This name is used in the [Add RMON Alarm Page](#) to attach an alarm to an event.
  - ◆ **Notification Type**—Select the type of action that results from this event. Values are:
    - *None*—No action occurs when the alarm goes off.
    - *Log (Event Log Table)*—Add a log entry to the Event Log table when the alarm goes off.
    - *Trap (SNMP Manager and Syslog Server)*—Send a trap to the remote log server when the alarm goes off.
    - *Log and Trap*—Add a log entry to the Event Log table and send a trap to the remote log server when the alarm goes off.
  - ◆ **Owner**—Enter the device or user that defined the event.
4. Click **Apply**. The RMON event is added and the Running Configuration file is updated.

## VIEWING THE RMON EVENTS LOGS

The *Event Log Table Page* displays the log of events (actions) that occurred. An event can be logged when the type of the event is *Log* or *Log and Trap*. The action in the event is performed when the event is bound to an alarm (see the *Alarms Page*) and the conditions of the alarm have occurred.

1. Click **System Status > RMON > Events**. The *Events Page* opens.
2. Click **Event Log Table**. The *Event Log Table Page* opens.

**Figure 12: Event Log Table Page**



This page displays the following fields:

- ◆ **Event**—Events log entry number.
- ◆ **Log No.**—Log number.
- ◆ **Log Time**—Time that the log entry was entered.
- ◆ **Description**—Log entry description.

## DEFINING RMON ALARMS

RMON alarms provide a mechanism for setting thresholds and sampling intervals to generate exception events on any counter or any other SNMP object counter maintained by the agent. Both the rising and falling thresholds must be configured in the alarm. After a rising threshold is crossed, another rising event is not generated until the companion falling threshold is crossed. After a falling alarm is issued, the next alarm is issued when a rising threshold is crossed.

RMON alarms provide a mechanism for setting thresholds and sampling intervals. Exception events can be generated on remote log servers maintained by the agent. Both the rising and falling thresholds must be configured in the alarm. After a rising threshold is crossed, another rising event is not generated until the companion falling threshold is crossed. After a falling alarm is issued, the next alarm is issued when the rising threshold is crossed.

One or more alarms are bound to an event. The event indicates the action to be taken when the alarm occurs.

The *Alarms Page* provides the ability to configure alarms and to bind them with events. Alarm counters can be monitored by either absolute values or changes (delta) in the counter values.

To enter RMON alarms (if at least one RMON event has been defined):

1. Click **System Status** > **RMON** > **Alarms**. The *Alarms Page* opens.

**Figure 13: Alarms Page**

Alarm Entry No.	Interface	Counter Name	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Startup Alarm	Interval (sec.)	Owner
Table is empty											
											Add...
											Edit...
											Delete
											Back
											Next

2. Click **Add**. The *Add RMON Alarm Page* opens.

**Figure 14: Add RMON Alarm Page**

Alarm Entry: 1

Interface:  Port   LAG

Counter Name:

Sample Type:

Rising Threshold:  (0 - 2147483647, Default: 100)

Rising Event:

Falling Threshold:  (0 - 2147483647, Default: 20)

Falling Event:

Startup Alarm:

Interval:  sec. (1 - 2147483647, Default: 100)

Owner:

3. Enter the parameters.

◆ **Alarm Entry**—Displays the alarm entry number.

- ◆ **Interface**—Select the port/LAG for which RMON statistics are displayed.
  - ◆ **Counter Name**—Select the MIB variable that indicates the type of occurrence measured.
  - ◆ **Sample Type**—Select the sampling method to generate an alarm. The options are:
    - *Delta*—Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold. If the threshold was passed, an alarm is generated.
    - *Absolute*—If the threshold is passed, an alarm is generated.
  - ◆ **Rising Threshold**—Enter the rising counter value that triggers the rising threshold alarm.
  - ◆ **Rising Event**—Select an event, from those that you defined in the Events table, to be performed when a rising event is triggered. Events are created in the Events page.
  - ◆ **Falling Threshold**—Enter the falling counter value that triggers the falling threshold alarm.
  - ◆ **Falling Event**—Selects an event, from those defined in the Events table, to be performed when a falling event is triggered.
  - ◆ **Startup Alarm**—Select the first event from which to start generation of alarms. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
    - *Rising Alarm*—A rising counter value triggers the rising threshold alarm.
    - *Falling Alarm*—A falling counter value triggers the falling threshold alarm.
    - *Rising and Falling*—Both a rising and falling counter values trigger the alarm.
  - ◆ **Interval**—Enter the alarm interval time in seconds.
  - ◆ **Owner**—Enter the name of the user or network management system that receives the alarm.
4. Click **Apply**. The RMON alarm is added and the Running Configuration file is updated.

---

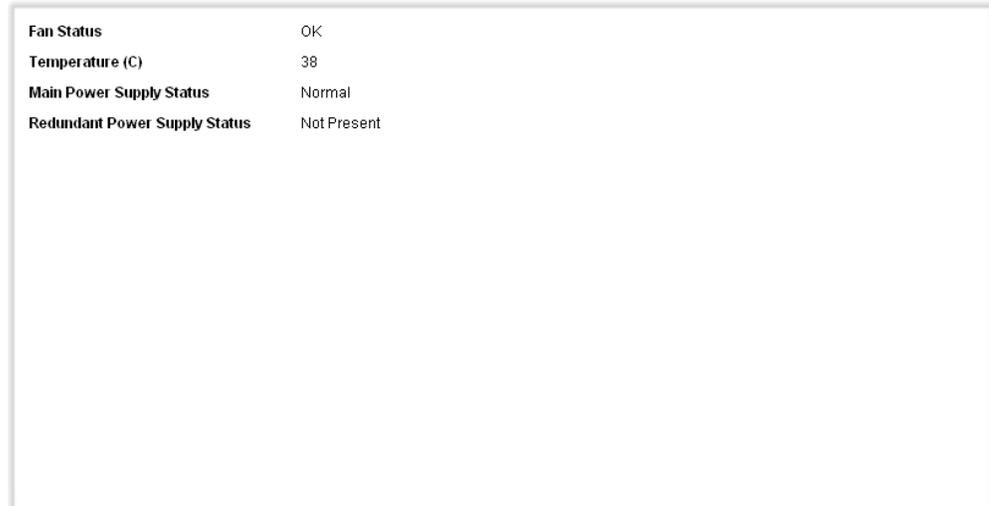
## MONITORING THE HEALTH

The *Health Page* displays the switch fan status and temperature.

To view the switch health parameters:

- ◆ Click **System Status** > **Health**. The *Health Page* opens.

**Figure 15: Health Page**



Fan Status	OK
Temperature (C)	38
Main Power Supply Status	Normal
Redundant Power Supply Status	Not Present

The Health page displays the following fields:

- ◆ **Fan Status**—Fan status.
- ◆ **Temperature**—Switch temperature.
- ◆ **Main Power Supply**—Status of main power supply.
- ◆ **Redundant Power Supply Status**—Status of redundant power supply.

---

## VIEWING MEMORY LOGS

The switch can write to the following logs:

- ◆ Log in RAM (cleared during reboot).
- ◆ Log in Flash memory (cleared only upon user command).

You can configure the messages that are written to each log by severity, and a message can go to more than one log, including logs that reside on external SYSLOG servers.

**RAM MEMORY** The *RAM Memory Page* displays all messages, in chronological order, that were saved in RAM (cache).

To view log entries:

1. Click **System Status > Show Log > RAM Memory**. The *RAM Memory Page* opens.

**Figure 16: RAM Memory Page**

Log Index	Log Time	Severity	Description
2147483580	2010-Jan-01 05:50:16	Informational	%AAA-I-CONNECT: New http connection for user admin, source 192.168.1.9 destination 192.168.1.1 ACCEPTED
2147483581	2010-Jan-01 05:42:26	Informational	%AAA-I-DISCONNECT: http connection for user admin, source 192.168.1.9 destination 192.168.1.1 TERMINATED
2147483582	2010-Jan-01 05:41:14	Informational	%AAA-I-DISCONNECT: User CLI session for user admin over console, source 0.0.0.0 destination 0.0.0.0 TERMINATED. The Telnet/SSH session may still be connected.
2147483583	2010-Jan-01 05:31:55	Informational	%AAA-I-CONNECT: New http connection for user admin, source 192.168.1.9 destination 192.168.1.1 ACCEPTED
2147483584	2010-Jan-01 05:28:57	Informational	%AAA-I-CONNECT: User CLI session for user admin over console, source 0.0.0.0 destination 0.0.0.0 ACCEPTED
2147483585	2010-Jan-01 05:27:46	Informational	%INIT-I-Startup: Warm Startup
2147483586	2010-Jan-01 05:27:15	Warning	%STP-VV-PORTSTATUS: te0/3: STP status Forwarding
2147483587	2010-Jan-01 05:26:45	Informational	%LINK-I-Up: Vlan 1
2147483588	2010-Jan-01 05:26:45	Informational	%LINK-I-Up: te0/3
2147483589	2010-Jan-01 05:26:44	Warning	%LINK-W-Down: te0/48
2147483590	2010-Jan-01 05:26:43	Warning	%LINK-W-Down: te0/47
2147483591	2010-Jan-01 05:26:41	Warning	%LINK-W-Down: te0/46
2147483592	2010-Jan-01 05:26:40	Warning	%LINK-W-Down: te0/45
2147483593	2010-Jan-01 05:26:39	Warning	%LINK-W-Down: te0/44
2147483594	2010-Jan-01 05:26:37	Warning	%LINK-W-Down: te0/43
2147483595	2010-Jan-01 05:26:36	Warning	%LINK-W-Down: te0/42
2147483596	2010-Jan-01 05:26:35	Note	%SYSLOG-N-LOGGING: Logging started.
2147483597	2010-Jan-01 05:26:35	Warning	%LINK-W-Down: te0/41
2147483598	2010-Jan-01 05:26:33	Warning	%LINK-W-Down: te0/40
2147483599	2010-Jan-01 05:26:32	Warning	%LINK-W-Down: te0/39
2147483600	2010-Jan-01 05:26:31	Warning	%LINK-W-Down: te0/38
2147483601	2010-Jan-01 05:26:29	Warning	%LINK-W-Down: te0/37
2147483602	2010-Jan-01 05:26:28	Warning	%LINK-W-Down: te0/36
2147483603	2010-Jan-01 05:26:27	Warning	%LINK-W-Down: te0/35
2147483604	2010-Jan-01 05:26:26	Warning	%LINK-W-Down: te0/34

This page displays the following fields:

- ◆ **Log Index**—Log entry number.
- ◆ **Log Time**—Time when message was generated.
- ◆ **Severity**—Event severity.
- ◆ **Description**—Message text describing the event.

2. To clear the log messages, click **Clear Logs**. The messages are cleared.

**FLASH MEMORY** The *Flash Memory Page* displays the messages that were stored in Flash memory, in chronological order. Flash logs remain when the switch is rebooted. You can clear the logs manually.

To view the Flash logs:

1. Click **System Status > View Log > Flash Memory**. The *Flash Memory Page* opens.

Figure 17: Flash Memory Page

Flash Memory Log Table			
Log Index	Log Time	Severity	Description
2147479817	2010-Jan-01 20:48:08	Alert	%TFTP-A-TftpRx:ERROR: An error message was received: 0 <User asked to overwrite an existing file! Access denied!>
2147479996	2010-Jan-01 20:45:35	Alert	%TFTP-A-TftpRx:ERROR: An error message was received: 0 <User asked to overwrite an existing file! Access denied!>
2147480175	2010-Jan-01 20:45:15	Alert	%TFTP-A-TftpRx:ERROR: An error message was received: 0 <User asked to overwrite an existing file! Access denied!>
2147480315	2010-Jan-01 05:45:40	Alert	%TFTP-A-TftpTx:ERROR: An error message was sent: 0 <Closed by application>
2147480455	2010-Jan-01 05:33:08	Alert	%TFTP-A-TftpTx:ERROR: An error message was sent: 0 <Closed by application>
2147480595	2010-Jan-01 06:21:46	Alert	%TFTP-A-TftpTx:ERROR: An error message was sent: 0 <Closed by application>
2147480735	2010-Jan-01 16:24:46	Alert	%TFTP-A-TftpTx:ERROR: An error message was sent: 0 <Closed by application>
2147480875	2011-Jan-17 21:35:26	Alert	%TFTP-A-TftpTx:ERROR: An error message was sent: 0 <Closed by application>
2147481015	2010-Jan-01 06:09:21	Alert	%TFTP-A-TftpTx:ERROR: An error message was sent: 0 <Closed by application>
2147481155	2010-Jan-01 05:56:25	Alert	%TFTP-A-TftpTx:ERROR: An error message was sent: 0 <Closed by application>
2147481295	2010-Jan-01 05:50:27	Alert	%TFTP-A-TftpTx:ERROR: An error message was sent: 0 <Closed by application>
2147481435	2010-Jan-01 05:48:46	Alert	%TFTP-A-TftpTx:ERROR: An error message was sent: 0 <Closed by application>
2147481614	2010-Jan-01 05:48:35	Alert	%TFTP-A-TftpRx:ERROR: An error message was received: 0 <User asked to overwrite an existing file! Access denied!>
2147481754	2010-Jan-01 05:47:58	Alert	%TFTP-A-TftpTx:ERROR: An error message was sent: 0 <Closed by application>
2147481933	2010-Jan-01 05:47:37	Alert	%TFTP-A-TftpRx:ERROR: An error message was received: 0 <User asked to overwrite an existing file! Access denied!>
2147482112	2010-Jan-01 05:47:01	Alert	%TFTP-A-TftpRx:ERROR: An error message was received: 0 <User asked to overwrite an existing file! Access denied!>
2147482291	2010-Jan-01 05:46:44	Alert	%TFTP-A-TftpRx:ERROR: An error message was received: 0 <User asked to overwrite an existing file! Access denied!>
2147482470	2010-Jan-01 12:16:52	Alert	%TFTP-A-TftpRx:ERROR: An error message was received: 0 <User asked to overwrite an existing file! Access denied!>
2147482649	2010-Jan-01 12:16:13	Alert	%TFTP-A-TftpRx:ERROR: An error message was received: 0 <User asked to overwrite an existing file! Access denied!>
2147482828	2010-Jan-01 12:15:56	Alert	%TFTP-A-TftpRx:ERROR: An error message was received: 0 <User asked to overwrite an existing file! Access denied!>

This page displays the following fields:

- ◆ **Log Index**—Log entry number.
  - ◆ **Log Time**—Time when message was generated.
  - ◆ **Severity**—Event severity.
  - ◆ **Description**—Message text describing the event.
2. To clear the messages, click **Clear Logs**. The messages are cleared.



This chapter contains the following topics:

- ◆ [Defining Users](#)
- ◆ [Managing the Time Settings](#)
- ◆ [Managing System Logs](#)
- ◆ [Managing System Files](#)
- ◆ [Rebooting the Switch](#)
- ◆ [Managing Device Diagnostics](#)
- ◆ [Configuring LLDP](#)
- ◆ [Configuring sFlow](#)

---

## DEFINING USERS

A user, in this context, is a system administrator or superuser, who manages the switch.

The default username is **admin** and the default password is empty.

The [User Accounts Page](#) enables entering additional users that are permitted to manage the switch or changing the passwords of existing users.



**NOTE:** It is not permitted to delete all users. If all users are selected, the **Delete** button is disabled.

---

To add a new user:

1. Click **Administration > User Accounts**. The [User Accounts Page](#) displays.

**Figure 18: User Accounts Page**



This page displays the users defined in the system.

- Click **Add** to add a new user or click **Edit** to modify a user. The [Add/Edit User Account Page](#) displays.

**Figure 19: Add/Edit User Account Page**

The screenshot shows a form for adding or editing a user account. It has four input fields: "User Name" (text input), "Access Level" (dropdown menu with "1" selected), "Password" (text input), and "Confirm Password" (text input). An "Apply" button is located at the bottom right of the form.

User Name \*

Access Level \*  ▼

Password

Confirm Password

- Enter the parameters.
  - ◆ **User Name**—Enter a new username between 0 and 20 characters. UTF-8 characters are not permitted.
  - ◆ **Access Level**—Select an access level.
  - ◆ **Password**—Enter a password (UTF-8 characters are not permitted).
  - ◆ **Confirm Password**—Enter the password again.
- Click **Apply**. The user is added, and the Running Configuration file is updated with the settings..

---

## MANAGING THE TIME SETTINGS

Network time synchronization is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events occur. Time also provides the only frame of reference between all devices on the network. Without synchronized time, accurately correlating log files between these devices is difficult, even impossible.

A few of the specific reasons include, tracking security breaches, network usage. Problems affecting a large number of components can be nearly impossible to track if timestamps in logs are inaccurate.

Time also reduces confusion in shared file systems, as it is important for the modification times to be consistent, regardless of the machine on which the filesystems reside.

For these reasons, it is important that the time configured on the all devices on the network be accurate.



**NOTE:** The switch supports Simple Network Time Protocol (SNTP) and when enabled, the switch dynamically synchronizes the switch time with the SNTP server time. The switch operates only as an SNTP client, and cannot provide time services to other devices.

---

This section describes the options for configuring system time, time zone, and Daylight Savings Time (DST). It includes the following topics:

- ◆ [System Time Options](#)
- ◆ [Configuring System Time](#)
- ◆ [Adding an SNTP Server](#)
- ◆ [Defining SNTP Authentication](#)

**SYSTEM TIME OPTIONS** System time can be set manually by the user or dynamically by using an SNTP server. If an SNTP server is chosen, the manual time settings are overwritten when communications with the server is established.

As part of the boot process, the switch always configures the time, time-zone, and DST in some way, either from DHCP, from SNTP, from values set manually, or if all else fails from the factory defaults.

### TIME

The following methods are available for obtaining or setting the time on the switch:

- ◆ SNTP that ensures accurate network time synchronization of the switch up to the millisecond by using an SNTP server for the clock source.



---

**NOTE:** Without synchronized time, accurately correlating log files between devices is difficult, even impossible. We recommend that you use SNTP for the clock source.

---

- ◆ Manual entry of the system time by the user.
- ◆ Entry of the time by the computer that accesses the switch through the device configuration utility. If this feature is enabled, the switch uses the system time from the configuring computer, unless the time has been configured on the switch manually by the user or SNTP server support is not available or enabled.



---

**NOTE:** Receiving the time from the computer configuring the switch should be the last resort, such as after a power outage and no other time source is available.

---

#### TIME ZONE AND DAYLIGHT SAVINGS TIME (DST)

The Time Zone and DST can be set on the switch in the following ways:

- ◆ Dynamic configuration of the switch through a DHCP server, where:
  - Dynamic DST, when enabled and available, always takes precedence over the manual configuration of DST.
  - If the server supplying the source parameters fails or dynamic configuration is disabled by the user, the manual settings are used.
  - Dynamic configuration of the time zone and DST continues after the IP address lease time has expired.
- ◆ Manual configuration of the time zone and DST by the user, where the time zone and DST set manually becomes the Operational time zone and DST, only if the dynamic configuration of the time zone and DST is disabled or fails.

#### CONFIGURING SYSTEM TIME

Use the [System Time Page](#) to configure the current time, time zone, DST, and the time source. If the time is determined manually, enter the manual time here.

The switch does not have an internal clock that updates this value. If the system time is set manually and the switch is rebooted, the manual time settings must be reentered.

To define system time:

1. Click **Administration > Time Settings > System Time**. The [System Time Page](#) is displayed.

Figure 20: System Time Page

2. Enter the parameters.

- ◆ **Clock Source**—Select the source used to set the system clock.
  - **Use Local Settings**—The system time is either entered manually or taken from the configuring computer. If this radio button is selected, enter the Local Settings.
  - **Use SNTP Server**—The system time is obtained from an SNTP server. Also, add an SNTP server and enable SNTP broadcast mode by using the [SNTP Settings Page](#). Enforce authentication of the SNTP sessions by using the [SNTP Authentication Page](#).
- ◆ **Local Settings**—The local time is used when there is no alternate source of time, such as an SNTP server:
  - **Date**—Enter the system date.
  - **Local Time**—Enter the system time.
  - **Time Zone Offset**—Select the difference in hours between *Greenwich Mean Time* (GMT) and the local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT – 5.
  - **Daylight Savings**—Select Daylight Savings to enable DST.
  - **Time Set Offset**—Enter the number of minutes that Daylight Savings Time causes clocks to adjust.
  - **Daylight Savings Type**—Select how DST is defined:
    - **USA**—According to the dates used in the USA

- **European**—According to the dates used by the European Union and other countries that use this standard.
  - **By Dates**—Manually, typically for a country other than the USA or a European country. Enter the following parameters:
    - **From**—Day and time that DST starts.
    - **To**—Day and time that DST ends.
    - **Recurring**—DST occurs on the same date every year. Enter the following parameters:
      - **From**—Date when DST begins each year.
        - **Day**—Day of the week on which DST begins every year.
        - **Week**—Week within the month from which DST begins every year.
        - **Month**—Month of the year in which DST begins every year.
        - **Time**—The time at which DST begins every year.
      - **To**—Date when DST ends each year. For example, DST ends locally every fourth Friday in October at 5:00 am. The parameters are:
        - **Day**—Day of the week on which DST ends every year.
        - **Week**—Week within the month from which DST ends every year.
        - **Month**—Month of the year in which DST ends every year.
        - **Time**—The time at which DST ends every year.
3. Click **Apply**. The system time values are defined, and the Running Configuration file is updated with the settings..

The time settings are displayed in the *Actual Time Details* block.

#### ADDING AN SNTP SERVER

A switch can be configured to synchronize its system clock with an SNTP server by using the [SNTP Settings Page](#).



**NOTE:** If specifying an SNTP server by name, this feature requires that the DNS servers be configured on the switch (see ["Defining DNS Servers" on page 231](#)) to work properly.

---

The switch supports the following modes:

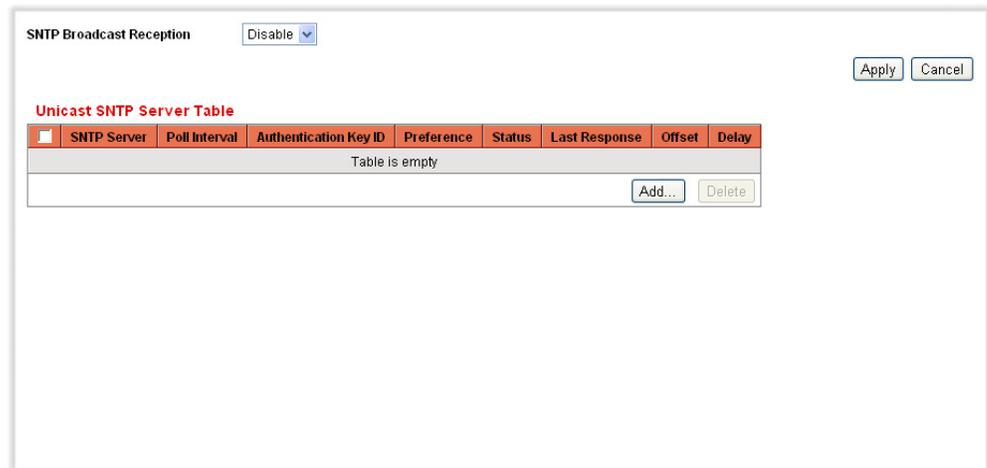
- ◆ **Broadcast**—The SNTP server broadcasts the time, and the switch listens to these broadcasts. When the switch is in this mode, there is no need to define a Unicast SNTP server.
- ◆ **Unicast SNTP Server Mode**—The switch sends Unicast queries to the list of manually-configured SNTP servers, and waits for a response.

The switch supports having both modes active at the same time, choosing the best source of the parameters according to the closest stratum (distance from the reference clock).

To add an SNTP server:

1. Click **Administration > Time Settings > SNTP Settings**. The [SNTP Settings Page](#) is displayed.

**Figure 21: SNTP Settings Page**



2. (Optional) Enable **SNTP Broadcast Reception** to listen to SNTP Broadcast synchronization packets for system time information. If this option is selected, the system does not display the SNTP server from which the time parameters are received.

This page displays the following information for each Unicast SNTP server:

- ◆ **SNTP Server**—SNTP server IP address. Up to eight SNTP servers can be defined. The preferred server, or hostname, is chosen according to its stratum level.
- ◆ **Poll Interval**—Interval (in seconds) at which the SNTP server is polled for system time information. The poll interval is 1024 seconds.
- ◆ **Authentication Key ID**—Key Identification used to communicate between the SNTP server and switch.
- ◆ **Preference**—Priority of use for the SNTP server.

- *Primary*—Server with the lowest stratum level. Stratum level is the distance from the reference clock. Time information is taken from this server.
  - *Secondary*—Server with the next lowest stratum level after the primary server. Serves as a backup to the primary server.
  - *In progress*—SNTP server that is currently sending or receiving SNTP information.
- ◆ **Status**—SNTP server status. The possible options are:
- *Up*—SNTP server is currently operating normally.
  - *Down*—SNTP server is currently not available.
  - *Unknown*—SNTP server is currently being searched for by the switch.
- ◆ **Last Response**—Date and time of the last time a response was received from this SNTP server.
- ◆ **Offset**—The estimated offset of the server's clock relative to the local clock, in milliseconds. The host determines the value of this offset using the algorithm described in RFC 2030.
- ◆ **Delay**—The estimated round-trip delay of the server's clock relative to the local clock over the network path between them, in milliseconds. The host determines the value of this delay using the algorithm described in RFC 2030.

3. Click **Add** to display the [Add SNTP Server Page](#).

**Figure 22: Add SNTP Server Page**

The screenshot shows a configuration page for adding an SNTP server. It features several sections with radio buttons, dropdown menus, and text input fields. The 'Server Definition' section has radio buttons for 'By IP address' (selected) and 'By name'. The 'IP Version' section has radio buttons for 'Version 6' (selected) and 'Version 4'. The 'IPv6 Address Type' section has radio buttons for 'Link Local' (selected) and 'Global'. The 'Link Local Interface' section has a dropdown menu with 'None' selected. The 'SNTP Server IP Address' section has a text input field. The 'SNTP Server' section has a dropdown menu with 'time-a.timefreq.bldrdoc.gov' selected and a text input field. The 'Poll Interval' section has a dropdown menu with 'Enabled' selected. The 'Authentication' section has a dropdown menu with 'Disabled' selected. The 'Authentication Key ID' section has a dropdown menu. An 'Apply' button is located in the bottom right corner.

4. Enter the following parameters:

- ◆ **Server Definition**—Select if the SNTP server is going to be identified by its IP address or if you are going to choose a well-known SNTP server by name from the list.



**NOTE:** To specify a well-known SNTP server, the switch must be connected to the Internet and configured with a DNS server or configured so that a DNS server is identified by using DHCP. (See "[Defining DNS Servers](#)" on page 231.)

- ◆ **IP Version**—Select the version of the IP address: **Version 6** or **Version 4**.
  - ◆ **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are
    - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
    - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
  - ◆ **Link Local Interface**—Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
  - ◆ **SNTP Server IP Address**—Enter the SNTP server IP address. The format depends on which address type was selected.
  - ◆ **SNTP Server**—Select the name of the SNTP server from a list of well-known SNTP servers. If **other** is chosen, enter the hostname of SNTP server in the adjacent field.
  - ◆ **Poll Interval**—Select to enable polling of the SNTP server for system time information. All SNTP servers that are registered for polling are polled, and the clock is selected from the server with the lowest stratum level (distance from the reference clock.) that is reachable. The server with the lowest stratum is considered to be the primary server. The server with the next lowest stratum is a secondary server, and so forth. If the primary server is down, the switch polls all servers with the polling setting enabled, and selects a new primary server with the lowest stratum.
  - ◆ **Authentication**—Select the check box to enable authentication.
  - ◆ **Authentication Key ID**—If authentication is enabled, select the value of the key ID. (Create the authentication keys using the [SNTP Authentication Page](#).)
5. Click **Apply**. The SNTP server is added, and the Running Configuration file is updated with the settings.

## DEFINING SNTP AUTHENTICATION

The *SNTP Authentication Page* enables configuration of the authentication keys that are used when communicating with an SNTP server that requires authentication.

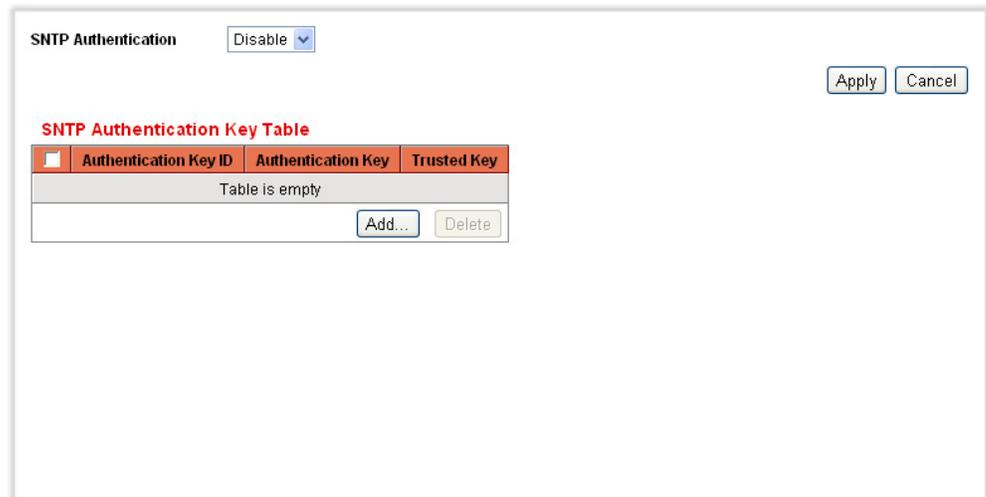
After a key has been created, it must be bound to one or more relevant SNTP servers to be authenticated. This authentication key can also be used for authentication when receiving Broadcast synchronization.

SNTP sessions might require authentication. A Unicast SNTP server that requires authentication must be bounded with an authentication key when it is added by using the [Add SNTP Server Page](#).

To define SNTP authentication:

1. Click **Administration** > **Time Settings** > **SNTP Authentication**. The *SNTP Authentication Page* is displayed.

**Figure 23: SNTP Authentication Page**



2. Enable **SNTP Authentication** to require authentication of an SNTP session between the switch and an SNTP server.
3. Click **Apply** to update the switch.
4. Click **Add**. The [Add SNTP Authentication Page](#) is displayed.

**Figure 24: Add SNMP Authentication Page**

The screenshot shows a configuration page for adding SNMP authentication. It contains three input fields and one button:

- Authentication Key ID \***: A text input field containing the value "(1 - 4294967295)".
- Authentication Key \***: An empty text input field.
- Trusted Key**: A dropdown menu currently set to "Enabled".
- Apply**: A button located at the bottom right of the form.

5. Enter the following parameters:

- ◆ **Authentication Key ID**—Enter the number used to identify this SNMP authentication key internally.
  - ◆ **Authentication Key**—Enter the key used for authentication (up to eight characters). The SNMP server must send this key for the switch to synchronize to it.
  - ◆ **Trusted Key**—Select the check box to allow the switch to receive broadcast synchronization information only from a SNMP server by using this authentication key.
6. Click **Apply**. The SNMP Authentication is defined, and the Running Configuration file is updated with the settings.

---

## MANAGING SYSTEM LOGS

This section describes the System Log feature, which enables the switch to keep several independent logs. Each log is a set of messages recording system events.

The switch generates the following local logs:

- ◆ Log written into a cyclical list of logged events in RAM and is erased when the switch reboots.
- ◆ Log written to a cyclical log-file saved to Flash memory and persists across reboots.

In addition, you can send messages to remote SYSLOG servers in the form of SNMP traps and SYSLOG messages.

This section contains the following sections:

- ◆ [Setting System Log Settings](#)

◆ [Setting Remote Logging Settings](#)

**SETTING SYSTEM LOG SETTINGS** You can enable or disable logging on the [Log Settings Page](#), and select whether to aggregate log messages.

You can select the events by severity level. Each log message has a severity level marked with the first letter of the severity level concatenated with a dash (-) on each side (except for *Emergency* that is indicated by the letter F). For example, the log message "%INIT-I-InitCompleted: ..." has a severity level of **I**, meaning *Informational*.

The event severity levels are listed from the highest severity to the lowest severity, as follows:

- ◆ *Emergency*—System is not usable.
- ◆ *Alert*—Action is needed.
- ◆ *Critical*—System is in a critical condition.
- ◆ *Error*—System is in error condition.
- ◆ *Warning*—System warning has occurred.
- ◆ *Notice*—System is functioning properly, but a system notice has occurred.
- ◆ *Informational*—Device information.
- ◆ *Debug*—Provides detailed information about an event.

You can select different severity levels for RAM and Flash logs. These logs are displayed in the [RAM Memory Page](#) and [Flash Memory Page](#), respectively.

Selecting a severity level to be stored in a log causes all of the higher severity events to be automatically stored in the log. Lower severity events are not stored in the log.

For example, if **Warning** is selected, all severity levels that are **Warning** and higher are stored in the log (*Emergency*, *Alert*, *Critical*, *Error*, and *Warning*). No events with severity level below **Warning** are stored (*Notice*, *Informational*, and *Debug*).

To set global log parameters:

1. Click **Administration > System Log > Log Settings**. The [Log Settings Page](#) is displayed.

Figure 25: Log Settings Page

RAM Memory Logging		Flash Memory Logging	
Emergency	<input checked="" type="checkbox"/>	Emergency	<input checked="" type="checkbox"/>
Alert	<input checked="" type="checkbox"/>	Alert	<input checked="" type="checkbox"/>
Critical	<input checked="" type="checkbox"/>	Critical	<input checked="" type="checkbox"/>
Error	<input checked="" type="checkbox"/>	Error	<input checked="" type="checkbox"/>
Warning	<input checked="" type="checkbox"/>	Warning	<input type="checkbox"/>
Notice	<input checked="" type="checkbox"/>	Notice	<input type="checkbox"/>
Informational	<input checked="" type="checkbox"/>	Informational	<input type="checkbox"/>
Debug	<input type="checkbox"/>	Debug	<input type="checkbox"/>

2. Enter the parameters.

- ◆ **Logging**—Select to enable message logging.
  - ◆ **RAM Memory Logging**—Select the severity levels of the messages to be logged to RAM.
  - ◆ **Flash Memory Logging**—Select the severity levels of the messages to be logged to Flash memory.
3. Click **Apply**. The Running Configuration file is updated with the settings.

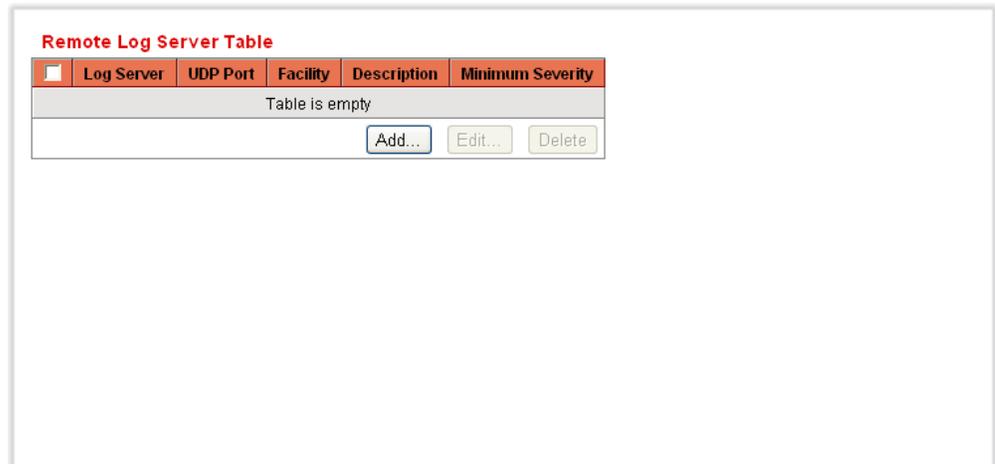
## SETTING REMOTE LOGGING SETTINGS

The [Remote Log Server Page](#) enables defining remote SYSLOG servers where log messages are sent (using the SYSLOG protocol). For each server, you can configure the severity of the messages that it receives.

To define SYSLOG servers:

1. Click **Administration** > **System Log** > **Remote Log Servers**. The [Remote Log Server Page](#) is displayed.

Figure 26: Remote Log Server Page



This page displays the list of remote log servers.

- Click **Add**. The [Add Remote Log Server Page](#) is displayed.

Figure 27: Add Remote Log Server Page

**Host Definition**  By IP address  By name

**IP Version**  Version 6  Version 4

**IPv6 Address Type**  Link Local  Global

**Link Local Interface**

**Log Server IP Address/Name \***

**UDP Port \***  (1 - 65535, Default: 514)

**Facility**

**Description**

**Minimum Severity**

- Enter the parameters.

- ◆ **Host Definition**—Select if the host is going to be identified by its IP address or by name.
- ◆ **IP Version**—Select the supported IP format.
- ◆ **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:
  - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local

network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.

- *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
  - ◆ **Link Local Interface**—Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
  - ◆ **Log Server IP Address**—Enter the IP address of the log server.
  - ◆ **UDP Port**—Enter the UDP port to which the log messages are sent.
  - ◆ **Facility**—Select a facility value from which system logs are sent to the remote server. Only one facility value can be assigned to a server. If a second facility code is assigned, the first facility value is overridden.
  - ◆ **Description**—Enter a server description.
  - ◆ **Minimum Severity**—Select the minimum level of system log messages to be sent to the server.
4. Click **Apply**. The [Add Remote Log Server Page](#) closes, the SYSLOG server is added, and the Running Configuration file is updated with the settings.

---

## MANAGING SYSTEM FILES

You can choose the firmware file from which the switch boots. You can also copy file types internally on the switch, or to or from an external device, such as a PC.

The methods of file transfer are:

- ◆ Internal copy
- ◆ HTTP that uses the facilities that the browser provides
- ◆ TFTP client, requiring a TFTP server

Configuration files on the switch are defined by their *type*, and contain the settings and parameter values for the device. When a configuration is referenced on the switch, it is referenced by its *configuration file type*, as opposed a file name that can be modified by the user. Content can be copied from one file type to another, but the names of the file types cannot be changed by the user. Other files on the device include firmware, boot code, and log files, and are referred to as *operational files*.

The configuration files are text files and can be edited by a user in a text editor, such as Notepad after they are copied to an external device, such as a PC.

### FILES AND FILE TYPES

The following types of configuration and operational files are found on the switch:

- ◆ **Running Configuration**—Parameters that are currently used by the switch to operate. It is the only file type that is modified by you when the parameter values are changed by using one of the configuration interfaces, and must be manually saved to be preserved.

If the switch is rebooted, the Running Configuration is lost. When the switch is rebooted, this file type is copied from the Startup Configuration stored in Flash to the Running Configuration stored in RAM.

To preserve any changes made to the switch, you must save the Running Configuration to the Startup Configuration, or another file type if you do not want the switch to reboot with this configuration. If you have saved the Running Configuration to the Startup Configuration, when the switch is rebooted, it recreates a Running Configuration that includes the changes you have made since the last time the Running Configuration was saved to the Startup Configuration.

- ◆ **Startup Configuration**—The parameter values that were saved by you by copying another configuration (usually the Running Configuration) to the Startup Configuration.
- ◆ The Startup Configuration is retained in Flash and is preserved any time the switch is rebooted. When it is rebooted, the Startup Configuration is copied to RAM and identified as the Running Configuration.
- ◆ **Backup Configuration**—A manual copy of the parameter definitions for protection against system shutdown or for the maintenance of a specific operating state. You can copy the Startup Configuration, or Running Configuration to a Backup Configuration file. The Backup Configuration exists in Flash and is preserved if the device is rebooted.
- ◆ **Firmware**—The program that controls the operations and functionality of the switch. More commonly referred to as the *image*.
- ◆ **Boot Code**—Controls the basic system startup and launches the firmware image.
- ◆ **Flash Log**—SYSLOG messages stored in Flash memory.

### FILE ACTIONS

The following actions can be performed to manage firmware and configuration files:

- ◆ Upgrade the firmware or boot code, as described in [Upgrading/Backing Up Firmware](#) section.
- ◆ View the firmware image currently in use or select the image to be used in the next reboot as described in the [Selecting the Active Image](#) section.

- ◆ Save configuration files on the switch to a location on another device as described in [Saving a Configuration](#).
- ◆ Copy one configuration file type onto another configuration file type as described in the [Copying/Saving Configuration Files](#) section.
- ◆ Automatically upload a configuration file from a TFTP server to the switch as described in the [Setting DHCP Auto Configuration](#) section.



**NOTE:** Unless the Running Configuration is manually copied to the Startup Configuration, Backup Configuration, or an external file, all changes made since the last time the file was saved are lost when the switch is rebooted. We recommend that you save the Running Configuration to the Startup Configuration before logging off to preserve any changes you made during this session.

A red X icon, displayed to the left of the Save application link, indicates that configuration changes have been made and have not yet been saved to the Startup Configuration file.

When you click **Save**, the *Copy/Save Configuration* Page is displayed. Save the Running Configuration file by copying it to the Startup Configuration file. After this save, the red X icon and the link to the Copy/Save Configuration Page are hidden.

This section describes how configuration and log files are managed.

It includes the following topics:

- ◆ [Upgrading/Backing Up Firmware](#)
- ◆ [Selecting the Active Image](#)
- ◆ [Saving a Configuration](#)
- ◆ [Copying/Saving Configuration Files](#)
- ◆ [Setting DHCP Auto Configuration](#)

## UPGRADING/BACKING UP FIRMWARE

The [Upgrading/Backing Up Firmware](#) process can be used to:

- ◆ Upgrade or backup the firmware image
- ◆ Upgrade or backup the boot code

The following methods for transferring files are supported:

- ◆ HTTP that uses the facilities provided by the browser
- ◆ TFTP that requires a TFTP server

There are two firmware images, **Image1** and **Image2**, stored on the switch. One of the images is identified as the *active image* and other image is identified as the *inactive image*.

When you upgrade the firmware, the new image is always replaces the image identified as the inactive image.

After uploading new firmware on the switch, the switch continues to boot by using the active image (the old version) until you change the status of the new image to be the active image by using the procedure in [Selecting the Active Image](#). Then boot the switch by using the process described in the [Rebooting the Switch](#) section.

To download or backup a system file:

1. Click **Administration > File Management > Upgrade/Backup Firmware**. The [Upgrade/Backup Firmware Page](#) is displayed.

**Figure 28: Upgrade/Backup Firmware Page**

The screenshot shows a configuration form for upgrading or backing up firmware. The form includes the following fields and options:

- Transfer Method:** Radio buttons for  via TFTP and  via HTTP.
- Save Action:** Radio buttons for  Upgrade and  Backup.
- File Type:** A dropdown menu currently set to "Firmware Image".
- Host Definition:** Radio buttons for  By IP address and  By name.
- IP Version:** Radio buttons for  Version 6 and  Version 4.
- IPv6 Address Type:** Radio buttons for  Link Local and  Global.
- Link Local Interface:** A dropdown menu currently set to "None".
- TFTP Server:** A text input field.
- Source File Name:** A text input field.

Below the form, there is a note: "The firmware is upgraded to the inactive image file. You must activate the firmware using the 'Active Image' page." At the bottom right, there are "Apply" and "Cancel" buttons.

2. Select the **Transfer Method**, either *via TFTP* or *via HTTP*.
3. If you selected *via TFTP* as the **Transfer Method**, select the **Save Action** and then enter the parameters as described in this step.
  - ◆ **File Type**—Select the configuration file type. Only valid file types are displayed. (The file types are described in the [Files and File Types](#) section.)
  - ◆ **Host Definition**—Select if the host is going to be identified by its IP address or by name.
  - ◆ **IP Version**—Select the supported IP format.
  - ◆ **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:

- *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- ◆ **Link Local Interface**—Select the link local interface (if IPv6 is used) from the list.
  - ◆ **TFTP Server**—Enter the IP address of the TFTP server.
  - ◆ **Source/Destination File Name**—Enter the name of the source/destination file.
4. If you selected *via HTTP* as the **Transfer Method**, and *Upgrade* as the **Save Action**, enter the parameters as described in this step.
    - ◆ **File Type**—Select the configuration file type. (The file types are described in the [Files and File Types](#) section.)
    - ◆ **File Name**—Click *Browse* to select a file or enter the path and source file name to be used in the transfer.
  5. If you selected *via HTTP* as the **Transfer Method**, and *Backup* as the **Save Action**, enter the parameters as described in this step.
    - ◆ **Source File Type**—Select the configuration file type. Only valid file types are displayed. (The file types are described in the [Files and File Types](#) section.)
  6. Click **Apply**. The file is upgraded or backed up.

## SELECTING THE ACTIVE IMAGE

There are two firmware images, **Image1** and **Image2**, stored on the switch. One of the images is identified as the *active image* and other image is identified as the *inactive image*. The switch boots from the image you set as the *active image*. You can change the image identified as the *inactive image* to the *active image*. (You can reboot the switch by using the process described in the [Rebooting the Switch](#) section.)

For a stackable device, the active image is indicated/selected per each stack unit.

To select the active image:

1. Click **Administration > File Management > Active Image**. The [Active Image Page](#) is displayed.

Figure 29: Active Image Page

Active Image	Image 1
Active Image Version Number	2.0.0.23
Active Image After Reboot	Image 1
Active Image Version Number After Reboot	2.0.0.23

Apply Cancel

The page displays the following:

- ◆ **Active Image**—Displays the image file that is currently active on the switch.
- ◆ **Active Image Version Number**—Displays the firmware version of the active image.
- 2. Select the image from the **Active Image After Reboot** menu to identify the firmware image that is used as the active image after the switch is rebooted. The **Active Image Version Number After Reboot** displays the firmware version of the active image that is used after the switch is rebooted.
- 3. Click **Apply**. The active image selection is updated.

## SAVING A CONFIGURATION

The [Save Configuration Page](#) enables the backup from configuration file types on the switch to a file on another device or the restoration of configuration file types from another device to the switch.

When restoring a configuration file to the Running Configuration, the imported file *adds* any configuration commands that did not exist in the old file and *overrides* any parameter values in the existing configuration commands.

When restoring a configuration file to the Startup Configuration or a backup configuration file, the new file *replaces* the previous file.

When restoring to Startup Configuration, the switch must be rebooted for the restored Startup Configuration to be used as the Running Configuration. You can reboot the switch by using the process described in the [Rebooting the Switch](#) section.

To save the system configuration file:

1. Click **Administration > File Management > Save Configuration**. The [Save Configuration Page](#) is displayed.

Figure 30: Save Configuration Page

The screenshot shows a configuration window with the following fields and options:

- Transfer Method:** Radio buttons for  via TFTP and  via HTTP.
- Save Action:** Radio buttons for  Download and  Backup.
- Host Definition:** Radio buttons for  By IP address and  By name.
- IP Version:** Radio buttons for  Version 6 and  Version 4.
- IPv6 Address Type:** Radio buttons for  Link Local and  Global.
- Link Local Interface:** A dropdown menu currently showing "None".
- TFTP Server:** An empty text input field.
- Source File Name:** An empty text input field.
- Destination File Type:** A dropdown menu currently showing "Running configuration".

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

2. Select the **Transfer Method**, either *via TFTP* or *via HTTP*.
3. If you selected *via TFTP* as the **Transfer Method**, select the **Save Action** and then enter the parameters as described in this step.
  - **File Type**—Select the configuration file type. Only valid file types are displayed. (The file types are described in the [Files and File Types](#) section.)
  - **Host Definition**—Select if the host is going to be identified by its IP address or by name.
  - **IP Version**—Select the supported IP format.
  - **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:
    - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
    - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
  - **Link Local Interface**—Select the link local interface (if IPv6 is used) from the list.
  - **TFTP Server**—Enter the IP address of the TFTP server.
  - **Source/Destination File Name**—Enter the name of the source/destination file.

- **Destination File Type**—Select the configuration file type.
4. If you selected *via HTTP* as the **Transfer Method**, and *Download* as the **Save Action**, enter the parameters as described in this step.
    - **Source File Name**—Click *Browse* to select a file or enter the path and source file name to be used in the transfer.
    - **Destination File Type**—Select the configuration file type. (The file types are described in the [Files and File Types](#) section.)
  5. If you selected *via HTTP* as the **Transfer Method**, and *Backup* as the **Save Action**, enter the parameters as described in this step.
    - **Source File Type**—Select the configuration file type. Only valid file types are displayed. (The file types are described in the [Files and File Types](#) section.)
  6. Click **Apply**. The configuration file is downloaded or backed up.

## COPYING/SAVING CONFIGURATION FILES

When you click **Apply** on any window, changes that you made to the switch configuration settings are stored *only* in the Running Configuration. To preserve the parameters in the Running Configuration, the Running Configuration must be copied to another configuration type or saved as a file on another device.

The [Copy/Save Configuration Page](#) enables copying or saving one configuration file to another for backup purposes.



---

**NOTE:** Unless the Running Configuration is copied to the Startup Configuration or another configuration file, all changes made since the last time the file was copied are lost when the switch is rebooted.

---

The following combinations of copying internal file types are allowed:

- ◆ From the Running Configuration to the Startup Configuration or Backup Configuration.
- ◆ From the Startup Configuration to the Backup Configuration.
- ◆ From the Backup Configuration to the Startup Configuration.

To copy one configuration from one file type to another file type:

1. Click **Administration > File Management > Copy/Save Configuration**. The [Copy/Save Configuration Page](#) is displayed.

**Figure 31: Copy/Save Configuration Page**

The screenshot shows a configuration dialog box with two dropdown menus. The first dropdown, labeled 'Source File Name', is set to 'Running configuration'. The second dropdown, labeled 'Destination File Name', is set to 'Startup configuration'. To the right of these dropdowns are two buttons: 'Apply' and 'Cancel'.

2. Select the **Source File Name** to be copied. Only valid file types are displayed. (The file types are described in the [Files and File Types](#) section.)
3. Select the **Destination File Name** to be overwritten by the source file.
4. Click **Apply**. The file is copied and the Running Configuration file is updated with the settings..

## SETTING DHCP AUTO CONFIGURATION

Dynamic Host Configuration Protocol (DHCP) provides a means of passing configuration information (including the IP address of a TFTP server and a configuration file name) to hosts on a TCP/IP network. By default, the switch is enabled as a DHCP client.

When the IP address is allocated or renewed, such as during a reboot or upon an explicit DHCP renewal request and if the switch and the server are configured to do so, the switch transfers a configuration file from the TFTP server identified to the switch by DHCP. This process is known as *auto configuration*.



**NOTE:** If you enable DHCP Auto Configuration on a switch with DHCP disabled, you must enable the DHCP by using the procedure is described in the [Defining an IPv4 Interface](#) section.

The [DHCP Auto Configuration Page](#) configures the switch to receive DHCP information pointing to a TFTP server for auto configuration purposes or manual configuration of the TFTP server and configuration file in the event that the information is not provided in a DHCP message.

Note the following limitations regarding the DHCP auto-configuration process:

- ◆ A configuration file that is placed on the TFTP server must match the form and format requirements of a supported configuration file. The form and format of the file are checked, but the validity of the configuration *parameters* is not checked prior to loading it to the Startup Configuration.

- ◆ To make sure the configuration of devices functions as intended and due to allocation of different IP addresses with each DHCP renew cycle, IP addresses must be bound to MAC addresses in the DHCP server table. This ensures that each device has its own reserved IP address and other relevant information.

To configure DHCP server auto configuration:

1. Click **Administration > File Management > DHCP Auto Configuration**. The [DHCP Auto Configuration Page](#) is displayed.

**Figure 32: DHCP Auto Configuration Page**

Auto Configuration Via DHCP  Enable

Backup TFTP Server IP Address

Backup Configuration File

Note: DHCP Auto Configuration is operational only when the IP Address configuration is dynamic.

Apply Cancel

2. Enter the values.
  - **Auto Configuration Via DHCP**—Select this field to enable or disable the automatic transfer of a configuration from a TFTP server to the Startup Configuration on the switch.
  - **Backup TFTP Server IP Address**—Enter the IP address of the TFTP server to be used if no TFTP server IP address was specified in the DHCP message.
  - **Backup Configuration File**—Enter the path and file name of the file to be used when no configuration file name was specified in the DHCP message.
3. Click **Apply**. The DHCP Auto Configuration is updated and the Running Configuration file is updated with the settings.

## REBOOTING THE SWITCH

Some configuration changes, such as enabling jumbo frame support, require the system to be rebooted before they take effect. However, rebooting the switch deletes the Running Configuration, so it is critical that the Running Configuration is saved to the Startup Configuration before the switch is rebooted. Clicking **Apply** does not save the configuration to the Startup Configuration. For more information on files and file types, see the [Files and File Types](#) section.

You can backup the configuration by using Administration > Save/Copy Configuration or click **Save** at the top of the window. You can also upload the configuration from a remote device see the *Copying/Saving Configuration Files* section.

To reboot the switch:

1. Click **Administration** > **Reboot**. The *Reboot Page* is displayed.

**Figure 33: Reboot Page**



2. Click one of the Reboot buttons to reboot the switch.
  - ◆ **Reboot**—Reboots the switch. Since any unsaved information in the Running Configuration is discarded when the switch is rebooted, you must click **Save** in the upper-right corner of any window to preserve current configuration across the boot process. (If the Save option is not displayed, the Running Configuration matches the Startup Configuration and no action is necessary.)
  - ◆ **Reboot to Factory Defaults**—Reboots the switch by using factory default configuration. This process erases the Startup Configuration file; any settings that are not saved to another file are cleared when this action is selected.



**NOTE:** DHCP Auto Configuration should be disabled (enabled by default), otherwise a configuration file might be loaded from a TFTP server, instead of the factory default settings.

---

## MANAGING DEVICE DIAGNOSTICS

This section contains information for running cable tests, and viewing device operational information.

It includes the following topics:

- ◆ [Displaying Optical Module Status](#)
- ◆ [Viewing CPU Utilization](#)

### DISPLAYING OPTICAL MODULE STATUS

The [Optical Module Status Page](#) displays the operating conditions reported by the SFP (Small Form-factor Pluggable) transceiver. Some information might not be available for SFPs that do not support the digital diagnostic monitoring standard SFF-8472.

#### MSA-COMPATIBLE SFPs

The following FE SFP (100Mbps) transceivers are supported:

- ◆ MFEBX1: 100BASE-BX-20U SFP transceiver for single-mode fiber, 1310 nm wavelength, supports up to 20 km.
- ◆ MFEFX1: 100BASE-FX SFP transceiver, for multimode fiber, 1310 nm wavelength, supports up to 2 km.
- ◆ MFELX1: 100BASE-LX SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 10 km.

The following GE SFP (1000Mbps) transceivers are supported:

- ◆ MGBBX1: 1000BASE-BX-20U SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 40 km.
- ◆ MGBLH1: 1000BASE-LH SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 40 km.
- ◆ MGBLX1: 1000BASE-LX SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 10 km.
- ◆ MGBSX1: 1000BASE-SX SFP transceiver, for multimode fiber, 850 nm wavelength, supports up to 550 m.
- ◆ MGBT1: 1000BASE-T SFP transceiver for category 5 copper wire, supports up to 100 m.

To view the results of optical tests, click **Administration > Diagnostics > Optical Module Status**. The [Optical Module Status Page](#) is displayed.

**Figure 34: Optical Module Status Page**

**Optical Module Status Table**

Port	Temperature	Voltage	Current	Output Power	Input Power	Transmitter Fault	Loss of Signal	Data Ready
te0/1	0			10	10	False	False	

This page displays the following fields:

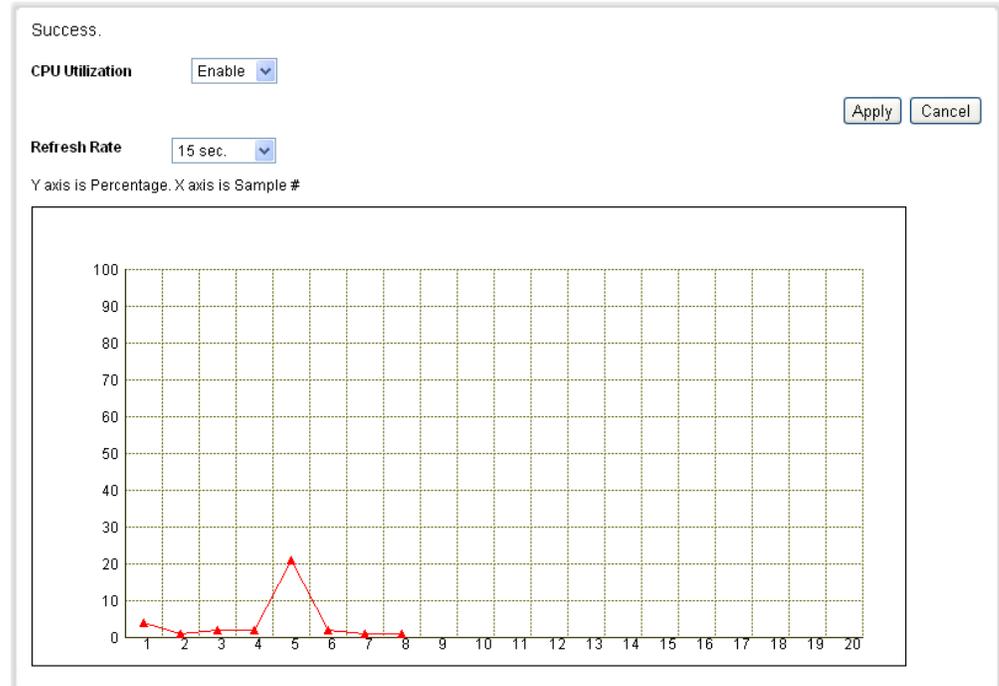
- ◆ **Port**—Port number on which the SFP is connected.
- ◆ **Temperature**—Temperature (Celsius) at which the SFP is operating.
- ◆ **Voltage**—SFP’s operating voltage.
- ◆ **Current**—SFP’s current consumption.
- ◆ **Output Power**—Transmitted optical power.
- ◆ **Input Power**—Received optical power.
- ◆ **Transmitter Fault**—Remote SFP reports signal loss. Values are True, False, and No Signal (N/S).
- ◆ **Loss of Signal**—Local SFP reports signal loss. Values are True and False.
- ◆ **Data Ready**—SFP is operational. Values are True and False

**VIEWING CPU UTILIZATION** The *CPU Utilization Page* displays the switch CPU utilization. You can enable or disable CPU utilization monitoring, and configure the rate at which the graph is updated.

To enable and display CPU utilization:

1. Click **Administration > Diagnostics > CPU Utilization**. The [CPU Utilization Page](#) is displayed.

Figure 35: CPU Utilization Page



2. Select **CPU Utilization** to enable viewing CPU resource utilization information.
3. Select the **Refresh Rate** (time period in seconds) that passes before the statistics are refreshed. A new sample is created for each time period.

The window displays a graph of the CPU utilization. The Y axis is percentage of usage, and the X axis is the sample number.

## CONFIGURING LLDP

The Link Layer Discovery Protocol (LLDP) enables network managers to troubleshoot and enhance network management by discovering and maintaining network topologies over multi-vendor environments. LLDP discovers network neighbors by standardizing methods for network devices to advertise themselves to other systems, and to store discovered information.

LLDP enables a device to advertise its identification, configuration, and capabilities to neighboring devices that then store the data in a Management Information Base (MIB). The network management system models the topology of the network by querying these MIB databases.

The LLDP protocol operates in Layer 2 by broadcasting Multicast frames from each port. These are referred to as Protocol Data Units (PDUs or LLDP PDUs), and are processed by devices that are aware of the LLDP protocol.

The LLDP PDU contains TLVs (type-length-value tuples), which contain the information broadcast by the device. The types of TLVs to be broadcast can be configured.

The LLDP protocol has an extension called LLDP Media Endpoint Discovery (LLDP-MED), which provides and accepts information from voice or video devices. For further information about LLDP-MED, see the [LLDP MED Protocol](#) section.

### LLDP CONFIGURATION WORKFLOW

Following are examples of actions that can be performed with the LLDP feature:

1. Enable LLDP globally (LLDP is enabled by default), and enter LLDP global parameters, such as the time interval for sending LLDP updates using the [Properties Page](#).
2. Configure LLDP per interface by using the [Port Settings Page](#).
3. Create LLDP MED network policies by using the [LLDP MED Network Policy Page](#).
4. Associate LLDP MED network policies to ports by using the [LLDP MED Port Settings Page](#).
5. View LLDP local port status details by using the [LLDP MED Port Status Details Page](#).
6. View the LLDP information that was discovered from neighbors, such as local port, system name, time to live, system description, system capabilities by using the [LLDP Neighbors Information Page](#).
7. View LLDP-related statistical information per interface by using the [LLDP Statistics Page](#).
8. Display overloading information by using the [LLDP Overloading Page](#).

### SETTING LLDP PROPERTIES

The *LLDP Properties Page* enables entering LLDP general parameters. These include enabling/disabling the feature globally and setting timers.

To enter LLDP properties:

1. Click **Administration** > **LLDP** > **Properties**. The [Properties Page](#) is displayed.

Figure 36: Properties Page

**LLDP Properties**

LLDP Status  ▾

TLV Advertise Interval  sec. (5 - 32768, Default: 30)  Use default

Topology Change SNMP Notification Interval  sec. (5 - 3600, Default: 5)  Use default

Hold Multiplier  (2 - 10, Default: 4)  Use default

Reinitializing Delay  sec. (1 - 10, Default: 2)  Use default

Transmit Delay  sec. (1 - 8192, Default: 2)  Use default

---

**LLDP-MED Properties**

Fast Start Repeat Count  Times (1 - 10, Default: 3)

2. Enter the parameters.

- ◆ **LLDP Status**—Select to enable LLDP on the switch.
- ◆ **TLV Advertise Interval**—Enter the rate in seconds at which LLDP advertisement updates are sent. Click **Use Default** to use the value 30 seconds.
- ◆ **Topology Change SNMP Notification Interval**—Enter the minimum time interval between SNMP notifications. Click **Use Default** to use the value 5 seconds.
- ◆ **Hold Multiplier**—Enter the amount of time that LLDP packets are held before the packets are discarded, measured in multiples of the TLV Advertise Interval. For example, if the TLV Advertise Interval is 30 seconds, and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds. Click **Use Default** to use the value 4 seconds.
- ◆ **Reinitializing Delay**—Enter the time interval in seconds that passes between disabling and reinitializing LLDP, following an LLDP enable/disable cycle. Click **Use Default** to use the value 2 seconds.
- ◆ **Transmit Delay**—Enter the amount of time in seconds that passes between successive LLDP frame transmissions due to changes in the LLDP local systems MIB. Click **Use Default** to use the value 2 seconds.

For a description of LLDP MED, refer to the [LLDP MED Protocol](#) section.

3. In the **Fast Start Repeat Count** field, enter the number of times LLDP packets are sent when the LLDP-MED Fast Start mechanism is initialized. This occurs when a new endpoint device links to the switch.
4. Click **Apply**. The LLDP properties are defined and the Running Configuration file is updated with the settings..

**EDITING LLDP PORT SETTINGS** The [Port Settings Page](#) enables activating LLDP and SNMP notification per port, and entering the TLVs that are sent in the LLDP PDU.

By setting these properties it is possible to select the types of information to be provided to devices that support the LLDP protocol.

The LLDP-MED TLVs to be advertised can be selected in the [LLDP MED Port Settings Page](#).

To define the LLDP port settings:

1. Click **Administration > LLDP > Port Settings**. The [Port Settings Page](#) is displayed.

**Figure 37: Port Settings Page**

LLDP Port Setting Table							
	Entry No.	Interface	Administrative Status	SNMP Notification	Selected Optional TLVs	Management IP Address	
						Mode	IP Address
<input type="radio"/>	1	te0/1	Tx & Rx	Disabled		None	
<input type="radio"/>	2	te0/2	Tx & Rx	Disabled		None	
<input type="radio"/>	3	te0/3	Tx & Rx	Disabled		None	
<input type="radio"/>	4	te0/4	Tx & Rx	Disabled		None	
<input type="radio"/>	5	te0/5	Tx & Rx	Disabled		None	
<input type="radio"/>	6	te0/6	Tx & Rx	Disabled		None	
<input type="radio"/>	7	te0/7	Tx & Rx	Disabled		None	
<input type="radio"/>	8	te0/8	Tx & Rx	Disabled		None	
<input type="radio"/>	9	te0/9	Tx & Rx	Disabled		None	
<input type="radio"/>	10	te0/10	Tx & Rx	Disabled		None	
<input type="radio"/>	11	te0/11	Tx & Rx	Disabled		None	

This page displays the port LLDP information.

2. Select a port and click **Edit**. The [Edit LLDP Port Settings Page](#) is displayed.

Figure 38: Edit LLDP Port Settings Page

**Properties**

Interface: te0/2

Administrative Status: Tx & Rx

SNMP Notification: Disable

Available Optional TLVs: Port Description, System Name, System Description, System Capabilities, 802.3 MAC-PHY

Selected Optional TLVs: (empty)

Management Address Optional TLV: None

Advertisement Mode: None

IP Address: 192.168.1.5

Apply

This page provides the following fields:

- ◆ **Interface**—Select the port to be defined.
- ◆ **Administrative Status**—Select the LLDP publishing option for the port. The values are:
  - *Tx Only*—Publishes only but does not discover.
  - *Rx Only*—Discovers but does not publish.
  - *Tx & Rx*—Publishes and discovers.
  - *Disable*—Indicates that LLDP is disabled on the port.
- ◆ **SNMP Notification**—Select **Enable** to send notifications to SNMP notification recipients, for example a SNMP managing system, when there is a topology change.
- ◆ The time interval between notifications is entered in the Topology Change SNMP Notification Interval field in the [Properties Page](#). Define SNMP Notification Recipients by using the **SNMP > Notification Recipient v1,2** and/or **SNMP > Notification Recipient v3**.
- ◆ **Available Optional TLVs**—Select the information to be published by the switch by moving the TLV to the **Selected Optional TLVs** list. The available TLVs contain the following information:
  - *Port Description*—Information about the port, including manufacturer, product name and hardware/software version.
  - *System Name*—System's assigned name (in alpha-numeric format). The value equals the sysName object.

- *System Description*—Description of the network entity (in alpha-numeric format). This includes the system's name and versions of the hardware, operating system, and networking software supported by the switch. The value equals the sysDescr object.
- *System Capabilities*—Primary functions of the switch, and whether or not these functions are enabled in the switch. The capabilities are indicated by two octets. Bits 0 through 7 indicate Other, Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and station respectively. Bits 8 through 15 are reserved.
- *802.3 MAC-PHY*—Duplex and bit rate capability and the current duplex and bit rate settings of the sending device. It also indicates whether the current settings are due to auto-negotiation or manual configuration.
- *802.3 Link Aggregation*—Whether the link (associated with the port on which the LLDP PDU is transmitted) can be aggregated. It also indicates whether the link is currently aggregated, and if so, provides the aggregated port identifier.
- *802.3 Maximum Frame*—Maximum frame size capability of the MAC/PHY implementation.

The following fields relate to the Management Address:

- ◆ **Advertisement Mode**—Select one of the following ways to advertise the IP management address of the switch:
    - *Auto Advertise*—Send the current management IP address of the switch, regardless of whether it was acquired via DHCP or manually.
    - *None*—Do not advertise the management IP address.
    - *Manual Advertise*—Select this option and the management IP address to be advertised. We recommended that this option be selected when the switch is in Layer 3 mode and the switch is configured with multiple IP addresses.
  - ◆ **IP Address**—If Manual Advertise was selected, select the Management IP address from the addresses provided.
3. Enter the relevant information, and click **Apply**. The port settings are modified, and the Running Configuration file is updated with the settings.

**LLDP MED PROTOCOL** *LLDP Media Endpoint Discovery (LLDP-MED)* is an enhancement of LLDP that provides additional capabilities to support media devices.

LLDP-MED:

- ◆ Provides detailed network topology information, including the devices located on the network and their location, for example, which IP phone

is connected to which port, which software is running on which switch, and which port is connected to which PC.

- ◆ Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Emergency Call Service (E-911) by using IP Phone location information.
- ◆ Provides troubleshooting information. LLDP MED sends alerts to network managers:
  - Port speed and duplex mode conflicts
  - QoS policy misconfigurations



**NOTE:** The switch automatically *advertises* the policy according to your configuration; however, you must also manually configure the switch to *use* that policy.

---

## SETTING LLDP MED NETWORK POLICY

An LLDP-MED network policy is a related set of configuration settings identified by a network policy number. This set is loaded into an LLDP-MED TLV, and sent to devices connected to the switch. This information is used by the connected device to send traffic, as specified in the network policy. For example, a policy can be created for VoIP phones that instructs them to:

- ◆ Send voice traffic on VLAN 10
- ◆ Tag voice traffic with DSCP=63
- ◆ Transmit data-traffic to the switch (from the PC connected to the switch through the VoIP phone) without modification to traffic sent by the PC (typically, Untagged).

Network policies are associated with ports by using the [LLDP MED Port Settings Page](#). (An administrator must create the VLANs, and configure memberships in the VLANs based on the specification in the LLDP-MED network policies.)

To define an LLDP MED network policy:

1. Click **Administration > LLDP > LLDP MED Network Policy**. The [LLDP MED Network Policy Page](#) is displayed.

**Figure 39: LLDP MED Network Policy Page**

<input type="checkbox"/>	Network Policy Number	Application	VLAN ID	VLAN Tag	User Priority	DSCP Value
Table is empty						
						<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>

This page displays previously-created network policies.

- Click **Add** and the [Add LLDP MED Network Policy Page](#) is displayed.

**Figure 40: Add LLDP MED Network Policy Page**

Network Policy Number	1
Application	Voice
VLAN ID	<input type="text"/> (0 - 4095)
VLAN Tag	Tagged
User Priority	0
DSCP Value	0

This page enables the definition of new policies.

- Enter the values.

- ◆ **Network Policy Number**—Select the number of the policy to be created.
- ◆ **Application**—Select from the list the type of application (type of traffic) for which the network policy is being defined:
  - **Voice**
  - **Voice Signaling**
  - **Guest Voice**
  - **Guest Voice Signaling**
  - **Softphone Voice**
  - **Video Conferencing**

- **Streaming Video**
  - **Video Signaling**
  - ◆ **VLAN ID**—Enter the VLAN ID to which the traffic should be sent.
  - ◆ **VLAN Tag**—Select whether the traffic is Tagged or Untagged.
  - ◆ **User Priority**—Select the traffic priority applied to traffic defined by this network policy.
  - ◆ **DSCP Value**—Select the DSCP value to associate with application data sent by neighbors. This informs them how they should mark the application traffic they send to the switch.
4. Click **Apply**. The network policy is defined. Associate the network policy with a port by using the [LLDP MED Port Settings Page](#).

### CONFIGURING LLDP MED PORT SETTINGS

The *LLDP MED Port Settings Page* enables selecting the network policies, configured in the [LLDP MED Network Policy Page](#), to be advertised on the port, and selecting the LLDP-MED TLVs to be sent inside the LLDP PDU.

To configure LLDP MED on each port:

1. Click **Administration > LLDP > LLDP MED Port Settings**. The [LLDP MED Port Settings Page](#) is displayed.

**Figure 41: LLDP MED Port Settings Page**

LLDP MED Port Setting Table							
	Entry No.	Port	LLDP MED Status	SNMP Notification	Network Policy	Location	Inventory
<input type="radio"/>	1	te0/1	Disabled	Enabled	No	No	No
<input type="radio"/>	2	te0/2	Disabled	Enabled	No	No	No
<input type="radio"/>	3	te0/3	Disabled	Enabled	No	No	No
<input type="radio"/>	4	te0/4	Disabled	Enabled	No	No	No
<input type="radio"/>	5	te0/5	Disabled	Enabled	No	No	No
<input type="radio"/>	6	te0/6	Disabled	Enabled	No	No	No
<input type="radio"/>	7	te0/7	Disabled	Enabled	No	No	No
<input type="radio"/>	8	te0/8	Disabled	Enabled	No	No	No
<input type="radio"/>	9	te0/9	Disabled	Enabled	No	No	No
<input type="radio"/>	10	te0/10	Disabled	Enabled	No	No	No
<input type="radio"/>	11	te0/11	Disabled	Enabled	No	No	No

This page displays LLDP MED settings, including enabled TLVs, for all ports.

2. Select a port, and click **Edit**. The [Edit LLDP MED Port Settings Page](#) is displayed.

Figure 42: Edit LLDP MED Port Settings Page

The screenshot shows the 'Edit LLDP MED Port Settings Page' with the following fields and options:

- Port:** te0/3
- LLDP MED Status:** Disable
- SNMP Notification:** Enable
- Available Optional TLVs:** Network Policy, Location, Inventory
- Selected Optional TLVs:** (Empty)
- Available Network Policies:** (Empty)
- Selected Network Policies:** (Empty)
- Location Coordinate:** (16 pairs of hexadecimal characters)
- Location Civic Address:** (6-160 pairs of hexadecimal characters)
- Location ECS ELIN:** (10-25 pairs of hexadecimal characters)
- Apply** button

This page enables associating LLDP MED policies to ports.

### 3. Enter the parameters.

- **Port**—Select a port to configure. After you have configured this port and clicked **Apply**, you can configure another port without returning to the LLDP MED Port Settings Page.
- **LLDP MED Status**—Enable/disable LLDP MED on this port.
- **SNMP Notification**—Select whether SNMP notification is sent on a per-port basis when an end station that supports MED is discovered, for example a SNMP managing system, when there is a topology change.
- **Available Optional TLVs**—Select the TLVs that can be published by the switch, by moving them to the *Selected Optional TLVs* list.
- **Available Network Policies**—Select the LLDP MED policies that will be published by LLDP, by moving them to the *Selected Network Policies* list. These were created in the [LLDP MED Network Policy Page](#).



**NOTE:** The following fields must be entered in hexadecimal characters in the exact data format that is defined in the LLDP-MED standard (ANSI-TIA-1057\_final\_for\_publication.pdf).

- **Location Coordinate**—Enter the coordinate location to be published by LLDP.
- **Location Civic Address**—Enter the civic address to be published by LLDP.

- **Location (ECS) ELIN**—Enter the Emergency Call Service (ECS) ELIN location to be published by LLDP.
4. Click **Apply**. The LLDP MED port settings are modified, and the Running Configuration file is updated.

**DISPLAYING LLDP NEIGHBORS INFORMATION**

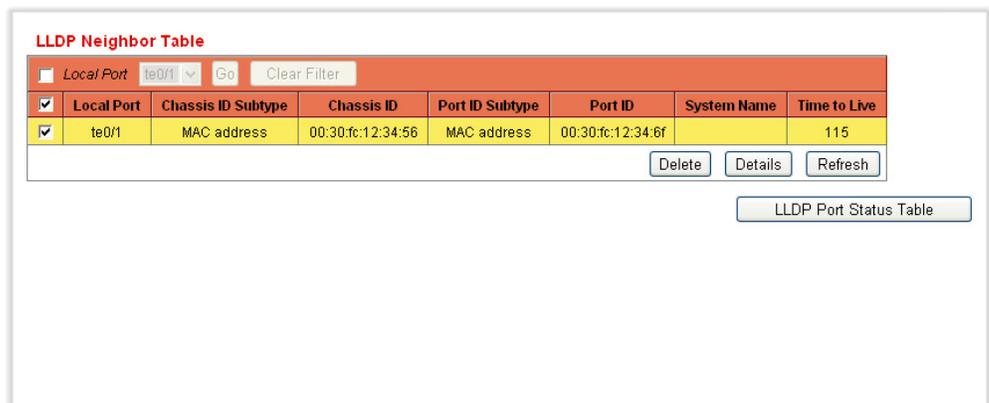
The [LLDP Neighbors Information Page](#) displays information that was received using the LLDP protocol from neighboring devices.

After timeout (based on the value received from the neighbor Time To Live TLV during which no LLDP PDU was received from a neighbor), the information is deleted.

To view the LLDP neighbors information:

1. Click **Administration > LLDP > Neighbors Information**. The [LLDP Neighbors Information Page](#) is displayed.

**Figure 43: LLDP Neighbors Information Page**

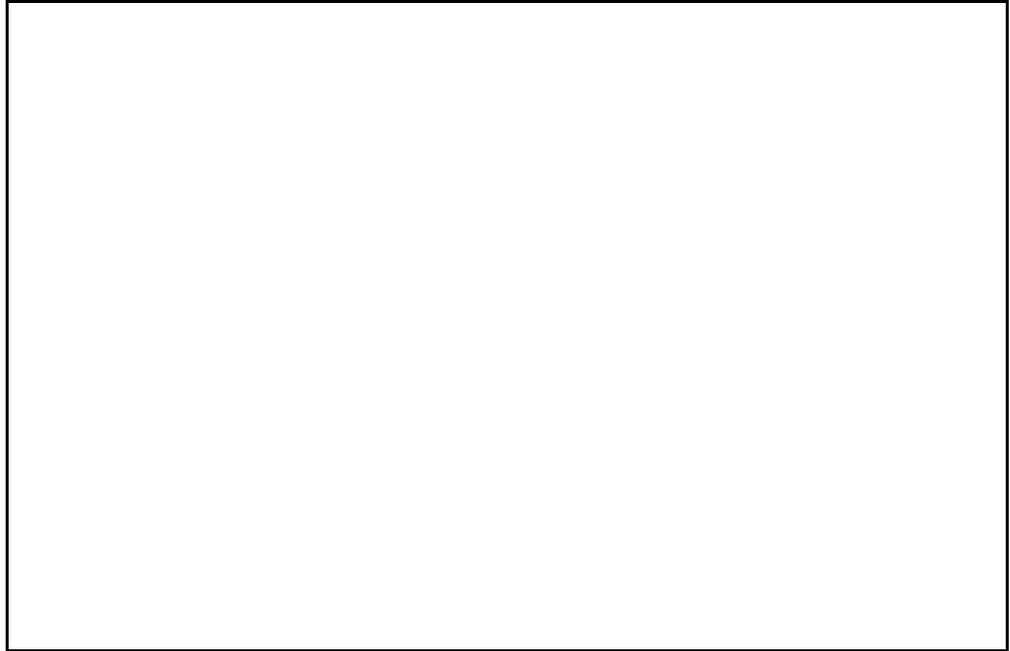


This page displays the following fields:

- ◆ **Local Port**—Number of the local port to which the neighbor is connected.
- ◆ **Chassis ID Subtype**—Type of chassis ID (for example, MAC address).
- ◆ **Chassis ID**—Identifier of the 802 LAN neighboring device's chassis.
- ◆ **Port ID Subtype**—Type of the port identifier that is shown.
- ◆ **Port ID**—Identifier of port.
- ◆ **System Name**—Published name of the switch.
- ◆ **Time to Live**—Time interval (in seconds) after which the information for this neighbor is deleted.

1. Select a local port, and click **Details**. The [Neighbors Information Page](#) is displayed.

**Figure 44: Neighbors Information Page**



This page displays the following fields:

#### **PORT DETAILS**

- ◆ **Local Port**—Port number.
- ◆ **MSAP Entry**—Device Media Service Access Point (MSAP) entry number.

#### **BASIC DETAILS**

- ◆ **Chassis ID Subtype**—Type of chassis ID (for example, MAC address).
- ◆ **Chassis ID**—Identifier of the 802 LAN neighboring device chassis.
- ◆ **Port ID Subtype**—Type of the port identifier that is shown.
- ◆ **Port ID**—Identifier of port.
- ◆ **Port Description**—Information about the port, including manufacturer, product name and hardware/software version.
- ◆ **System Name**—Name of system that is published.
- ◆ **System Description**—Description of the network entity (in alphanumeric format). This includes the system name and versions of the hardware, operating system, and networking software supported by the device. The value equals the sysDescr object.

- ◆ **Supported System Capabilities**—Primary functions of the device. The capabilities are indicated by two octets. Bits 0 through 7 indicate Other, Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and station respectively. Bits 8 through 15 are reserved.
- ◆ **Enabled System Capabilities**—Primary enabled function(s) of the device.

### MANAGED ADDRESS

- ◆ **Address Subtype**—Managed address subtype, for example, MAC or IPv4.
- ◆ **Address**—Managed address.
- ◆ **Interface Subtype**—Port subtype.
- ◆ **Interface Number**—Port number.

### MAC/PHY DETAILS

- ◆ **Auto-Negotiation Supported**—Port speed auto-negotiation support status. The possible values are True and False.
- ◆ **Auto-Negotiation Enabled**—Port speed auto-negotiation active status. The possible values are True and False.
- ◆ **Auto-Negotiation Advertised Capabilities**—Port speed auto-negotiation capabilities, for example, 1000BASE-T half duplex mode, 100BASE-TX full duplex mode.
- ◆ **Operational MAU Type**—Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network, for example, 100BASE-TX full duplex mode.

### 802.3 POWER VIA MDI

- ◆ **MDI Power Support Port Class**—Advertised power support port class.
- ◆ **PSE MDI Power Support**—Indicates if MDI power is supported on the port.
- ◆ **PSE MDI Power State**—Indicates if MDI power is enabled on the port.
- ◆ **PSE Power Pair Control Ability**—Indicates if power pair control is supported on the port.
- ◆ **PSE Power Pair**—Power pair control type supported on the port.
- ◆ **PSE Power Class**—Advertised power class of the port.

### 802.3 DETAILS

- ◆ **802.3 Maximum Frame Size**—Advertised maximum frame size that is supported on the port.

### 802.3 LINK AGGREGATION

- ◆ **Aggregation Capability**—Indicates if the port can be aggregated.
- ◆ **Aggregation Status**—Indicates if the port is currently aggregated.
- ◆ **Aggregation Port ID**—Advertised aggregated port ID.

### MED DETAILS

- ◆ **Capabilities Supported**—MED capabilities enabled on the port.
- ◆ **Current Capabilities**—MED TLVs advertised by the port.
- ◆ **Device Class**—LLDP-MED endpoint device class. The possible device classes are:
  - *Endpoint Class 1*—Indicates a generic endpoint class, offering basic LLDP services.
  - *Endpoint Class 2*—Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features.
  - *Endpoint Class 3*—Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support and device information management capabilities.
- ◆ **PoE Device Type**—Port PoE type, for example, powered.
- ◆ **PoE Power Source**—Port's power source.
- ◆ **PoE Power Priority**—Port's power priority.
- ◆ **PoE Power Value**—Port's power value.
- ◆ **Hardware Revision**—Hardware version.
- ◆ **Firmware Revision**—Firmware version.
- ◆ **Software Revision**—Software version.
- ◆ **Serial Number**—Device serial number.
- ◆ **Manufacturer Name**—Device manufacturer name.
- ◆ **Model Name**—Device model name.
- ◆ **Asset ID**—Asset ID.

## 802.1 VLAN AND PROTOCOL

- ◆ **PVID**—Advertised port VLAN ID.

### PPVID

- ◆ **VID**—Protocol VLAN ID.
- ◆ **Supported**—Supported Port and Protocol VLAN IDs.
- ◆ **Enabled**—Enabled Port and Protocol VLAN IDs.

### VLAN IDs

- ◆ **VID**—Port and Protocol VLAN ID.
- ◆ **VLAN Names**—Advertised VLAN names.

### PROTOCOL IDs

- ◆ **Protocol ID**—Advertised protocol IDs.

## LOCATION INFORMATION

Enter the following data structures in hexadecimal as described in section 10.2.4 of the ANSI-TIA-1057 standard:

- ◆ **Civic**—Civic or street address.
- ◆ **Coordinates**—Location map coordinates—latitude, longitude, and altitude.
- ◆ **ECS ELIN**—Device's Emergency Call Service (ECS) Emergency Location Identification Number (ELIN).
- ◆ **Unknown**—Unknown location information.

## NETWORK POLICIES

- ◆ **Application Type**—Network policy application type, for example, Voice.
- ◆ **VLAN ID**—VLAN ID for which the network policy is defined.
- ◆ **VLAN Type**—VLAN type, Tagged or Untagged, for which the network policy is defined.
- ◆ **User Priority**—Network policy user priority.
- ◆ **DSCP**—Network policy DSCP.

**ACCESSING LLDP STATISTICS** The *LLDP Statistics Page* displays LLDP statistical information per port.

To view the LLDP statistics:

1. Click **Administration > LLDP > LLDP Statistics**. The [LLDP Statistics Page](#) is displayed.

**Figure 45: LLDP Statistics Page**

**LLDP Statistics Table**

Interface	Tx Frames	Rx Frames			Rx TLVs		Neighbor's Information
	Total	Total	Discarded	Errors	Discarded	Unrecognized	Deletion Count
te0/1	188	0	0	0	0	0	0
te0/2	0	0	0	0	0	0	0
te0/3	0	0	0	0	0	0	0
te0/4	0	0	0	0	0	0	0
te0/5	0	0	0	0	0	0	0
te0/6	0	0	0	0	0	0	0
te0/7	0	0	0	0	0	0	0
te0/8	0	0	0	0	0	0	0
te0/9	0	0	0	0	0	0	0
te0/10	0	0	0	0	0	0	0

For each port, the fields are displayed:

- ◆ **Interface**—Identifier of interface.
  - ◆ **Tx Frames Total**—Number of transmitted frames.
  - ◆ **Rx Frames**
    - **Total**—Number of received frames.
    - **Discarded**—Total number of received frames that were discarded.
    - **Errors**—Total number of received frames with errors.
  - ◆ **Rx TLVs**
    - **Discarded**—Total number of received TLVs that were discarded.
    - **Unrecognized**—Total number of received TLVs that were unrecognized.
  - ◆ **Neighbor's Information Deletion Count**—Number of neighbor ageouts on the interface.
2. Click **Refresh** to view the latest statistics.

**LLDP OVERLOADING** LLDP adds information to packets, and can create oversized packets. The information that LLDP adds is divided into groups. The switch transmits the maximum number of whole groups possible, meaning that no partial groups are transmitted.

The [LLDP Overloading Page](#) displays the number of bytes sent and number of bytes remaining to be sent for LLDP TLVs per port, and the port's transmission status.

To view LLDP overloading information:

1. Click **Administration > LLDP > LLDP Overloading**. The [LLDP Overloading Page](#) is displayed.

**Figure 46: LLDP Overloading Page**



LLDP Overloading Table				
	Interface	Total (Bytes)	Left to Send (Bytes)	Status
<input type="radio"/>	te0/1	88	1409	Not Overloading
<input type="radio"/>	te0/2	74	1423	Not Overloading
<input type="radio"/>	te0/3	74	1423	Not Overloading
<input type="radio"/>	te0/4	74	1423	Not Overloading
<input type="radio"/>	te0/5	74	1423	Not Overloading
<input type="radio"/>	te0/6	74	1423	Not Overloading
<input type="radio"/>	te0/7	74	1423	Not Overloading
<input type="radio"/>	te0/8	74	1423	Not Overloading
<input type="radio"/>	te0/9	74	1423	Not Overloading
<input type="radio"/>	te0/10	75	1422	Not Overloading
<input type="radio"/>	te0/11	75	1422	Not Overloading

This page displays the following fields for each port:

- ◆ **Interface**—Port identifier.
  - ◆ **Total (Bytes)**—Total number of bytes in each packet.
  - ◆ **Left to Send (Bytes)**—Total number of bytes left to add into the packet.
  - ◆ **Status**—Whether TLVs are being transmitted or if they are overloaded.
2. To view the overloading details for a port, select it and click **Details**. The [LLDP Overloading Details](#) is displayed.

**Figure 47: LLDP Overloading Details**

Interface	
te0/1	
<b>LLDP Mandatory TLVs</b>	
Size (Bytes)	23
Status	Transmitted
<b>LLDP MED Capabilities</b>	
Size (Bytes)	
Status	
<b>LLDP MED Location</b>	
Size (Bytes)	
Status	
<b>LLDP MED Network Policy</b>	
Size (Bytes)	
Status	
<b>LLDP MED Extended Power via MDI</b>	
Size (Bytes)	
Status	
<b>802.3 TLVs</b>	
Size (Bytes)	
Status	
<b>LLDP Optional TLVs</b>	
Size (Bytes)	14
Status	Transmitted
<b>LLDP MED Inventory</b>	
Size (Bytes)	
Status	
<b>Total</b>	
Total (Bytes)	88
Left to Send (Bytes)	1409

This page displays the following information for each TLV sent on the port:

◆ **LLDP Mandatory TLVs**

- *Size (Bytes)*—Total mandatory TLV byte size.
- *Status*—If the mandatory TLV group is being transmitted, or if the TLV group was overloaded.

◆ **LLDP MED Capabilities**

- *Size (Bytes)*—Total LLDP MED capabilities packets byte size.
- *Status*—If the LLDP MED capabilities packets were sent, or if they were overloaded.

◆ **LLDP MED Location**

- *Size (Bytes)*—Total LLDP MED location packets byte size.
- *Status*—If the LLDP MED locations packets were sent, or if they were overloaded.

◆ **LLDP MED Network Policy**

- *Size (Bytes)*—Total LLDP MED network policies packets byte size.
- *Status*—If the LLDP MED network policies packets were sent, or if they were overloaded.

◆ **LLDP MED Extended Power via MDI**

- *Size (Bytes)*—Total LLDP MED extended power via MDI packets byte size.
- *Status*—If the LLDP MED extended power via MDI packets were sent, or if they were overloaded.

◆ **802.3 TLVs**

- *Size (Bytes)*—Total LLDP MED 802.3 TLVs packets byte size.
- *Status*—If the LLDP MED 802.3 TLVs packets were sent, or if they were overloaded.

◆ **LLDP Optional TLVs**

- *Size (Bytes)*—Total LLDP MED optional TLVs packets byte size.
- *Status*—If the LLDP MED optional TLVs packets were sent, or if they were overloaded.

◆ **LLDP MED Inventory**

- *Size (Bytes)*—Total LLDP MED inventory TLVs packets byte size.
- *Status*—If the LLDP MED inventory packets were sent, or if they were overloaded.

◆ **Total (Bytes)**—Total number of packets sent (in bytes).

◆ **Left to Send (Bytes)**—Total number of packet bytes left to transmit.

**DISPLAYING LLDP  
MED PORT STATUS  
DETAILS**

To view the LLDP port status details

1. Click **Administration > LLDP > LLDP MED Port Status Details**. The [LLDP MED Port Status Details Page](#) is displayed.

Figure 48: LLDP MED Port Status Details Page

Port	te0/1
<b>Global</b>	
Chassis ID Subtype	MAC address
Chassis ID	00:11:22:33:44:55
System Name	
System Description	Standalone Managed L3 10G Switch with 48 SFP+ slots
Supported System Capabilities	Bridge, Router
Enabled System Capabilities	Bridge, Router
Port ID Subtype	Interface name
Port ID	te0/1
Port Description	Ethernet Interface
<b>Management Address</b>	
Address Subtype	IPv4
Address	192.168.1.5

2. Select the desired port from the **Port** list.

This page provides the following fields:

### GLOBAL

- ◆ **Chassis ID Subtype**—Type of chassis ID. (For example the MAC address.)
- ◆ **Chassis ID**—Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.
- ◆ **System Name**—Name of switch.
- ◆ **System Description**—Description of the switch (in alpha-numeric format).
- ◆ **Supported System Capabilities**—Primary functions of the device, such as Bridge, WLAN AP, or Router.
- ◆ **Enabled System Capabilities**—Primary enabled function(s) of the device.
- ◆ **Port ID Subtype**—Type of the port identifier that is shown.
- ◆ **Port ID**—Identifier of port.
- ◆ **Port Description**—Information about the port, including manufacturer, product name and hardware/software version.

## MANAGEMENT ADDRESS

Displays the table of addresses of the local LLDP agent. Other remote managers can use this address to obtain information related to the local device. The address consists of the following elements:

- ◆ **Address Subtype**—Type of management IP address that is listed in the Management Address field, for example, IPv4.
- ◆ **Address**—Returned address most appropriate for management use, typically a Layer 3 address.
- ◆ **Interface Subtype**—Numbering method used for defining the interface number.
- ◆ **Interface Number**—Specific interface associated with this management address.

## MAC/PHY DETAILS

- ◆ **Auto-Negotiation Supported**—Port speed auto-negotiation support status.
- ◆ **Auto-Negotiation Enabled**—Port speed auto-negotiation active status.
- ◆ **Auto-Negotiation Advertised Capabilities**—Port speed auto-negotiation capabilities, for example, 1000BASE-T half duplex mode, 100BASE-TX full duplex mode.
- ◆ **Operational MAU Type**—Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network, for example, 100BASE-TX full duplex mode.

## 802.3 DETAILS

- ◆ **802.3 Maximum Frame Size**—The maximum supported IEEE 802.3 frame size.

## 802.3 LINK AGGREGATION

- ◆ **Aggregation Capability**—Indicates whether the interface can be aggregated.
- ◆ **Aggregation Status**—Indicates whether the interface is aggregated.
- ◆ **Aggregation Port ID**—Advertised aggregated interface ID.

## MED DETAILS

- ◆ **Capabilities Supported**—MED capabilities supported on the port.
- ◆ **Current Capabilities**—MED capabilities enabled on the port.

- ◆ **Device Class**—LLDP-MED endpoint device class. The possible device classes are:
  - **Endpoint Class 1**—Indicates a generic endpoint class, offering basic LLDP services.
  - **Endpoint Class 2**—Indicates a media endpoint class, offering media streaming capabilities, as well as all Class 1 features.
  - **Endpoint Class 3**—Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support, and device information management capabilities.
- ◆ **PoE Device Type**—Port PoE type, for example, powered.
- ◆ **PoE Power Source**—Port power source.
- ◆ **PoE Power Priority**—Port power priority.
- ◆ **PoE Power Value**—Port power value.
- ◆ **Hardware Revision**—Hardware version.
- ◆ **Firmware Revision**—Firmware version.
- ◆ **Software Revision**—Software version.
- ◆ **Serial Number**—Device serial number.
- ◆ **Manufacturer Name**—Device manufacturer name.
- ◆ **Model Name**—Device model name.
- ◆ **Asset ID**—Asset ID.

#### LOCATION INFORMATION

Enter the following data structures in hexadecimal as described in section 10.2.4 of the ANSI-TIA-1057 standard:

- ◆ **Civic**—Street address.
- ◆ **Coordinates**—Map coordinates: latitude, longitude, and altitude.
- ◆ **ECS ELIN**—Emergency Call Service (ECS) Emergency Location Identification Number (ELIN).

#### NETWORK POLICY TABLE

- ◆ **Application Type**—Network policy application type, for example, Voice.
- ◆ **VLAN ID**—VLAN ID for which the network policy is defined.

- ◆ **VLAN Type**—VLAN type for which the network policy is defined. The possible field values are:
  - Tagged—Indicates the network policy is defined for tagged VLANs.
  - Untagged—Indicates the network policy is defined for untagged VLANs.
- ◆ **User Priority**—Network policy user priority.
- ◆ **DSCP**—Network policy DSCP.

**DISPLAYING LLDP  
MED PORT STATUS  
TABLE**

The [LLDP MED Port StatusTable Page](#) displays the LLDP global information, as well as the LLDP status for every port.

To view the LLDP MED port status table:

1. Click **Administration > LLDP > LLDP MED Port Status**. The [LLDP MED Port StatusTable Page](#) is displayed.

**Figure 49: LLDP MED Port StatusTable Page**

The screenshot shows the 'LLDP Port Status Global Information' section with the following details:

- Chassis ID Subtype:** MAC address
- Chassis ID:** 00:11:22:33:44:55
- System Name:**
- System Description:** Standalone Managed L3 10G Switch with 48 SFP+ slots
- Supported System Capabilities:** Bridge, Router
- Enabled System Capabilities:** Bridge, Router
- Port ID Subtype:** Interface name

Below this is the 'LLDP Port Status Table' with the following data:

	Interface	LLDP Status	LLDP MED Status	# of neighbors	Neighbor capability of 1st device
<input type="radio"/>	te0/1	Tx & Rx	Enabled	0	
<input type="radio"/>	te0/2	Tx & Rx	Disabled	0	
<input type="radio"/>	te0/3	Tx & Rx	Disabled	0	
<input type="radio"/>	te0/4	Tx & Rx	Disabled	0	

**LLDP PORT STATUS GLOBAL INFORMATION**

- ◆ **Chassis ID Subtype**—Type of chassis ID (for example, MAC address).
- ◆ **Chassis ID**—Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.
- ◆ **System Name**—Name of switch.
- ◆ **System Description**—Description of the switch (in alpha-numeric format).

- ◆ **Supported System Capabilities**—Primary functions of the device, such as Bridge, WLAN AP, or Router.
- ◆ **Enabled System Capabilities**—Primary enabled function(s) of the device.
- ◆ **Port ID Subtype**—Type of the port identifier that is shown.

#### LLDP PORT STATUS TABLE

- ◆ **Interface**—Port identifier.
  - ◆ **LLDP Status**—LLDP publishing option.
  - ◆ **LLDP MED Status**—Enabled or disabled.
  - ◆ **# of neighbors**—Number of neighbors discovered.
  - ◆ **Neighbor Capability of 1st Device**—Displays the primary enabled device functions of the neighbor, for example: Bridge or Router.
2. Click **LLDP Local Information Details** to see the details of the LLDP and LLDP-MED TLVs sent to the neighbor.
  3. Click **LLDP Neighbor Information Details** to see the details of the LLDP and LLDP-MED TLVs received from the neighbor.

---

## CONFIGURING SFLOW

This section describes sFlow monitoring of traffic.

It includes the following topics:

- ◆ sFlow Overview
- ◆ Configuring sFlow Receiver Settings
- ◆ Configuring sFlow Interface Settings
- ◆ Viewing sFlow Statistics

**SFLOW OVERVIEW** The sFlow feature enables collecting statistics using the sFlow sampling technology, based on RFC 3176.

This sampling technology is embedded within switches and routers. It provides the ability to continuously monitor traffic flows on some or all the interfaces, simultaneously.

The sFlow monitoring system consists of an sFlow agent (embedded in a switch or router or in a stand alone probe) and a central data collector, known as the sFlow analyzer.

The sFlow agent uses sampling technology to capture traffic and statistics from the device it is monitoring. sFlow datagrams are used to immediately forward the sampled traffic and statistics to an sFlow analyzer for analysis.

RFC 3176 defines:

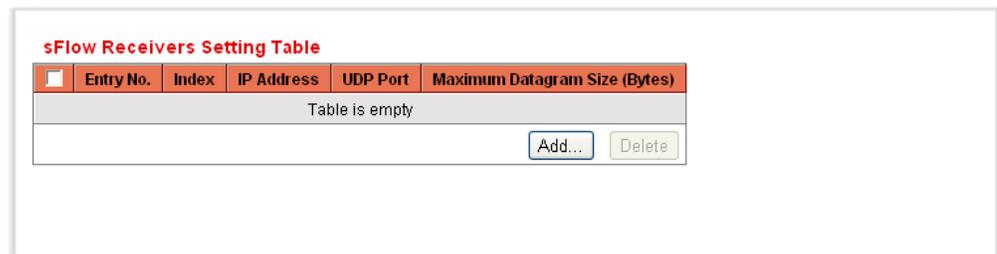
- ◆ How traffic is monitored.
- ◆ The sFlow MIB that controls the sFlow agent.
- ◆ The format of the sample data used by the sFlow agent when forwarding data to a central data collector. The device provides support for two types of sFlow sampling: flow sampling and counters sampling. The following counters sampling is performed according to RFC 3176 (if supported by the interface):
  - Generic interface counters (RFC 2233)
  - Ethernet interface counters (RFC 2358)

## CONFIGURING SFLOW RECEIVER SETTINGS

To set the IP address and UDP port of the sFlow receivers:

1. Click **Administration > sFlow > sFlow Receivers Settings**. The [sFlow Receivers Settings Page](#) is displayed.

**Figure 50: sFlow Receivers Settings Page**



<input type="checkbox"/>	Entry No.	Index	IP Address	UDP Port	Maximum Datagram Size (Bytes)
Table is empty					
					<input type="button" value="Add..."/> <input type="button" value="Delete"/>

The sflow parameters are displayed.

2. To add a receiver (sflow analyzer), click **Add** and select one of the pre-defined sampling definition indices in **Index**.
3. Enter the receiver's address fields:
  - ◆ **IP Version**—Select whether IPv4 or IPv6 format is supported.
  - ◆ **IPv6 Address Type**—When the server supports IPv6, this specifies the type of static address supported. The possible options are:
    - *Link Local*—A Link Local address that is non-routable and used for communication on the same network only.

- *Global*—A globally unique IPv6 address; visible and reachable from different subnets.
  - ◆ **Link Local Interface**—When the server supports an IPv6 Link Local address, this specifies the Link Local interface. The possible options are:
    - *None*—Disable the ISATAP tunnel.
    - *ISATAP*—The IPv6 interface is configured on an ISATAP tunnel.
    - *IP Address*—Enter the receiver’s IP address.
4. Enter the fields:
- **IP Address**—IP address to which the messages are sent.
  - **UDP Port Number**—Port to which SYSLOG message are sent.
  - **Maximum Header Size (Bytes)**—Maximum number of bytes that can be sent to the receiver in a single sample datagram (frame).

**CONFIGURING SFLOW INTERFACE SETTINGS**

After a receiver is defined, it must be associated with a port. sFlow port settings can be configured only after a receiver has been defined in the **sFlow Receiver Settings** pages.

To enable sampling and configure the port from which to collect the sFlow information:

1. Click **Administration > sFlow > sFlow Interface Settings**. The [sFlow Interface Settings Page](#) is displayed.

**Figure 51: sFlow Interface Settings Page**

sFlow Interface Setting Table						
Entry No.	Interface	Flow Sampling		Counters Sampling	Receiver Index	
		Rate	Maximum Header Size (Bytes)	Interval (Sec)	Sampling	Counters
Table is empty						
						<input type="button" value="Add..."/> <input type="button" value="Delete"/>

The sflow interface settings are displayed.

2. To associate an sFlow receiver with a port, click **Add**, and enter the fields:
  - ◆ **Interface**—Select the unit/port from which information is collected.

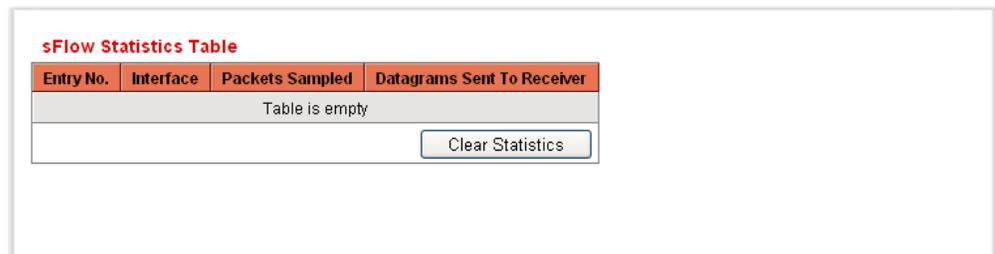
- ◆ **Flow Sampling**—Enable/disable flow sampling. This cannot be disabled if **Counters Sampling** is disabled.
- ◆ **Flow Sampling Average Sampling Rate(1024–1073741823)**—If x is entered, a flow sample will be taken for each x frames.
- ◆ **Flow Sampling Receiver Index**—Select one of the indices that was defined in the **sFlow Receivers Settings** pages.
- ◆ **Flow Sampling Maximum Header Size (20–256)**—Maximum number of bytes that should be copied from a sampled packet.
- ◆ **Counters Sampling**—Enable/disable counters sampling. This cannot be disabled if **Flow Sampling** is disabled
- ◆ **Counters Sampling Interval (15–86400)**—If x is entered, this specifies that a counter sample will be taken for each x frames.
- ◆ **Counters Sampling Receiver Index**—Select one of the indices that was defined in the **sFlow Receivers Settings** pages.

## VIEWING SFLOW STATISTICS

To view sFlow statistics:

3. Click **System > sFlow > sFlow Statistics**. The [sFlow Statistics Page](#) is displayed.

Figure 52: sFlow Statistics Page



The screenshot shows a web interface for sFlow statistics. At the top, there is a title "sFlow Statistics Table" in red. Below it is a table with four columns: "Entry No.", "Interface", "Packets Sampled", and "Datagrams Sent To Receiver". The table is currently empty, with the text "Table is empty" centered in the first row. Below the table is a button labeled "Clear Statistics".

Entry No.	Interface	Packets Sampled	Datagrams Sent To Receiver
Table is empty			

Clear Statistics

The following sflow statistics per interface are displayed:

- ◆ **Interface**—Port for which sample was collected.
  - ◆ **Packets Sampled**—Number of packets sampled.
  - ◆ **Datagrams Sent to Receiver**—Number of sFlow sampling packets sent.
4. Click **Clear Statistics** to clear the counters.

This chapter contains the following topics:

- ◆ [Configuring Ports](#)
- ◆ [Configuring Link Aggregation](#)
- ◆ [Configuring VLANs](#)
- ◆ [Creating VLANs](#)
- ◆ [Configuring VLAN Interface Settings](#)
- ◆ [Defining VLAN Membership](#)
- ◆ [Defining GVRP Settings](#)
- ◆ [Managing VLAN Groups](#)

---

## CONFIGURING PORTS

**PORT MANAGEMENT WORKFLOW** To configure ports, perform the following actions:

1. Configure port by using the [Port Settings Page](#).
2. Enable/disable the Link Aggregation Control protocol, and configure the potential member ports to the desired Link Aggregation Groups (LAGs) by using the [LAG Management Page](#). By default, all LAGs have no port members.
3. Configure the Ethernet parameters, such as speed and auto negotiation for the Link Aggregation Groups by using the [LAG Settings Page](#).
4. Configure the LACP parameters for the ports that are members or candidates of a Link Aggregation Group by using the [LACP Page](#).

### SETTING THE BASIC PORT CONFIGURATION

The [Port Settings Page](#) displays the global and per port setting of all the ports. This page enables you to select and configure the desired ports from the [Edit Port Settings Page](#).

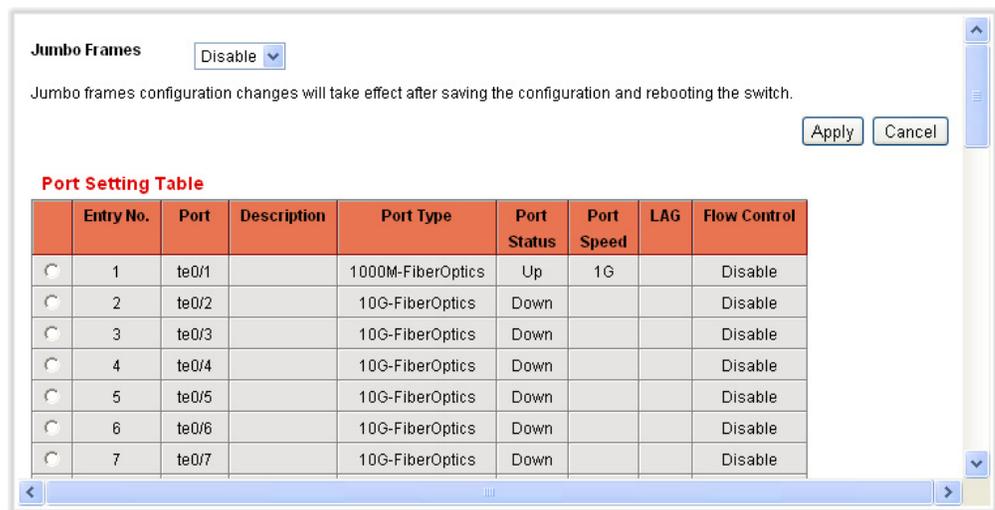


**NOTE:** SFP Fiber takes precedence when both ports are being used.

To configure port settings:

1. Click **Port & VLAN Management > Port Settings**. The [Port Settings Page](#) is displayed.

**Figure 53: Port Settings Page**



2. Enable **Jumbo Frames** to support packets of up to 10 Kb in size. If **Jumbo Frames** is not enabled, the system supports packet size up to 1,632 bytes.

3. Click **Apply** to update the global setting.

Jumbo frames configuration changes take effect *only* after the Running Configuration is explicitly saved to the Startup Configuration File using the [Copying/Saving Configuration Files](#), and the switch is rebooted.

4. To update the port settings, select the desired port, and click **Edit**. The [Edit Port Settings Page](#) is displayed.

**Figure 54: Edit Port Settings Page**

Port	te0/2	Port Type	10G-FiberOptics
Port Description	<input type="text"/>		
Administrative Status	Up	Operational Status	Down
Reactivate Suspended Port	<input type="checkbox"/>		
Administrative Port Speed	10G	Operational Port Speed	
Flow Control	Disable		
Member in LAG			
<input type="button" value="Apply"/>			

5. Modify the following Settings parameters:

- **Port**—Select the port number.
- **Port Description**—Enter the port user-defined name or comment.
- **Port Type**—Displays the port type. The possible options are:
  - *Copper Ports*—Regular, not combo, support the following values: 10M, 100M, 1000M (type: Copper).
  - *Combo Ports Copper*—Combo port connected with copper CAT5 cable, supports the following values: 10M, 100M, 1000M (type: ComboC).
  - *Combo Fiber*—SFP Fiber Gigabit Interface Converter Port with the following values: 100M and 1000M (type: ComboF)
- **Administrative Status**—Select whether the port should be operational (Up) or non-operational (Down) when the switch is rebooted.
- **Operational Status**—Displays the current port connection status.
- **Reactivate Suspended Port**—Select to reactivate a port that has been suspended. There are numerous ways that a port can be suspended, such as through the locked port security option, Access Control List (ACL) configurations, BPDU Guard, or Root-Guard.
- **Administrative Port Speed**—Select the configured rate for the port. The port type determines the speed setting options are available. You can designate *Administrative Speed* only when port auto-negotiation is disabled.
- **Operational Port Speed**—Displays the current port speed that is the result of negotiation.

- **Flow Control**—Enable or disable 802.3x Flow Control, or enable the auto-negotiation of Flow Control on the port (only when in Full Duplex mode).
  - **Member in LAG**—Displays the LAG, if the port is a member of a LAG.
6. Click **Apply**. *The Port Settings* are modified, and the Running Configuration file is updated with the settings.

---

## CONFIGURING LINK AGGREGATION

Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. Link aggregation optimizes port usage by linking multiple ports together to form a Link Aggregation Group (LAG). LAGs multiply the bandwidth, increase port flexibility, and provide link redundancy between two devices.

Two types of LAGs are supported:

- ◆ *Static*—A LAG is static if the LACP (Link Aggregation Control Protocol) is disabled. You configure a static LAG with a group of ports that are always active members of the LAG.
- ◆ *Dynamic*—A LAG is dynamic if it is LACP-enabled. You define a group of ports as candidate ports of a dynamic LAG. The LACP determines which candidate ports from the LAG are active member ports. The non-active member ports are *standby* ports ready to replace any failing active member ports.

### LOAD BALANCING

Traffic forwarded to a LAG is load-balanced across the active member ports, thus achieving an effective bandwidth close to the aggregate bandwidth of all the active member ports of the LAG.

This traffic balancing is managed by a hash-based distribution function that distributes Unicast and Multicast traffic based on packet header information.

The switch support several modes of load balancing:

- ◆ **By MAC Addresses**—Based on the destination and source MAC addresses of all packets.
- ◆ **By IP Address**—Based on source and destination IP addresses on all packets.
- ◆ **By IP and MAC Addresses**—Based on the destination and source IP addresses for IP packets, and destination and source MAC addresses for non-IP packets.

- ◆ Port IP/MAC Address—Based on source and destination Port IP addresses on IP packets, and by the source and destination Port MAC addresses on non-IP packets

## LAG MANAGEMENT

Active member ports in a LAG are defined statically by explicit user assignment or are dynamically selected by the Link Aggregation Control Protocol (LACP). The LACP selection process selects the active member ports for the LAG after exchanging LACP information between the local and remote devices.

In general, a LAG is treated by the system as a single logical port. In particular, the LAG has port attributes similar to a regular port, such as state and speed.

The switch supports eight LAGs.

Every LAG has the following characteristics:

- ◆ All ports in a LAG must be of the same media type.
- ◆ To add a port to the LAG, it cannot belong to any VLAN except the default VLAN.
- ◆ Ports in a LAG must not be assigned to another LAG.
- ◆ No more than eight ports are assigned to a static LAG and no more than 16 ports can be candidates for a dynamic LAG.
- ◆ When a port is added to the original configuration of the LAG, the configuration that existed for the port is no longer applied, and the configuration of the LAG applies to the port. When the port is removed from the LAG, its original configuration is reapplied.
- ◆ Protocols, such as Spanning Tree, consider all the ports in the LAG to be one port.
- ◆ All the ports in the LAG must have the same 802.1p priority.

## STATIC AND DYNAMIC LAG WORKFLOW

To configure a **static** LAG, perform the following actions:

1. Configure the selected LAG as a static LAG by disabling LACP on the LAG. Assign up to eight active member ports to the static LAG by selecting and moving the ports from the **Port List** to the **LAG Members** list by using the [LAG Management Page](#).
2. Configure the LAG speed and flow control by using the [LAG Settings Page](#).

To configure a **dynamic** LAG, perform the following actions:

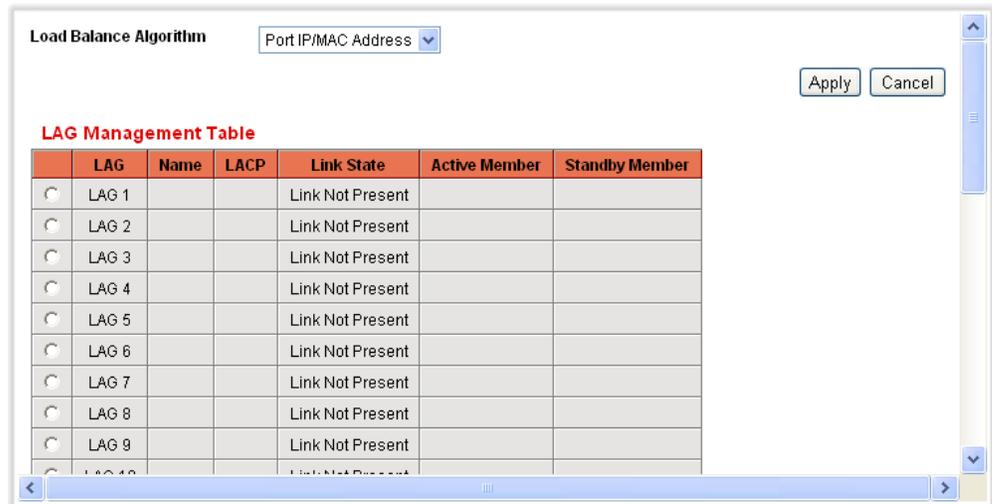
1. Configure the selected LAG as a dynamic LAG by enabling LACP on the LAG. Assign up to 16 candidates ports to the dynamic LAG by selecting and moving the ports from the **Port List** to the **LAG Members List** by using the [LAG Management Page](#).
2. Configure the LAG speed and flow control by using the [LAG Management Page](#).
3. Configure the LACP parameters of the ports in the LAG by using the [LACP Page](#).

**DEFINING LAG MANAGEMENT**

The [LAG Management Page](#) displays the global and per LAG settings. The page also enables you to configure the global setting and to select and edit the desired LAG on the [Edit LAG Membership Page](#).

1. To configure LAG management, click **Port & VLAN Management > Link Aggregation > LAG Management**. The [LAG Management Page](#) is displayed.

**Figure 55: LAG Management Page**



2. Select one of the following **Load Balance Algorithms**:
  - *MAC Address*—Perform loading balancing by source and destination MAC addresses on all packets.
  - *IP Address*—Perform loading balancing by source and destination IP addresses on all packets.
  - *IP/MAC Address*—Perform load balancing by the source and destination IP addresses on IP packets, and by the source and destination MAC addresses on non-IP packets

- *Port IP/MAC Address*—Perform load balancing by the source and destination Port IP addresses on IP packets, and by the source and destination Port MAC addresses on non-IP packets
3. Click **Apply**. The Load Balance Algorithm is defined, and the Running Configuration file is updated with the settings.

**DEFINING MEMBER PORTS IN A LAG**

The [LAG Management Page](#) enables you to define the member ports in a LAG.

Select the LAG to be configured, and click **Edit**. The [Edit LAG Membership Page](#) is displayed.

**Figure 56: Edit LAG Membership Page**



4. Enter the values for the following fields:
- **LAG**—Select the LAG number.
  - **LAG Name**—Enter the LAG name or a comment.
  - **LACP**—Select to enable LACP on the selected LAG. This makes it a dynamic LAG.
  - **Port List**—Move those ports that are to be assigned to the LAG from the **Port List** to the **LAG Members** list. Up to eight ports per static LAG can be assigned, and 16 ports can be assigned to a dynamic LAG.
5. Click **Apply**. The LAG membership is defined, and the Running Configuration file is updated with the settings.

**CONFIGURING LAG SETTINGS** The [LAG Settings Page](#) displays a table of current settings for all LAGs. You can configure the settings of selected LAGs, and reactivate suspended LAGs by launching the [Edit LAG Settings Page](#).

To configure the LAG:

1. Click **Port & VLAN Management > Link Aggregation > LAG Settings**. The [LAG Settings Page](#) is displayed.

**Figure 57: LAG Settings Page**

LAG Setting Table						
Entry No.	LAG	Description	Type	Status	Speed	Flow Control
1	LAG 1					
2	LAG 2					
3	LAG 3					
4	LAG 4					
5	LAG 5					
6	LAG 6					
7	LAG 7					
8	LAG 8					
9	LAG 9					
10	LAG 10					

2. Select a LAG, and click **Edit**. The [Edit LAG Settings Page](#) is displayed.

**Figure 58: Edit LAG Settings Page**

LAG	1	LAG Type
Description	<input type="text"/>	
Administrative Status	Up	Operational Status
Reactivate Suspended LAG	<input type="checkbox"/>	
Administrative Speed	1G	Operational LAG Speed
Administrative Flow Control	Disable	Operational Flow Control
<input type="button" value="Apply"/>		

3. Enter the values for the following fields:
  - **LAG**—Select the LAG ID number.
  - **Description**—Enter the LAG name or a comment.
  - **LAG Type**—Displays the port type that comprises the LAG.
  - **Administrative Status**—Set the selected LAG to operational (Up) or non-operational (Down).

- **Operational Status**—Displays whether the LAG is currently operating.
  - **Reactivate Suspended LAG**—Select to reactivate a port if the LAG has been disabled through the locked port security option or through the ACL configurations.
  - **Administrative Speed**—Select the LAG speed.
  - **Operational LAG Speed**—Displays the current speed at which the LAG is operating.
  - **Administrative Flow Control**—Enable or disable Flow Control or enable the auto-negotiation of Flow Control on the LAG.
  - **Operational Flow Control**—Displays the current Flow Control setting.
4. Click **Apply**. The Running Configuration file is updated with the settings.

**CONFIGURING LACP** A dynamic LAG is LACP-enabled; the Link Aggregation Control Protocol is run on every candidate port defined in the LAG.

LACP system priority and LACP port priority determine which of the candidate ports become active member ports in a dynamic LAG configured with more than eight candidate ports. The selected candidate ports of the LAG are all connected to the same remote device.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel-group, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other switch (the non-controlling end of the link) are ignored.

The LACP priority is taken either from the local or the remote device according to the following rule: The local LACP System Priority is compared to the remote LACP System Priority device. The lowest priority is used. If both priorities are the same, the local and remote MAC addresses are compared. The priority of the device with the lowest MAC address is used.

The additional rules in selecting the active or standby ports in a dynamic LACP are as follows:

- ◆ Any link operating at a different speed from the highest-speed active member or operating at half-duplex is made standby. All the active ports in a dynamic LAG operate at the same baud rate.
- ◆ If the port LACP priority of the link is lower than that of the currently-active link members, and the number of active members is already at

the maximum number, the link is made inactive, and placed in standby mode.

### SETTING PORT LACP PARAMETER SETTINGS

The [LACP Page](#) displays and enables configuration of the LACP System Priority, LACP timeout, and LACP port priority. LACP timeout is a per port parameter, and is the time interval between the sending and receiving of consecutive LACP PDUs. With all factors equal, when the LAG is configured with more candidate ports than the maximum number of active ports allowed, the switch selects ports as active from the dynamic LAG that has the highest priority.

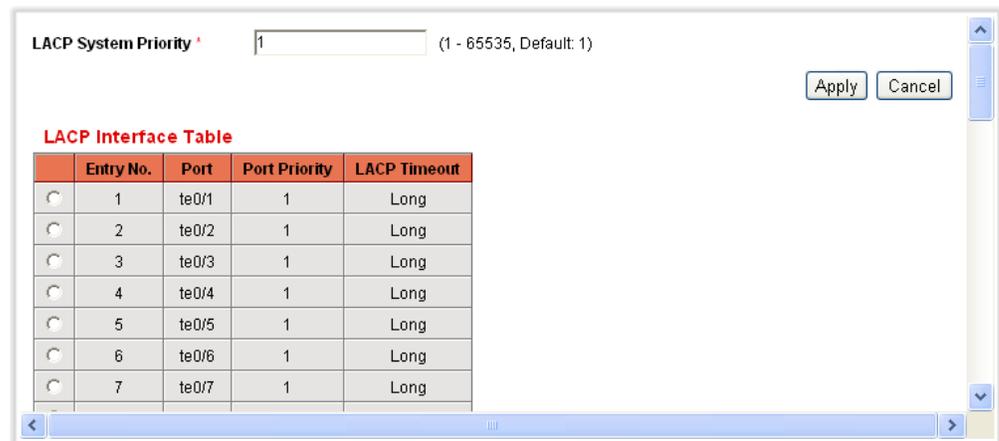


**NOTE:** The LACP setting is irrelevant on ports that are not members of a dynamic LAG.

To define the LACP settings:

1. Click **Port & VLAN Management > Link Aggregation > LACP**. The [LACP Page](#) is displayed.

**Figure 59: LACP Page**



2. Enter the global **LACP System Priority** value that determines which candidate ports will become members of the LAG.

The page displays the LACP settings of every port.

3. Select a port, and click **Edit**. The [Edit LACP Page](#) is displayed.

Figure 60: Edit LACP Page

Port	te0/2
LACP Port Priority *	1 (1 - 65535, Default: 1)
LACP Timeout	Long

Apply

4. Enter the values for the following fields:
  - **Port**—Select the port number to which timeout and priority values are assigned.
  - **LACP Port Priority**—Enter the LACP priority value for the port.
  - **LACP Timeout**—Select the periodic transmissions of LACP PDUs occur at either a slow or fast transmission rate, depending upon the expressed LACP timeout preference.
5. Click **Apply**. The Running Configuration file is updated with the settings.

---

## CONFIGURING VLANS

A VLAN is a logical group that enables devices connected to the VLAN to communicate with each other over the Ethernet MAC layer, regardless of the physical LAN segment of the bridged network to which they are connected.

Each VLAN is configured with a unique VID (VLAN ID) with a value from 1 to 4094. A port on a device in a bridged network is a member of a VLAN if it can send data to and receive data from the VLAN. A port is an untagged member of a VLAN if all packets destined for that port into the VLAN have no VLAN tag. A port is a tagged member of a VLAN if all packets destined for that port into the VLAN have a VLAN tag. A port can be a member of one or more VLANs.

A port in VLAN Access mode can be part of only one VLAN. If it is in General or Trunk mode, the port can be part of one or more VLANs.

VLANs address security and scalability issues. Traffic from a VLAN stays within the VLAN, and terminates at devices in the VLAN. It also eases network configuration by logically connecting devices without physically relocating those devices.

If a frame is VLAN-tagged, a four-byte VLAN tag is added to each Ethernet frame, increasing the maximum frame size from 1518 to 1522. The tag contains a VLAN ID between 1 and 4094, and a VLAN Priority Tag (VPT) between 0 and 7. See "[QoS Features and Components](#)" on page 299 for details about VPT.

When a frame enters a VLAN-aware device, it is classified as belonging to a VLAN, based on the four-byte VLAN tag in the frame.

If there is no VLAN tag in the frame or the frame is priority-tagged only, the frame is classified to the VLAN based on the PVID (Port VLAN Identifier) configured at the ingress port where the frame is received.

The frame is discarded at the ingress port if Ingress Filtering is enabled and the ingress port is not a member of the VLAN to which the packet belongs. A frame is regarded as priority-tagged only if the VID in its VLAN tag is 0.

Frames belonging to a VLAN remain within the VLAN. This is achieved by sending or forwarding a frame only to egress ports that are members of the target VLAN. An egress port may be a tagged or untagged member of a VLAN.

The egress port:

- ◆ Adds a VLAN tag to the frame if the egress port is a tagged member of the target VLAN, and the original frame does not have a VLAN tag.
- ◆ Removes the VLAN tag from the frame if the egress port is an untagged member of the target VLAN, and the original frame has a VLAN tag.

## VLAN ROLES

VLANs function at Layer 2. All VLAN traffic (Unicast/Broadcast/Multicast) remains within its VLAN. Devices attached to different VLANs do not have direct connectivity to each other over the Ethernet MAC layer. Devices from different VLANs can communicate with each other only through Layer 3 routers. An IP router, for example, is required to route IP traffic between VLANs if each VLAN represents an IP subnet.

The IP router might be a traditional router, where each of its interfaces connects to only one VLAN. Traffic to and from a traditional IP router must be VLAN untagged. The IP router can be a VLAN-aware router, where each of its interfaces can connect to one or more VLANs. Traffic to and from a VLAN-aware IP router can be VLAN tagged or untagged.

Adjacent VLAN-aware devices exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). As a result, VLAN information is propagated through a bridged network.

VLANs on a device can be created statically or dynamically, based on the GVRP information exchanged by devices. A VLAN can be static or dynamic (from GVRP), but not both. For more information about GVRP, refer to the [Defining GVRP Settings](#) section.

## VLAN CONFIGURATION WORKFLOW

To configure VLANs:

1. Create the required VLANs by using the [Creating VLANs](#) section.

2. Set the desired per port VLAN-related configuration using the [Configuring VLAN Interface Settings](#) section.
3. Assign interfaces to VLANs by using the [Configuring Port to VLAN](#) section
4. You can view the current VLAN port membership for all the interfaces in the [Viewing VLAN Membership](#) section.

## CREATING VLANS

You can create a VLAN, but this has no effect until the VLAN is attached to at least one port, either manually or dynamically. Ports must always belong to one or more VLANs. The switch supports 256 VLANs, including the default VLAN.

Each VLAN must be configured with a unique VID (VLAN ID) with a value from 1 to 4094. The switch reserves VID 4095 as the Discard VLAN. All packets classified to the Discard VLAN are discarded at ingress, and are never forwarded to a port.

To create a VLAN:

1. Click **Port & VLAN Management > VLAN Settings > Create VLAN**. The [Create VLAN Page](#) is displayed.

**Figure 61: Create VLAN Page**

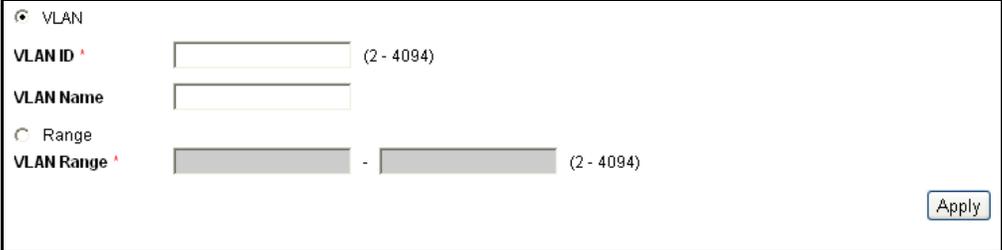
VLAN Table			
<input type="checkbox"/>	VLAN ID	VLAN Name	Type
<input type="checkbox"/>	1		Default

The Create VLAN page displays the following fields for all VLANs:

- ◆ **VLAN ID**—User-defined VLAN ID.
- ◆ **VLAN Name**—User-defined VLAN name.
- ◆ **Type**—VLAN type. The possible options are:
  - *Dynamic*—VLAN was dynamically created through Generic VLAN Registration Protocol (GVRP).
  - *Static*—VLAN is user-defined.
  - *Default*—VLAN is the default VLAN.

2. Click **Add** to add a new VLAN or select an existing VLAN and click **Edit** to modify the VLAN parameters. The [Add/Edit VLAN Page](#) is displayed.

**Figure 62: Add/Edit VLAN Page**



The screenshot shows a configuration form for VLANs. At the top left, there is a radio button labeled 'VLAN' which is selected. Below it are two text input fields: 'VLAN ID' with a range '(2 - 4094)' and 'VLAN Name'. Below these is another radio button labeled 'Range' which is not selected. Below that is a range input field for 'VLAN Range' with a range '(2 - 4094)'. In the bottom right corner, there is an 'Apply' button.

The page enables the creation of either a single VLAN or a range of VLANs.

3. To create a single VLAN, select **VLAN**, enter the **VLAN ID** (VID), and optionally the **VLAN Name**.
4. To create a range of VLANs, select **Range**, and specify the range of VLANs to be created by entering the Starting VID and Ending VID, inclusive.
5. Click **Apply** to create the VLANs. The Running Configuration file is updated with the settings.

---

## CONFIGURING VLAN INTERFACE SETTINGS

The [Interface Settings Page](#) displays and enables configuration of VLAN-related parameters for all interfaces. The switch supports 256 VLANs; default VLAN included.

To configure the VLAN settings:

1. Click **Port & VLAN Management > VLAN Settings > Interface Settings**. The [Interface Settings Page](#) is displayed.

**Figure 63: Interface Settings Page**

Interface Setting Table						
Interface Type: Port						
	Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering
<input type="radio"/>	1	te0/1	Access	1	Admit All	Enabled
<input type="radio"/>	2	te0/2	Access	1	Admit All	Enabled
<input type="radio"/>	3	te0/3	Access	1	Admit All	Enabled
<input type="radio"/>	4	te0/4	Access	1	Admit All	Enabled
<input type="radio"/>	5	te0/5	Access	1	Admit All	Enabled
<input type="radio"/>	6	te0/6	Access	1	Admit All	Enabled
<input type="radio"/>	7	te0/7	Access	1	Admit All	Enabled
<input type="radio"/>	8	te0/8	Access	1	Admit All	Enabled
<input type="radio"/>	9	te0/9	Access	1	Admit All	Enabled

The Interface Settings page lists all ports or LAGs and their VLAN parameters.

2. Select an interface type (Port or LAG).
3. Select a port or LAG, and click **Edit**. The [Edit Interface Setting Page](#) is displayed.

**Figure 64: Edit Interface Setting Page**

**Interface**  Port **te0/3**  LAG **1**  
**Interface VLAN Mode** **Access**  
**Administrative PVID \***  (1 - 4094, Default: 1)  
**Frame Type** **Admit All**  
**Ingress Filtering** **Enable**

4. Enter the values for the following fields:
  - ◆ **Interface**—Select a port/LAG.
  - ◆ **Interface VLAN Mode**—Select the interface mode for the VLAN. The options are:
    - *General*—The interface can support all functions as defined in the IEEE 802.1q specification. The interface can be a tagged or untagged member of one or more VLANs.
    - *Access*—The interface is an untagged member of a single VLAN. A port configured in this mode is known as an access port.

- *Trunk*—The interface is an untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. A port configured in this mode is known as a trunk port.
  - *Customer*—When a port is in Customer mode, an added tag provides a VLAN ID to each customer, ensuring private and segregated network traffic for that customer.
  - ◆ **Administrative PVID**—Enter the Port VLAN ID (PVID) of the VLAN to which incoming untagged and priority tagged frames are classified. The possible values are 1 to 4094.
  - ◆ **Frame Type**—Select the type of frame that the interface can receive. Frames that are not of the configured frame type are discarded at ingress. These frame types are only available in General mode. Possible values are:
    - *Admit All*—The interface accepts all types of frames: untagged frames, tagged frames, and priority tagged frames.
    - *Admit Tagged Only*—The interface accepts only tagged frames.
    - *Admit Untagged Only*—The interface accepts only untagged and priority frames.
  - ◆ **Ingress Filtering**—(Available only in General mode) Select to enable ingress filtering. When an interface is ingress filtering enabled, the interface discards all incoming frames that are classified as VLANs of which the interface is not a member. Ingress filtering can be disabled or enabled on general ports. It is always enabled on access ports and trunk ports.
5. Click **Apply**. The parameters are set, and the Running Configuration file is updated with the settings.

---

## DEFINING VLAN MEMBERSHIP

The [Port to VLAN Page](#) and [Port VLAN Membership Page](#) display the VLAN memberships of the ports in various presentations. You can use the [Port to VLAN Page](#) to add or remove memberships to or from the VLANs.

When a port is forbidden default VLAN membership, that port is not allowed membership in any other VLAN. An internal VID of 4095 is assigned to the port.

To forward the packets properly, intermediate VLAN-aware devices that carry VLAN traffic along the path between end nodes, must either be manually configured or must dynamically learn the VLANs and their port memberships from Generic VLAN Registration Protocol (GVRP).

Untagged port membership between two VLAN-aware devices with no intervening VLAN-aware devices, should be to the same VLAN. In other

words, the PVID on the ports between the two devices must be the same if the ports are to send and receive untagged packets to and from the VLAN. Otherwise, traffic might leak from one VLAN to another.

VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices. If a destination end node is VLAN-unaware, but is to receive traffic from a VLAN, then the last VLAN-aware device (if there is one), must send frames of the destination VLAN to the end node untagged. That is, the egress port that reaches the end node must be an untagged member of the VLAN.

**CONFIGURING PORT TO VLAN**

Use the *Port to VLAN Page* to display and configure a VLAN and all its port members on a single page.

To map ports or LAGs to a VLAN:

1. Click **Port & VLAN Management > VLAN Settings > Port to VLAN**. The [Port to VLAN Page](#) is displayed.

**Figure 65: Port to VLAN Page**



2. Select a **VLAN ID** and the **Interface Type** (Port or LAG), to display or to change the port characteristic with respect to the VLAN.

The port mode for each port or LAG is displayed with its current port mode (Access, Trunk or General) configured on the [Interface Settings Page](#). Each port or LAG is displayed with its current registration to the VLAN.

3. Change the registration of an interface to the VLAN by selecting the desired option from the following list:
  - **Forbidden**—The interface is not allowed to join the VLAN even from GVRP registration. When a port is not a member of any other VLAN,

enabling this option on the port makes the port part of internal VLAN 4095 (a reserved VID).

- **Excluded**—The interface is currently not a member of the VLAN. This is the default for all the ports and LAGs. The port can join the VLAN through GVRP registration.
  - **Tagged**—The interface is a tagged member of the VLAN. Frames of the VLAN are sent tagged to the interface VLAN.
  - **Untagged**—The interface is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the interface VLAN.
  - **PVID**—Select to set the PVID of the interface to the VID of the VLAN. PVID is a per-port setting.
4. Click **Apply**. The interfaces are assigned to the VLAN, and the Running Configuration file is updated with the settings.

**VIEWING VLAN MEMBERSHIP**

The [Port VLAN Membership Page](#) displays a list of VLANs to which each port belongs. If the port-based authentication method for an interface is 802.1x and the Administrative Port Control is Auto, then:

- ◆ Until the port is authenticated, it is excluded from all VLANs, except guest and unauthenticated ones. In the VLAN to Port page, the port will be marked with “P”.
- ◆ When the port is authenticated, it receives membership in the VLAN in which it was configured.

To view VLAN membership:

1. Click **Port & VLAN Management > VLAN Settings > Port VLAN Membership**. The [Port VLAN Membership Page](#) is displayed.

**Figure 66: Port VLAN Membership Page**

The screenshot shows a web interface titled "Port VLAN Membership Table". At the top, there is a dropdown menu for "Interface Type" set to "Port". Below this is a table with the following data:

Port	Mode	PVID	Operational VLANs
te0/1	Access	1	1U
te0/2	Access	1	1U
te0/3	Access	1	1U
te0/4	Access	1	1U
te0/5	Access	1	1U
te0/6	Access	1	1U
te0/7	Access	1	1U
te0/8	Access	1	1U
te0/9	Access	1	1U
te0/10	Access	1	1U

2. Select an interface type (Port or LAG).

The Port VLAN Membership page displays the operational membership of the ports or LAGs:

- **Port** number.
- **Mode**—Port mode defined in the [Interface Settings Page](#).
- **PVID**—Port VLAN Identifier of the VLAN to which incoming untagged frames are assigned at ingress. This assumes that no other VLAN assignment mechanism is used, such as MAC-based-VLAN.
- **VLANs**—VLAN to which the port belongs.

---

## CONFIGURING PORT AND VLAN MIRRORING

Port Mirroring is used on a network switch to send a copy of network packets seen on one switch port, multiple switch ports, or an entire VLAN to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system. A network analyzer connected to the monitoring port displays the data packets for diagnosing, debugging, and performance monitoring. Up to eight sources can be mirrored. This can be any combination of eight individual ports and/or VLANs.

A packet that is received on a network port assigned to a VLAN that is subject to mirroring, is mirrored to the analyzer port even if the packet was eventually trapped or discarded. Packets sent by the switch are mirrored when Transmit (Tx) Mirroring is activated.

Mirroring does not guarantee that all traffic from the source port(s) is received on the analyzer (destination) port. If more data is sent to the analyzer port than it can support, some data might be lost.

VLAN mirroring is not active on a VLAN that was not created. For example, if VLAN 23 was created by GVRP and later on removed from the VLAN database for any reason and you manually created VLAN 34, and you create port mirroring that includes VLAN 23, VLAN 34, or both, and later on delete VLAN 34, the status in port mirroring is set to **Not Ready**, because the VLANs are no longer in the database.

Only one instance of mirroring is supported system-wide. The analyzer port (or target port for VLAN mirroring or port mirroring) is the same for all the mirrored VLANs or mirrored ports.

To enable port and VLAN mirroring:

1. Click **Port & VLAN Management** > **Port and VLAN Mirroring**. The [Port and VLAN Mirroring Page](#) is displayed.

Figure 67: Port and VLAN Mirroring Page



This page displays the following fields:

- ◆ **Destination Port**—Port to which traffic is to be copied; the analyzer port.
  - ◆ **Source Interface**—Interface, port, or VLAN, from which traffic is sent to the analyzer port.
  - ◆ **Type**—Type of monitoring: incoming to the port, outgoing from the port, or both.
  - ◆ **Status**—Whether the interface is up or down.
2. Click **Add** to add a port or VLAN to be mirrored. The [Add Port/VLAN Mirroring Page](#) is displayed.

Figure 68: Add Port/VLAN Mirroring Page



3. Enter the parameters:
- **Destination Port**—Select the analyzer port to where packets are copied. A network analyzer, such as a PC running Wireshark, is connected to this port. A port identified as an analyzer destination port, it remains the analyzer destination port until all the entries are removed.
  - **Source Interface**—Select Port or VLAN as the source port or source VLAN from where traffic is to be mirrored.
  - **Type**—Select whether incoming, outgoing, or both types of traffic are mirrored to the analyzer port. If **Port** is selected, the options are:
    - *Rx Only*—Port mirroring on incoming packets.

- *Tx Only*—Port mirroring on outgoing packets.
  - *Tx and Rx*—Port mirroring on both incoming and outgoing packets.
4. Click **Apply**. Port mirroring is added, and the Running Configuration file is updated with the settings.

## DEFINING GVRP SETTINGS

Adjacent VLAN-aware devices can exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network.

Since GVRP requires support for tagging, the port must be configured in Trunk mode or General mode.

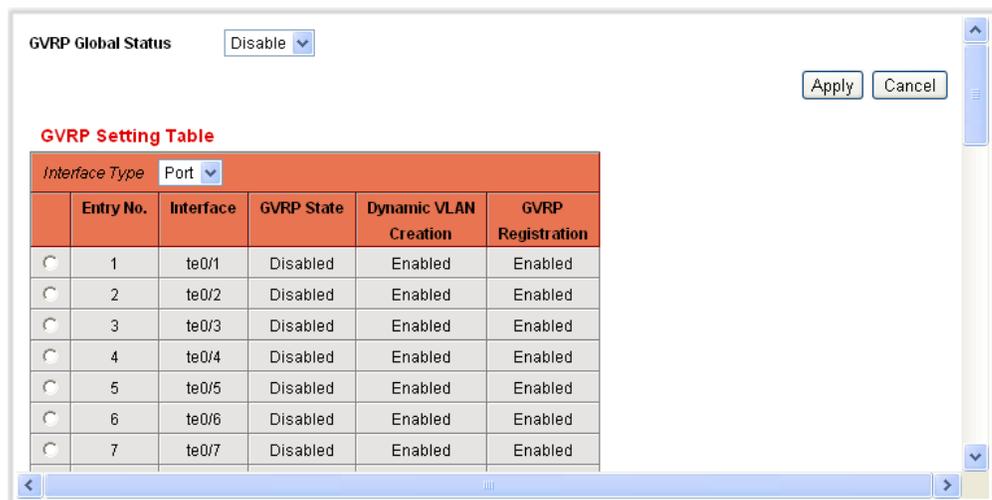
When a port joins a VLAN by using GVRP, it is added to the VLAN as a dynamic member. If the VLAN does not exist, it is dynamically created when Dynamic VLAN creation is enabled for this port.

GVRP must be activated globally as well as on each port. When it is activated, it transmits and receives GARP Packet Data Units (GPDUs). VLANs that are defined but not active are not propagated. To propagate the VLAN, it must be up on at least one port.

To define GVRP settings for an interface:

1. Click **Port & VLAN Management > GVRP Settings**. The [GVRP Settings Page](#) is displayed.

**Figure 69: GVRP Settings Page**



2. Enable or disable the **GVRP Global Status**.

3. Click **Apply** to set the global GVRP status.
4. Select an interface type (Port or LAG). The following fields are displayed in the GVRP Setting Table.
  - **Interface**—Port or LAG number.
  - **GVRP State**—Displays whether GVRP is enabled/disabled on the interface.
  - **Dynamic VLAN Creation**—Displays whether Dynamic VLAN creation is enabled/disabled on the interface. If it is disabled, GVRP can operate but new VLANs are not created.
  - **GVRP Registration**—Displays whether VLAN registration through GVRP is enabled/disabled on the port.
5. To define GVRP settings for a port, select it, and click **Edit**. The [Edit GVRP Setting Page](#) is displayed.

**Figure 70: Edit GVRP Setting Page**

Interface	<input checked="" type="radio"/> Port <input type="radio"/> LAG
	te0/3
GVRP State	Disable
Dynamic VLAN Creation	Enable
GVRP Registration	Enable
<input type="button" value="Apply"/>	

6. Enter the values for the following fields:
  - **Interface**—Select the interface (Port or LAG) to be edited.
  - **GVRP State**—Select to enable GVRP on this interface.
  - **Dynamic VLAN Creation**—Select to enable Dynamic VLAN Creation on this interface.
  - **GVRP Registration**—Select to enable VLAN Registration using GVRP on this interface.
7. Click **Apply**. GVRP settings are modified, and the Running Configuration file is updated with the settings.

---

## MANAGING VLAN GROUPS

VLAN assignment can be done through several classifications. If several classifications schemes are activated, packets would be classified to a VLAN according to the following precedence:

- ◆ TAG: If the packet is tagged, the VLAN would be taken from the tag.

- ◆ MAC-Based VLAN: VLAN is taken from the Source MAC-to-VLAN mapping of the ingress interface.
- ◆ Subnet-Based VLAN: VLAN is taken from the Source IP Subnet-to-VLAN mapping of the ingress interface.
- ◆ Protocol-Based VLAN: VLAN is taken from the (Ethernet type) Protocol-to-VLAN mapping of the ingress interface.
- ◆ PVID: VLAN is taken from the Port default VLAN ID

### ASSIGNING MAC-BASED GROUPS

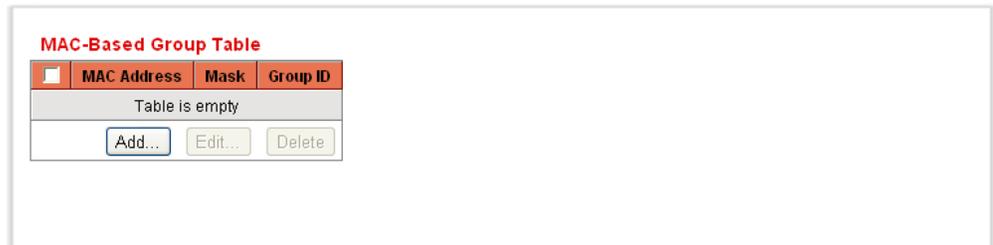
Use this feature to assign untagged traffic from specific MAC addresses to a specific VLAN. You can define several MAC-based VLAN groups. This assignment is performed in stages:

1. Assign the MAC address to a Group ID (an identifier created by using the [MAC-Based Groups Page](#)).
2. For each interface, assign the VLAN group to a VLAN by using [Mapping Group to VLAN Page](#). (The interfaces must be in General mode.)

To assign a MAC address to a VLAN Group:

1. Click **Port & VLAN Management > VLAN Groups > MAC-Based Groups**. The [MAC-Based Groups Page](#) is displayed.

**Figure 71: MAC-Based Groups Page**



2. Click **Add**. The [Add MAC-Based Group Page](#) is displayed.

**Figure 72: Add MAC-Based Group Page**

MAC Address \*

Mask \*  Host  Prefix

Group ID \*

3. Enter the values for the following fields:

- **MAC Address**—Enter a MAC address to be assigned to a VLAN group.



**NOTE:** This MAC address cannot be assigned to any other VLAN group.

- **Mask**—Enter one of the following:
  - *Host*—Source host of the MAC address
  - *Prefix* of the MAC address
- **Group ID**—Enter a user-created VLAN group ID number. Range is 1-2147483647.

4. Click **Apply**. The MAC address is assigned to a VLAN group and the Running Configuration file is updated with the settings.

### ASSIGNING SUBNET-BASED GROUPS

Use this feature to assign untagged traffic from specific subnets to a specific VLAN. You can define several subnet-based VLAN groups. This assignment is performed in stages:

1. Assign the subnet to a Group ID (an identifier created by using the [Add Subnet-Based Group Page](#)).
2. For each interface, assign the VLAN group to a VLAN by using [Mapping Group to VLAN Page](#). (The interface must be in General mode.)

To assign a subnet to a VLAN Group:

1. Click **VLAN Management > VLAN Groups > Subnet-Based Group**. The [Subnet-Based Groups Page](#) is displayed.

**Figure 73: Subnet-Based Groups Page**

IP Address	Prefix	Group ID
Table is empty		

Buttons: Add... Edit... Delete

The [Subnet-Based Groups Page](#) contains the following fields:

- ◆ **IP Address**—Displays the IP address.
- ◆ **Prefix**—Displays the subnet prefix

- ◆ **Subnet Group ID (Hex)**—Defines the subnet group ID to which the interface is added. Range is 1-2147483647.
2. Click **Add**. The [Add Subnet-Based Group Page](#) is displayed.

**Figure 74: Add Subnet-Based Group Page**

The screenshot shows a form with three input fields: "IP Address", "Prefix", and "Subnet Group ID". The "Subnet Group ID" field has a range of "1 - 2147483647" next to it. An "Apply" button is located at the bottom right of the form.

3. Define the relevant fields.
4. Click **Apply**. The Protocol Group is added, and the Running Configuration file is updated with the settings.

**ASSIGNING  
PROTOCOL-BASED  
GROUPS**

Use this feature to assign untagged traffic from specific protocols to a specific VLAN. You can define several protocol-based VLAN groups. This assignment is performed in stages:

1. Assign the subnet to a Group ID (an identifier created by using the [Add Protocol-Based Group Page](#)).
2. For each interface, assign the VLAN group to a VLAN by using [Mapping Group to VLAN Page](#). (The interface must be in General mode and not have DVA configured on it.)

To assign a protocol to a VLAN Group:

1. Click **VLAN Management > VLAN Groups > Protocol-Based Group**. The [Protocol-Based Groups Page](#) is displayed.

**Figure 75: Protocol-Based Groups Page**

The screenshot shows a table titled "Protocol-Based Group Table" with the following columns: "Frame Type", "Protocol Value", and "Group ID". The table is currently empty, and there are "Add..." and "Delete" buttons below it.

Frame Type	Protocol Value	Group ID
Table is empty		

The [Protocol-Based Groups Page](#) contains the following fields:

- ◆ **Frame Type**—Displays the frame type. The possible types are Ethernet, RFC1042, LLC Other.

- ◆ **Protocol Value**—Displays the protocol value. The possible values are
    - *Protocol Value*—The possible values are IP, IPX, IPv6, or ARP.
    - *Ethernet-Based Protocol Value*—Specify the value in hexadecimal format.
  - ◆ **Group ID (Hex)**—Defines the Protocol group ID to which the interface is added. Range is 1-2147483647.
2. Click **Add**. The [Add Protocol-Based Group Page](#) is displayed.

**Figure 76: Add Protocol-Based Group Page**

Frame Type: Ethernet

Protocol Value \*  
 Protocol Value IP  
 Ethernet-Based Protocol Value (0x0600-0xFFFF)

Group ID \*  
(1 - 2147483647)

Apply

3. Define the relevant fields.
4. Click **Apply**. The Protocol Group is added, and the Running Configuration file is updated with the settings.

**MAPPING VLAN GROUP TO VLAN** The [Mapping Group to VLAN Page](#) displays the groups created in the [MAC-Based Groups Page](#), [Protocol-Based Groups Page](#).

To assign a VLAN group ID to a VLAN per interface.

1. Click **Port & VLAN Management > VLAN Groups > Mapping Group to VLAN**. The [Mapping Group to VLAN Page](#) is displayed.

**Figure 77: Mapping Group to VLAN Page**

Mapping Group to VLAN Table

Group Type: MAC-Based

Interface	Group ID	VLAN ID
Table is empty		

Add... Edit... Delete

The window displays:

- ◆ **Interface**—Type of interface (Port or LAG), through which traffic is received for this group.

- ◆ **Group ID**—VLAN group defined in the [MAC-Based Groups Page](#), [Subnet-Based Groups Page](#), or [Protocol-Based Groups Page](#).
  - ◆ **VLAN ID**—Traffic is forwarded from the VLAN group to this VLAN.
2. Click **Add**. The [Add Mapping Group to VLAN Page](#) is displayed. (The interface must be in General mode.)

**Figure 78: Add Mapping Group to VLAN Page**

3. Enter the values for the following fields:
  - ◆ **Group Type**—Displays the group type (MAC-Based, Subnet-Based, or Protocol-Based).
  - ◆ **Interface**—Enter an interface (Port or LAG) through which traffic is received.
  - ◆ **Group ID**—Select one of the VLAN groups defined in the [MAC-Based Groups Page](#), [Subnet-Based Groups Page](#), or [Protocol-Based Groups Page](#).
  - ◆ **VLAN ID**—Select the VLAN to where traffic from the VLAN group is forwarded.



**NOTE:** For each interface, you can select any group and VLAN.

4. Click **Apply**. The Running Configuration file is updated with the settings.



# CONFIGURING THE SPANNING TREE PROTOCOL

The Spanning Tree Protocol (STP) (IEEE802.1D and IEEE802.1Q) is enabled by default, set to RSTP (Rapid Spanning Tree Protocol) mode, and protects a Layer 2 Broadcast domain from broadcast storms by selectively setting links to standby mode to prevent loops. In standby mode, these links temporarily do not transfer user data. They are automatically re-activated when the topology changes to make it desirable to transfer user data.

This chapter contains the following topics:

- ◆ [STP Flavors](#)
- ◆ [Configuring STP Global Settings](#)
- ◆ [Defining STP Interface Settings](#)
- ◆ [Configuring RSTP Settings](#)
- ◆ [Multiple Spanning Tree Protocol Overview](#)
- ◆ [Defining MSTP Properties](#)
- ◆ [Mapping VLANs to an MST Instance](#)
- ◆ [Defining MST Instance Settings](#)
- ◆ [Defining MSTP Interface Settings](#)

---

## STP FLAVORS

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause switches to forward traffic indefinitely, resulting in increased traffic and reduced network efficiency.

STP provides a tree topology for any arrangement of switches and interconnecting links, creating a unique path between end stations on a network, eliminating loops.

The switch supports the following Spanning Tree Protocol versions:

- ◆ Classic STP provides a single path between any two end stations, avoiding and eliminating loops.

- ◆ Rapid STP (RSTP) detects network topologies to provide faster convergence of the spanning tree. This is most effective when the network topology is naturally tree-structured, and therefore faster convergence might be possible. RSTP is enabled by default.

Although Classic STP is guaranteed to prevent forwarding loops in a general network topology, there might be an unacceptable delay before convergence. This means that each bridge or switch in the network needs to decide, if it should actively forward traffic or not on each of its ports.

## CONFIGURING STP GLOBAL SETTINGS

The [STP Global Settings Page](#) contains parameters for enabling STP, RSTP, or MSTP.

Use the [STP Interface Settings Page](#), [RSTP Interface Settings Page](#), and [MST Interface Settings Page](#) to *configure each mode*, respectively.

To set STP status and global settings:

1. Click **Spanning Tree > STP Global Settings**. The [STP Global Settings Page](#) is displayed.

Figure 79: STP Global Settings Page

STP Global Settings	
Spanning Tree State	Enabled
STP Operation Mode	Rapid STP
BPDU Handling	Flooding
Path Cost Default Values	Long

Bridge Settings	
Priority *	32768 (0 - 61440, Default: 32768)
Hello Time *	2 sec. (1 - 10, Default: 2)
Max Age *	20 sec. (6 - 40, Default: 20)
Forward Delay *	15 sec. (4 - 30, Default: 15)

Designated Root	
Bridge ID	32768-00:11:22:33:44:55
Root Bridge ID	32768-00:11:22:33:44:55
Root Port	0
Root Path Cost	0
Topology Changes Counts	1
Last Topology Change	0D/3H/17M/47S

2. Enter the parameters:

Global Settings:

- **Spanning Tree State**—Enable or disable STP on the switch.
- **STP Operation Mode**—Select an STP mode.
- **BPDU Handling**—Select how Bridge Protocol Data Unit (BPDU) packets are managed when STP is disabled on the port or the switch. BPDUs are used to transmit spanning tree information.
  - *Filtering*—Filters BPDU packets when Spanning Tree is disabled on an interface.
  - *Flooding*—Floods BPDU packets when Spanning Tree is disabled on an interface.
- **Path Cost Default Values**—Selects the method used to assign default path costs to the STP ports. The default path cost assigned to an interface varies according to the selected method.
  - *Short*—Specifies that the default port path costs are within the range:  
1–65,535.
  - *Long*—Specifies that the default port path costs are within the range:  
1–200,000,000.

Bridge Settings:

- **Priority**—Sets the bridge priority value. After exchanging BPDUs, the device with the lowest priority becomes the Root Bridge. In the case that all bridges use the same priority, then their MAC addresses are used to determine which is the Root Bridge. The bridge priority value is provided in increments of 4096. For example, 4096, 8192, 12288, and so on.
- **Hello Time**—Set the interval in seconds that a Root Bridge waits between configuration messages. The range is 1 to 10 seconds.
- **Max Age**—Set the interval in seconds that the switch can wait without receiving a configuration message, before attempting to redefine its own configuration.
- **Forward Delay**—Set the interval in seconds that a bridge remains in a learning state before forwarding packets. For more information, refer to [Defining STP Interface Settings](#).

Designated Root:

- **Bridge ID**—The bridge priority concatenated with the MAC address of the switch.
- **Root Bridge ID**—The Root Bridge priority concatenated with the MAC address of the Root Bridge.

- **Root Port**—The port that offers the lowest cost path from this bridge to the Root Bridge. (This is significant when the bridge is not the root.)
  - **Root Path Cost**—The cost of the path from this bridge to the root.
  - **Topology Changes Counts**—The total number of STP topology changes that have occurred.
  - **Last Topology Change**—The time interval that elapsed since the last topology change occurred. The time is displayed in a days/hours/minutes/seconds format.
3. Click **Apply**. The Running Configuration file is updated with the settings.

## DEFINING STP INTERFACE SETTINGS

The [STP Interface Settings Page](#) enables you to configure STP on a per-port basis, and to view the information learned by the protocol, such as the designated bridge.

The configuration entered on this page is active for all flavors of the STP protocol.

To configure STP on an interface:

1. Click **Spanning Tree > STP Interface Settings**. The [STP Interface Settings Page](#) is displayed.

**Figure 80: STP Interface Settings Page**

STP Interface Setting Table											
										Interface Type	Port
Entry No.	Interface	STP	Edge Port	Root Guard	BPDU Guard	BPDU Handling	Port Role	Path Cost	Priority	Port State	
1	te0/1	Enabled	Disabled	Disabled	Disabled	STP	Designated	20000	128	Forwarding	
2	te0/2	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	
3	te0/3	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	
4	te0/4	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	
5	te0/5	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	
6	te0/6	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	
7	te0/7	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	
8	te0/8	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	
9	te0/9	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	
10	te0/10	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	
11	te0/11	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	

2. Select an interface and click **Edit**. The [Edit Interface Settings Page](#) is displayed.

**Figure 81: Edit Interface Settings Page**

Interface	<input checked="" type="radio"/> Port <span>te0/3</span> <input type="radio"/> LAG <span>1</span>
STP	<span>Enabled</span>
Edge Port	<span>Disable</span>
Root Guard	<input type="checkbox"/> Enable
BPDU Guard	<span>Disabled</span>
BPDU Handling	<span>Use Global Settings</span>
Path Cost *	<span>Default</span> <input checked="" type="checkbox"/> Use default
Priority	<span>128</span>
<hr/>	
Port State	Disabled
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Forward Transitions	N/A
<hr/>	
Speed	10G
LAG	N/A
<span>Apply</span>	

**3. Enter the parameters**

- **Interface**—Select the port number or LAG on which Spanning Tree is configured.
- **STP**—Enables or disables STP on the port.
- **Edge Port**—Enables or disables Fast Link on the port. If Fast Link mode is enabled for a port, the port state is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. The options are:
  - *Enabled*—Enables Fast Link immediately.
  - *Auto*—Enables Fast Link a few seconds after the interface becomes active. This allows STP to resolve loops before enabling Fast Link.
  - *Disabled*—Disables Fast Link.
- **Root Guard**—Enables or disables Root guard. If Root guard is enabled, devices outside the network core are prevented from being assigned the spanning tree root.
- **BPDU Guard**—Enables or disables BPDU guard. If BPDU guard is enabled, an interface is shut down when it receives a bridge protocol data unit (BPDU).
- **BPDU Handling**—Select how BPDU packets are managed when STP is disabled on the port or the switch. BPDUs are used to transmit spanning tree information.

- *Use Global Settings*—Select to use the settings defined in the [STP Global Settings Page](#).
  - *Filtering*—Filters BPDU packets when Spanning Tree is disabled on an interface.
  - *Flooding*—Floods BPDU packets when Spanning Tree is disabled on an interface.
  - **Path Cost**—Set the port contribution to the root path cost or use the default cost generated by the system.
  - **Priority**—Set the priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority is a value from 0 to 240, set in increments of 16.
  - **Port State**—Displays the current STP state of a port.
    - *Disabled*—STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
    - *Blocking*—The port is currently blocked, and cannot forward traffic (with the exception of BPDU data) or learn MAC addresses.
    - *Listening*—The port is in Listening mode. The port cannot forward traffic, and cannot learn MAC addresses.
    - *Learning*—The port is in Learning mode. The port cannot forward traffic, but it can learn new MAC addresses.
    - *Forwarding*—The port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
  - **Designated Bridge ID**—Displays the bridge priority and the MAC address of the designated bridge.
  - **Designated Port ID**—Displays the priority and interface of the selected port.
  - **Designated Cost**—Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
  - **Forward Transitions**—Displays the number of times the port has changed from the **Blocking** state to **Forwarding** state.
  - **Speed**—Displays the speed of the port.
  - **LAG**—Displays the LAG to which the port belongs. If a port is a member of a LAG, the LAG settings override the port settings.
4. Click **Apply**. The interface settings are modified, and the Running Configuration file is updated with the settings.

## CONFIGURING RSTP SETTINGS

Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that enable a faster STP convergence without creating forwarding loops.

The [RSTP Interface Settings Page](#) enables you to configure RSTP per port. Any configuration that is done on this page is active when the global STP mode is set to RSTP or MSTP.

To enter RSTP settings:

1. Click **Spanning Tree > STP Global Settings**. The [STP Global Settings Page](#) is displayed. Enable **RSTP**.
2. Click **Spanning Tree > RSTP Interface Settings**. The [RSTP Interface Settings Page](#) is displayed:

**Figure 82: RSTP Interface Settings Page**

The screenshot shows a table titled "RSTP Interface Setting Table" with a dropdown menu for "Interface Type" set to "Port". The table has 8 columns: Entry No., Interface, Point-to-Point Operational Status, Port Role, Mode, Fast Link Operational Status, and Port Status. There are 11 rows of data, each with a radio button in the first column.

Entry No.	Interface	Point-to-Point Operational Status	Port Role	Mode	Fast Link Operational Status	Port Status	
<input type="radio"/>	1	te0/1	Enabled	Designated	RSTP	Disabled	Forwarding
<input type="radio"/>	2	te0/2	Enabled	Disabled	RSTP	Disabled	Disabled
<input type="radio"/>	3	te0/3	Enabled	Disabled	RSTP	Disabled	Disabled
<input type="radio"/>	4	te0/4	Enabled	Disabled	RSTP	Disabled	Disabled
<input type="radio"/>	5	te0/5	Enabled	Disabled	RSTP	Disabled	Disabled
<input type="radio"/>	6	te0/6	Enabled	Disabled	RSTP	Disabled	Disabled
<input type="radio"/>	7	te0/7	Enabled	Disabled	RSTP	Disabled	Disabled
<input type="radio"/>	8	te0/8	Enabled	Disabled	RSTP	Disabled	Disabled
<input type="radio"/>	9	te0/9	Enabled	Disabled	RSTP	Disabled	Disabled
<input type="radio"/>	10	te0/10	Enabled	Disabled	RSTP	Disabled	Disabled
<input type="radio"/>	11	te0/11	Enabled	Disabled	RSTP	Disabled	Disabled

3. Select a port. Note: Activate Protocol Migration is only available after selecting the port connected to the bridge partner being tested.
4. If a link partner is discovered by using STP, click **Activate Protocol Migration** to run a Protocol Migration test. This discovers whether the link partner using STP still exists, and if so whether it has migrated to RSTP or MSTP. If it still exists as an STP link, the device continues to communicate with it by using STP. Otherwise, if it has been migrated to RSTP or MSTP, the device communicates with it using RSTP or MSTP, respectively.
5. Select an interface, and click **Edit**. The [Edit Rapid Spanning Tree Page](#) is displayed.

Figure 83: Edit Rapid Spanning Tree Page

Interface	Port <input type="text" value="te0/3"/> LAG <input type="text" value="1"/>
Point to Point Administrative Status	<input type="text" value="Disable"/>
Point to Point Operational Status	Enabled
Role	Disabled
Mode	RSTP
Fast Link Operational Status	Disabled
Port Status	Disabled

6. Enter the parameters

- **Interface**—Set the interface, and specify the port or LAG where RSTP is to be configured.
- **Point-to-Point Administrative Status**—Define the point-to-point link status. Ports defined as Full Duplex are considered Point-to-Point port links.
  - *Enable*—This port is a RSTP edge port when this feature is enabled, and brings it to Forwarding mode quickly (usually within 2 seconds).
  - *Disable*—The port is not considered point-to-point for RSTP purposes, which means that STP works on it at regular speed, as opposed to rapid speed.
  - *Auto*—Automatically determines switch status by using RSTP BPDUs.
- **Point-to-Point Operational Status**—Displays the Point-to-Point operating status if the **Point-to-Point Administrative Status** is set to Auto.
- **Role**—Displays the role of the port that has been assigned by STP to provide STP paths. The possible roles are:
  - *Root*—Lowest cost path to forward packets to the Root Bridge.
  - *Designated*—The interface through which the bridge is connected to the LAN, that provides the lowest cost path from the LAN to the Root Bridge.
  - *Alternate*—Provides an alternate path to the Root Bridge from the root interface.
  - *Backup*—Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

- *Disabled*—The port is not participating in Spanning Tree.
  - **Mode**—Displays the current Spanning Tree mode: Classic STP or RSTP.
  - **Fast Link Operational Status**—Displays whether the Fast Link (Edge Port) is enabled, disabled, or automatic for the interface. The values are:
    - *Enabled*—Fast Link is enabled.
    - *Disabled*—Fast Link is disabled.
    - *Auto*—Fast Link mode is enabled a few seconds after the interface becomes active.
  - **Port Status**—Displays the RSTP status on the specific port.
    - *Disabled*—STP is currently disabled on the port.
    - *Blocking*—The port is currently blocked, and it cannot forward traffic or learn MAC addresses.
    - *Listening*—The port is in Listening mode. The port cannot forward traffic, and cannot learn MAC addresses.
    - *Learning*—The port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
    - *Forwarding*—The port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
7. Click **Apply**. The Running Configuration file is updated with the settings.

---

## MULTIPLE SPANNING TREE PROTOCOL OVERVIEW

Multiple Spanning Tree Protocol (MSTP) provides solutions to various load balancing scenarios. For example, while port A is blocked in one STP instance, the same port can be placed in the Forwarding State in another STP instance. The [MSTP Properties Page](#) contains information for defining global MSTP.

### MSTP WORKFLOW

To configure MSTP perform the following:

1. Set the STP Operation Mode to MSTP as described in the [Configuring STP Global Settings](#) section.

2. Define MTP Instances. Each MST instance calculates and builds a loop free topology to bridge packets from the VLANs that map to the instance. Refer to the [Mapping VLANs to an MST Instance](#) section.
3. Associate these MTP instances to VLAN(s), deciding which MSTP instance will be active in what VLAN.
4. Configure the MSTP attributes by:
  - [Defining MSTP Properties](#)
  - [Mapping VLANs to an MST Instance](#)
  - [Defining MST Instance Settings](#)
  - [Defining MSTP Interface Settings](#)

---

## DEFINING MSTP PROPERTIES

The global Multiple Spanning Tree Protocol (MSTP) configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree. MSTP allows formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST).

MSTP is fully compatible with RSTP bridges, in that an MSTP BPDU can be interpreted by an RSTP bridge as an RSTP BPDU. This not only allows compatibility with RSTP bridges without configuration changes, but also causes any RSTP bridges outside of an MSTP region to see the region as a single RSTP bridge, regardless of the number of MSTP bridges inside the region itself.

For two or more switches to be in the same MST region, they must have the same VLANs to MST instance mapping, the same configuration revision number, and the same region name.

Switches intended to be in the same MST region are never separated by switches from another MST region. If they are separated, the region become two separate regions.

This mapping can be done in the [VLAN to MST Instance Page](#).

Configuration on this page applies if the system STP mode is MSTP.

To define MSTP:

1. Click **Spanning Tree > STP Global Settings**. The [STP Global Settings Page](#) is displayed. Enable MSTP.
2. Click **Spanning Tree > MSTP Properties**. The [MSTP Properties Page](#) is displayed.

**Figure 84: MSTP Properties Page**

<b>Region Name *</b>	<input type="text" value="00:11:22:33:44:55"/>	
<b>Revision</b>	<input type="text" value="0"/>	(0 - 65535, Default: 0)
<b>Max Hops *</b>	<input type="text" value="20"/>	(1 - 40, Default: 20)
<b>IST Master</b>	32768-00:11:22:33:44:55	

3. Enter the parameters.
  - **Region Name**—Define an MSTP region name.
  - **Revision**—Define an unsigned 16-bit number that identifies the revision of the current MST configuration. The field range is from 0 to 65535.
  - **Max Hops**—Set the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The field range is from 1 to 40.
  - **IST Master**—Displays the region’s master.
4. Click **Apply**. The MSTP properties are defined, and the Running Configuration file is updated with the settings.

## MAPPING VLANs TO AN MST INSTANCE

The [VLAN to MST Instance Page](#) enables you to map each VLAN to a Multiple Spanning Tree Instance (MSTI). For devices to be in the same region, they must have the same mapping of VLANs to MSTIs.



**NOTE:** The same MSTI can be mapped with more than one VLAN, but each VLAN can only have one MST Instance attached to it.

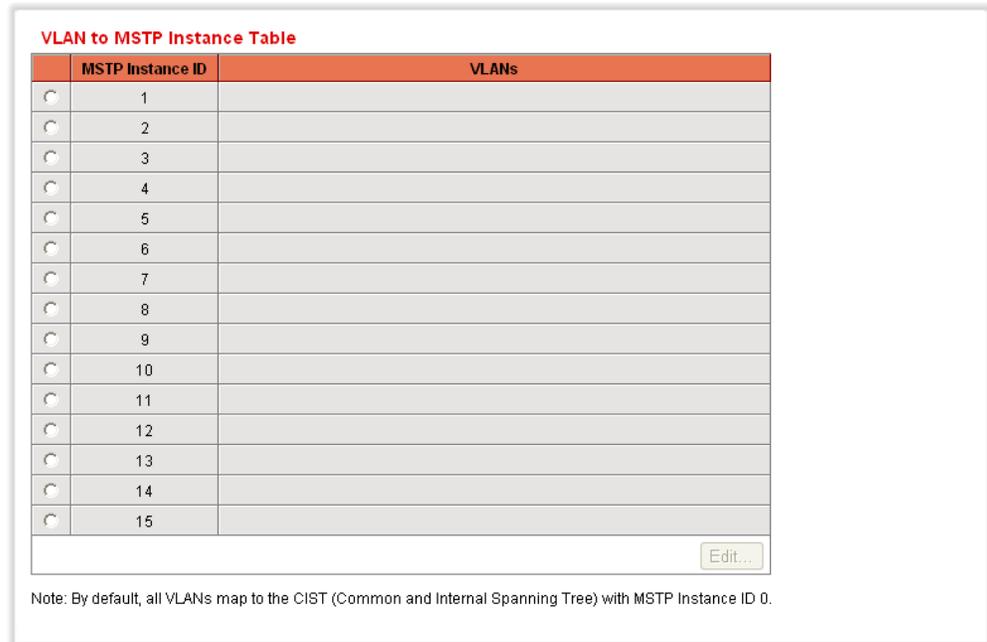
Configuration on this page (and all of the MSTP pages) applies if the system STP mode is MSTP.

Up to seven MST instances can be defined on switches. For those VLANs that are not explicitly mapped to one of the MST instances, the switch automatically maps them to the CIST (Core and Internal Spanning Tree) instance. The CIST instance is MST instance 0.

To map VLANs to MST Instances:

1. Click **Spanning Tree > VLAN to MST Instance**. The [VLAN to MST Instance Page](#) is displayed.

Figure 85: VLAN to MST Instance Page



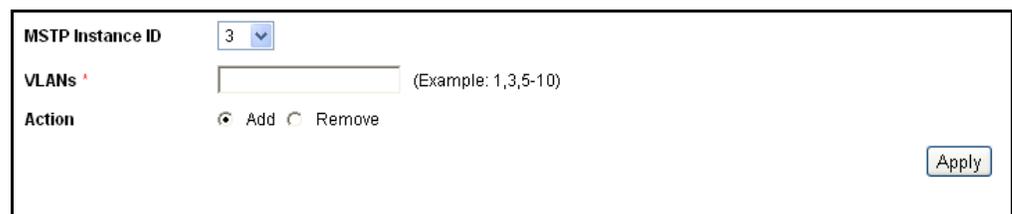
	MSTP Instance ID	VLANs
<input type="radio"/>	1	
<input type="radio"/>	2	
<input type="radio"/>	3	
<input type="radio"/>	4	
<input type="radio"/>	5	
<input type="radio"/>	6	
<input type="radio"/>	7	
<input type="radio"/>	8	
<input type="radio"/>	9	
<input type="radio"/>	10	
<input type="radio"/>	11	
<input type="radio"/>	12	
<input type="radio"/>	13	
<input type="radio"/>	14	
<input type="radio"/>	15	

Note: By default, all VLANs map to the CIST (Common and Internal Spanning Tree) with MSTP Instance ID 0.

The VLAN to MST Instance page contains the following fields:

- ◆ **MST Instance ID**—All MST instances are displayed.
  - ◆ **VLANs**—All VLANs belonging to the MST instance are displayed.
2. To add a VLAN to an MST instance, select the MST instance, and click **Edit**. The [Edit MST to VLAN Page](#) is displayed.

Figure 86: Edit MST to VLAN Page



MSTP Instance ID: 3

VLANs: (Example: 1,3,5-10)

Action:  Add  Remove

Apply

3. Enter the parameters.
  - **MST Instance ID**—Select the MST instance.
  - **VLANs**—Define the VLANs being mapped to this MST instance.
  - **Action**—Define whether to **Add** (map) or **Remove** the VLAN to/from the MST instance.
4. Click **Apply**. The MSTP VLAN mappings are defined, and the Running Configuration file is updated with the settings.

## DEFINING MST INSTANCE SETTINGS

The [MST Instance Settings Page](#) enables you to configure and view parameters per MST instance. This is the per-instance equivalent to the [Configuring STP Global Settings](#).

To enter MST instance settings:

1. Click **Spanning Tree > MST Instance Settings**. The [MST Instance Settings Page](#) is displayed.

**Figure 87: MST Instance Settings Page**

Instance ID	1	
Included VLAN		
Bridge Priority *	32768	(0 - 61440, Default: 32768)
Designated Root Bridge ID	32768-00:11:22:33:44:55	
Root Port	0	
Root Path Cost	0	
Bridge ID	32768-00:11:22:33:44:55	
Remaining Hops	20	

Apply Cancel

2. Enter the parameters.
  - **Instance ID**—Select an MST instance to be displayed and defined.
  - **Included VLANs**—Displays the VLANs mapped to the selected instance. The default mapping is that all VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).
  - **Bridge Priority**—Set the priority of this bridge for the selected MST instance.
  - **Designated Root Bridge ID**—Displays the priority and MAC address of the Root Bridge for the MST instance.
  - **Root Port**—Displays the root port of the selected instance.
  - **Root Path Cost**—Displays the root path cost of the selected instance.
  - **Bridge ID**—Displays the bridge priority and the MAC address of this switch for the selected instance.

- **Remaining Hops**—Displays the number of hops remaining to the next destination.
3. Click **Apply**. The MST Instance configuration is defined, and the Running Configuration file is updated with the settings.

## DEFINING MSTP INTERFACE SETTINGS

The [MST Interface Settings Page](#) enables you to configure the port MSTP settings for every MST instance, and to view information that has currently been learned by the protocol, such as the designated bridge per MST instance.

To configure the ports in an MST instance:

1. Click **Spanning Tree > MSTP Interface Settings**. The [MST Interface Settings Page](#) is displayed.

**Figure 88: MST Interface Settings Page**

MSTP Interface Setting Table													
Instance: 1 Interface Type: Port Go													
Entry No.	Interface	Interface Priority	Path Cost	Port State	Port Role	Mode	Type	Designated Bridge ID	Designated Port ID	Designated Cost	Remain Hops	Forward Transitions	
1	te0/1	128	200000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
2	te0/2	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
3	te0/3	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
4	te0/4	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
5	te0/5	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
6	te0/6	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
7	te0/7	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
8	te0/8	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
9	te0/9	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
10	te0/10	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
11	te0/11	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
12	te0/12	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
13	te0/13	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
14	te0/14	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
15	te0/15	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
16	te0/16	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	
17	te0/17	128	2000000	Disabled	Designated port	RSTP	Internal	N/A	N/A	N/A	N/A	N/A	

2. Enter the parameters.
  - **Instance equals To**—Select the MSTP instance to be configured.
  - **Interface Type equals to**—Select whether to display the list of ports or LAGs.

The MSTP parameters for the interfaces on the instance are displayed.
3. Select an interface, and click **Edit**. The [Edit Interface Settings Page](#) is displayed.

**Figure 89: Edit Interface Settings Page**

Instance ID	1
Interface	Port <b>te0/3</b> LAG <b>1</b>
Interface Priority	128
Path Cost	Default (1 - 200000000, Default: 2000000) <input checked="" type="checkbox"/> Use default
Port State	N/A
Port Role	N/A
Mode	RSTP
Type	N/A
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Remain Hops	N/A
Forward Transitions	N/A

**4.** Enter the parameters.

- **Instance ID**—Select the MST instance to be configured.
- **Interface**—Select the interface for which the MSTI settings are to be defined.
- **Interface Priority**—Set the port priority for the specified interface and MST instance.
- **Path Cost**—Set the port contribution to the root path cost or use the default value. The root path cost is the cost of the switch to the Root Bridge of the specified MST instance.
- **Port State**—Displays the MSTP status of the specific port on a specific MST instance. The parameters are defined as:
  - *Disabled*—STP is currently disabled.
  - *Blocking*—The port on this instance is currently blocked, and cannot forward traffic (with the exception of BPDU data) or learn MAC addresses.
  - *Listening*—The port on this instance is in Listening mode. The port cannot forward traffic, and cannot learn MAC addresses.
  - *Learning*—The port on this instance is in Learning mode. The port cannot forward traffic, but it can learn new MAC addresses.
  - *Forwarding*—The port on this instance is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Port Role**—Displays the port or LAG role, per port or LAG per instance, assigned by the MSTP algorithm to provide STP paths:

- *Root*—Forwarding packets through this interface provides the lowest cost path to forward packets to the root device.
  - *Designated*—The interface through which the bridge is connected to the LAN, that provides the lowest root path cost from the LAN to the Root Bridge for the MST instance.
  - *Alternate*—The interface provides an alternate path to the root device from the root interface.
  - *Backup*—The interface provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
  - *Disabled*—The interface does not participate in the Spanning Tree.
- **Mode**—Displays the current Spanning Tree mode.
    - *Classic STP*—Classic STP is enabled on the port.
    - *Rapid STP*—Rapid STP is enabled on the port.
    - *MSTP*—MSTP is enabled on the port.
  - **Type**—Displays the MST type of the port.
    - *Boundary Port*—A Boundary port attaches MST bridges to a LAN in an outlying region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode.
    - *Master Port*—A Master port provides connectivity from an MSTP region to the outlying CIST root.
    - *Internal*—The port is an internal port.
  - **Designated Bridge ID**—Displays the bridge ID number that connects the link or shared LAN to the root.
  - **Designated Port ID**—Displays the Port ID number on the designated bridge that connects the link or the shared LAN to the root.
  - **Designated Cost**—Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
  - **Remaining Hops**—Displays the hops remaining to the next destination.

- **Forward Transitions**—Displays the number of times the port has changed from the Forwarding state to the Blocking state.
5. Click **Apply**. The Running Configuration file is updated with the settings.



MAC addresses are stored in the *Static Address* table or the *Dynamic Address* table, along with VLAN and port information. Static addresses are configured by the user in the Static Address table and do not age out. MAC addresses seen in packets arriving at the switch are listed in the Dynamic Address table for a period of time. If another frame with the same source MAC address does not appear on the switch before that time expires, the entry is deleted from the table.

When a frame arrives on the switch, the switch searches for a MAC address that matches a static or dynamic table entry. If a match is found, the frame is marked for egress on a specific port based on the search of the tables. Frames addressed to a destination MAC address that is not found in the tables are flooded to all the ports on the relevant VLAN. These frames are called Unknown Unicast Frames.

The switch supports a maximum of 8,000 of static and dynamic MAC addresses.

This section contains information for defining both static and dynamic MAC address tables and includes the following topics:

- ◆ [Configuring Static MAC Addresses](#)
- ◆ [Dynamic MAC Addresses](#)

---

## CONFIGURING STATIC MAC ADDRESSES

Static addresses can be assigned to a specific interface and VLAN on the switch. The addresses are bound to the assigned interface. If a static address is seen on another interface, the address is ignored and it is not written to the address table.

The [Static Addresses Page](#) enables viewing statically-configured MAC addresses and creating new static MAC addresses.

To define a static address:

1. Click **MAC Address Tables > Static Addresses**. The [Static Addresses Page](#) is displayed.

Figure 90: Static Addresses Page



The [Static Addresses Page](#) displays the defined static addresses.

2. Click **Add**. The [Add Static Address Page](#) is displayed.

Figure 91: Add Static Address Page



3. Enter the parameters.
  - **VLAN ID**—Select the VLAN ID for the port.
  - **MAC Address**—Enter the interface MAC address.
  - **Interface**—Select an interface (port or LAG) for the entry.
  - **Status**—Select how the entry is treated. The options are:
    - *Permanent*—The static MAC address is never aged out of the table and if it is saved to the Startup Configuration, it is retained after rebooting.
    - *Delete on reset*—The static MAC address is never aged out of the table
    - *Delete on timeout*—The MAC address is deleted when aging occurs.
    - *Secure*—The MAC address is secure when the interface is in classic locked mode.
4. Click **Apply**. A new entry is made in the table.

## DYNAMIC MAC ADDRESSES

The Dynamic Address Table contains the MAC addresses acquired by monitoring the source addresses of 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 in the VLAN of the frame.

To prevent the bridging table from overflowing and to make room for new addresses, an address is deleted from the bridging table if no traffic is received from a dynamic MAC address for a certain period. This period of time is the aging interval.

### CONFIGURING DYNAMIC MAC ADDRESS PARAMETERS

The [Dynamic Addresses Setting Page](#) enables entering the aging interval for the MAC address table.

To enter the aging interval for dynamic addresses:

1. Click **MAC Address Tables > Dynamic Address Settings**. The [Dynamic Addresses Setting Page](#) is displayed.

**Figure 92: Dynamic Addresses Setting Page**



The screenshot shows a configuration window titled "Dynamic Addresses Setting Page". It features a text input field labeled "Aging Time" with the value "300" entered. To the right of the field, it says "sec. (10 - 630, Default: 300)". At the bottom right of the window, there are two buttons: "Apply" and "Cancel".

2. Enter **Aging Time**. The aging time is a value between the user-configured value and twice that value minus 1. For example, if you entered 300 seconds, the aging time is between 300 and 599 seconds.
3. Click **Apply**. The Dynamic MAC Address Table is updated and the Running Configuration file is updated with the settings.

### QUERYING DYNAMIC ADDRESSES

The [Dynamic Addresses Page](#) enables querying the Dynamic MAC Address table according to the following criteria:

- ◆ Interface type
- ◆ MAC addresses
- ◆ VLAN

This page displays the dynamically-learned MAC addresses. You can clear the dynamic addresses from the MAC address table and specify the query

criteria to display a subset of the table, such as the MAC addresses learned on a specific interface. You can also specify how the query results are sorted. If no filter criteria are entered, the entire table is displayed.

To perform query dynamic addresses:

1. Click **MAC Address Tables > Dynamic Addresses**. The [Dynamic Addresses Page](#) is displayed.

**Figure 93: Dynamic Addresses Page**

VLAN ID	MAC Address	Interface
VLAN 1	00:30:f1:2f:be:30	te0/1

2. In the *Filter* block, enter the following query criteria:
  - **VLAN ID**—Enter the VLAN ID for which the table is queried.
  - **MAC Address**—Enter the MAC address for which the table is queried.
  - **Interface**—Select the interface for which the table is queried. The query can search for specific ports or LAGs.
  - **Dynamic Address Table Sort Key**—Enter the field by which the table is sorted. The address table can be sorted by VLAN ID, MAC address, or interface.
3. Select the preferred option for sorting the addresses table in the Dynamic Address Sort Key.
4. Click **Query**. The Dynamic MAC Address Table is queried and the results are displayed.
5. Click **Clear Table** to delete all of the dynamic MAC addresses.

# CONFIGURING MULTICAST FORWARDING

This chapter describes the Multicast Forwarding feature, and contains the following topics:

- ◆ [Multicast Forwarding](#)
- ◆ [Defining Multicast Properties](#)
- ◆ [Adding MAC Group Address](#)
- ◆ [Adding IP Multicast Group Address](#)
- ◆ [Configuring IGMP Snooping](#)
- ◆ [Configuring MLD Snooping](#)
- ◆ [Viewing IGMP/MLD IP Multicast Groups](#)
- ◆ [Defining Multicast Router Ports](#)
- ◆ [Defining Forward All Multicast](#)
- ◆ [Defining Unregistered Multicast Settings](#)

---

## MULTICAST FORWARDING

Multicast forwarding enables one-to-many information dissemination. Multicast applications are useful for dissemination of information to multiple clients, where clients do not require reception of the entire content. A typical application is a Cable-TV like service, where clients can join a channel in the middle of a transmission, and leave before it ends.

The data is sent only to relevant ports. Forwarding the data only to the relevant ports conserves bandwidth and host resources on links.

For Multicast forwarding to work across IP subnets, nodes, and routers must be Multicast-capable. A Multicast-capable node must be able to:

- ◆ Send and receive Multicast packets.
- ◆ Register the Multicast addresses being listened to by the node with local routers, so that local and remote routers can route the Multicast packet to the nodes.

**TYPICAL MULTICAST SETUP** While Multicast routers route Multicast packets between IP subnets, Multicast-capable Layer 2 switches forward Multicast packets to registered nodes within a LAN or VLAN.

A typical setup involves a router that forwards the Multicast streams between private and/or public IP networks, a switch with Internet Group Membership Protocol (IGMP) snooping capabilities, or Multicast Listener Discovery (MLD) snooping, and a Multicast client that wants to receive a Multicast stream. In this setup, the router sends IGMP queries periodically.



**NOTE:** MLD for IPv6 is derived from the IGMP v2 for IPv4. Even though the description in this section is mostly for IGMP, it also describes coverage of MLD where implied.

These queries reach the switch that in turn floods the queries to the VLAN, and also learns the port where there is a Multicast router (Mrouter). When a host receives the IGMP query message, it responds with an IGMP Join message saying that the host wants to receive a specific Multicast stream and optionally from a specific source. The switch with the IGMP snooping analyzes the Join messages, and learns that the Multicast stream the host has requested must be forwarded to this specific port. It then forwards the IGMP Join to the Mrouter only. Similarly, when the Mrouter receives an IGMP Join message, it learns the interface where it receives the Join messages wants to receive a specific Multicast stream. The Mrouter forwards the requested Multicast stream to the interface.

**MULTICAST OPERATION** In a Layer 2 Multicast service, a Layer 2 switch receives a single frame addressed to a specific Multicast address. It creates copies of the frame to be transmitted on each relevant port.

When the switch is IGMP/MLD snooping enabled and receives a frame for a Multicast stream, it forwards the Multicast frame to all the ports that have registered to receive the Multicast stream using IGMP Join messages.

The switch can forward Multicast streams based on one of the following options:

- ◆ Multicast MAC Group Address
- ◆ IP Multicast Group Address (G)
- ◆ A combination of the source IP address (S) and the destination IP Multicast Group Address (G) of the Multicast packet.

One of these options can be configured per VLAN.

The system maintains lists of Multicast groups for each VLAN, and this manages the Multicast information that each port should receive. The Multicast groups and their receiving ports can be configured statically or learned dynamically using IGMP or Multicast Listener Discovery (MLD) protocols snooping.

**MULTICAST REGISTRATION** Multicast registration is the process of listening and responding to Multicast registration protocols. The available protocols are the IGMP for IPv4 and the MLD protocol for IPv6.

When IGMP/MLD snooping is enabled in a switch on a VLAN, it analyzes all of the IGMP/MLD packets it receives from the VLAN connected to the switch and Multicast routers in the network.

When a switch learns that a host is using IGMP/MLD messages to register to receive a Multicast stream, optionally from a specific source, the switch adds the registration in its Multicast forwarding data base.

IGMP/MLD snooping can effectively reduce Multicast traffic from streaming bandwidth-intensive IP applications. A switch using IGMP/MLD snooping only forwards Multicast traffic to the hosts interested in that traffic. This reduction of Multicast traffic reduces the packet processing at the switch, and also reduces the workload at the end hosts since they do not have to receive and filter all of the Multicast traffic generated in the network.

The following versions are supported:

- ◆ IGMP v1/v2/ v3
- ◆ MLD v1/v2
- ◆ A simple IGMP Snooping Querier

An IGMP Querier is required to facilitate the IGMP protocol on a given subnet. In general, a multicast router is also a IGMP Querier. When there are multiple IGMP Queriers in a subnet, the queriers elect a single querier as the primary querier.

The Sx300 can be configured to be an IGMP Querier as a backup querier, or in situation where a regular IGMP Querier does not exist. The Sx300 is not a full capability IGMP Querier.

If the switch is enabled as a IGMP Querier, it starts after 60 seconds have passed with no IGMP traffic (queries) detected from a Multicast router. In the presence of other IGMP Queriers, the switch might (or might not) stop sending queries, based on the results of the standard querier selection process.

**MULTICAST ADDRESS PROPERTIES** Multicast addresses have the following properties:

- ◆ Each IPv4 Multicast address is in the address range 224.0.0.0 to 239.255.255.255.
- ◆ The IPv6 Multicast address is FF00:/8.
- ◆ To map an IP Multicast group address to an Layer 2 Multicast address:
  - For IPv4, this is mapped by taking the 23 low order bits from the IPv4 address, and adding them to the 01:00:5e prefix. By standard,

the upper nine bits of the IP address are ignored, and any IP addresses that only differ in the value of these upper bits are mapped to the same Layer 2 address, since the lower 23 bits which are used are identical. For example, 234.129.2.3 is mapped to a MAC Multicast group address 01:00:5e:01:02:03. Up to 32 IP Multicast group addresses can be mapped to the same Layer 2 address.

- For IPv6, this is mapped by taking the 32 low order bits of the Multicast address, and adding them with the prefix of 33:33. For example, the IPv6 Multicast address FF00:1122:3344 is mapped to Layer 2 Multicast 33:33:11:22:33:44.

---

## DEFINING MULTICAST PROPERTIES

The [Properties Page](#) enables you to configure the Bridge Multicast filtering status.

By default, all Multicast frames are flooded to all port of the VLAN. To selectively forward only to relevant ports and filter (drop) the Multicast on the rest of the ports, enable Bridge Multicast filtering status in the [Properties Page](#).

If filtering is enabled, Multicast frames are forwarded to a subset of the ports in the relevant VLAN as defined in the Multicast Forwarding Data Base (MFDB). Multicast filtering is enforced on all traffic. By default, such traffic is flooded to all relevant ports, but you can limit forwarding to a smaller subset.

A common way of representing Multicast membership is the (S,G) notation where "S" is the (single) source sending a Multicast stream of data, and "G" is the IPv4 or IPv6 group address. If a Multicast client can receive Multicast traffic from any source of a specific Multicast group, this is written as (\*,G).

The following are ways of forwarding Multicast frames:

- ◆ **MAC Group Address**—Based on the destination MAC in the Ethernet frame.



**NOTE:** As mentioned in the Multicast Address Properties section, one or more IP Multicast group addresses can be mapped into a MAC group address. Forwarding based on MAC group address can result in an IP Multicast stream being forwarded out to ports that have no receiver for the stream.

- ◆ **IP Group Address**—Based on the destination IP address of the IP packet (\*,G).

- ◆ **Source Specific IP Group Address**—Based on both the destination IP address and the source IP address of the IP packet (S,G).

By selecting the forwarding mode, you can define the method used by hardware to identify Multicast flow by one of the following options: MAC Group Address, IP Group Address, or Source Specific IP Group Address.

(S,G) is supported by IGMPv3 and MLDv2, while IGMPv1/2 and MLDv1 support only (\*.G) which is just the group ID.

The switch supports a maximum of 256 static and dynamic Multicast group addresses.

To enable Multicast filtering, and select the forwarding method:

1. Click **Multicast > Properties**. The [Properties Page](#) is displayed.

**Figure 94: Properties Page**

The screenshot shows a configuration window with the following elements:

- Bridge Multicast Filtering Status:** A dropdown menu currently showing "Disable".
- VLAN ID:** A dropdown menu currently showing "1".
- Forwarding Method for IPv6:** A dropdown menu currently showing "IP Group Address".
- Forwarding Method for IPv4:** A dropdown menu currently showing "IP Group Address".
- Buttons:** "Apply" and "Cancel" buttons located at the bottom right of the form.

2. Enter the parameters.
  - **Bridge Multicast Filtering Status**—Enable or disable filtering.
  - **VLAN ID**—Select the VLAN ID to set its forwarding method.
  - **Forwarding Method for IPv6**—Set the forwarding method for IPv6 addresses. These are used by hardware to identify Multicast flow by one of the following options: MAC Group Address, IP Group Address, or Source Specific IP Group Address.
  - **Forwarding Method for IPv4**—Set the forwarding method for IPv4 addresses. These are used by hardware to identify Multicast flow by one of the following options: MAC Group Address, IP Group Address, or Source Specific IP Group Address.
3. Click **Apply**. The the Running Configuration file is updated with the settings.

## ADDING MAC GROUP ADDRESS

The switch supports forwarding incoming Multicast traffic based on the Multicast group information. This information is derived from the IGMP/MLD packets received or as the result of manual configuration, and stored in the Multicast Forwarding Database (MFDB).

When a frame is received from a VLAN that is configured to forward Multicast streams based on MAC group addresses, and its destination address is a Layer 2 Multicast address, the frame is forwarded to all ports that are members of the MAC group address.

The [MAC Group Address Page](#) has the following functions:

- ◆ Query and view information from the Multicast Filtering Database relating to a specific VLAN ID or a specific MAC address group. This data is acquired either dynamically through IGMP/MLD snooping or statically by manual entry.
- ◆ Add or delete static entries to this database which provides static forwarding information based on MAC destination addresses.
- ◆ Display a list of all ports/LAGs that are a member for each VLAN ID and MAC address group, and enter whether traffic is forwarded to it or not.

For viewing the forwarding information when the mode is *IP Address Group* or *IP and Source Group*, use the [IP Multicast Group Address Page](#).

To define and view MAC Multicast groups:

1. Click **Multicast > MAC Group Address**. The [MAC Group Address Page](#) is displayed.

**Figure 95: MAC Group Address Page**

VLAN ID	MAC Group Address
Table is empty	

2. Enter the parameters.
  - ◆ **VLAN ID**—Set the VLAN ID of the group to be displayed.
  - ◆ **MAC Group Address**—Set the MAC address of the Multicast group to be displayed. If no MAC Group Address is specified, the page displays all the MAC Group Addresses from the selected VLAN.

3. Click **Go**, and the MAC Multicast group addresses are displayed in the lower block.
4. Click **Add** to add a static MAC Group Address. The [Add MAC Group Address Page](#) is displayed.

**Figure 96: Add MAC Group Address Page**

5. Enter the parameters.
  - ◆ **VLAN ID**—Defines the VLAN ID of the new Multicast group.
  - ◆ **MAC Group Address**—Defines the MAC address of the new Multicast group.
6. Click **Apply**, the MAC Multicast group is added, and the Running Configuration file is updated with the settings.
7. To configure and display the registration for the interfaces within the group, select an address, and click **Details**. The [MAC Group Address Settings Page](#) is displayed.

**Figure 97: MAC Group Address Settings Page**

The page displays:

- ◆ **VLAN ID**—The VLAN ID of the Multicast group.
  - ◆ **MAC Group Address**—The MAC address of the group.
8. Select the port or LAG to be displayed from the **Filter: Interface Type** menu.
  9. Click **Go** to display the port or LAG membership.

10. Select the way that each interface is associated with the Multicast group:
  - ◆ **Static**—Attaches the interface to the Multicast group as a static member.
  - ◆ **Dynamic**—Indicates that the interface was added to the Multicast group as a result of IGMP/MLD snooping.
  - ◆ **Forbidden**—Specifies that this port is forbidden from joining this group on this VLAN.
  - ◆ **None**—Specifies that the port is not currently a member of this Multicast group on this VLAN.
11. Click **Apply**, and the Running Configuration file is updated with the settings.

---

## ADDING IP MULTICAST GROUP ADDRESS

The [IP Multicast Group Address Page](#) is similar to the [MAC Group Address Page](#) except that Multicast groups are identified by IP addresses.

The [IP Multicast Group Address Page](#) enables querying and adding IP Multicast groups.

To define and view IP Multicast groups:

1. Click **Multicast > IP Multicast Group Address**. The [IP Multicast Group Address Page](#) is displayed.

**Figure 98: IP Multicast Group Address Page**



**IP Multicast Group Address Table**

VLAN ID  (1 - 4094)

IP Version

IP Multicast Group Address

Source IP Address

<input type="checkbox"/>	VLAN ID	IP Multicast Group Address	Source IP Address
Table is empty			

Static multicast groups will appear in the table only when Bridge Multicast Filtering is globally enabled on the device.

The page displays all of the IP Multicast group addresses learned by snooping.

2. Enter the parameters required for filtering.
  - **VLAN ID**—Define the VLAN ID of the group to be displayed.
  - **IP Version**—Select IPv6 or IPv4.
  - **IP Multicast Group Address**—Define the IP address of the Multicast group to be displayed. This is only relevant when Forwarding mode is (S,G).
  - **Source IP Address**—Define the source IP address of the sending device. If mode is (S,G), enter the sender S. This together with the IP Group Address is the Multicast group ID (S,G) to be displayed. If mode is (\*,G), enter an \* to indicate that the Multicast group is only defined by destination.
3. Click **Go**. The results are displayed in the lower block.
4. Click **Add** to add a static IP Multicast Group Address. The [IP Multicast Interface Settings Page](#) is displayed.

**Figure 99: IP Multicast Group Address Details Page**

The screenshot shows a configuration form with the following fields and options:

- VLAN ID \***: A text input field with a range indicator "(1 - 4094)".
- IP Version**: Two radio button options, "Version 6" and "Version 4", with "Version 4" selected.
- IP Multicast Group Address \***: A text input field.
- Source Specific**: A checkbox labeled "Include", which is currently unchecked.
- IP Source Address \***: A text input field.
- An **Apply** button is located in the bottom right corner of the form.

5. Enter the parameters.
  - **VLAN ID**—Defines the VLAN ID of the group to be added.
  - **IP Version**—Select the IP address type.
  - **IP Multicast Group Address**—Define the IP address of the new Multicast group.
  - **Source Specific**—Indicates that the entry contains a specific source, and adds the address in the IP Source Address field. If not, the entry is added as a (\*,G) entry, an IP group address from any IP source.
  - **IP Source Address**—Defines the source address to be included.
6. Click **Apply**. The IP Multicast group is added, and the Running Configuration file is updated with the settings.
7. To configure and display the registration of an IP group address, select an address and click **Details**. The IP Multicast Interface Settings Page is displayed.

Figure 100: IP Multicast Interface Settings Page

8. Use the **Interface Type equals** filter to view the group membership on port or LAG and click **Go**.
9. For each interface, select its association type. The options are as follows:
  - *Static*—Attaches the interface to the Multicast group as a static member.
  - *Dynamic*—Indicates that the interface was added to the Multicast group as a result of IGMP/MLD snooping.
  - *Forbidden*—Specifies that this port is forbidden from joining this group on this VLAN.
  - *None*—Indicates that the port is not currently a member of this Multicast group on this VLAN.
10. Click **Apply**. The Running Configuration file is updated with the settings.

## CONFIGURING IGMP SNOOPING

To support selective Multicast forwarding (IPv4), Bridge Multicast filtering must be enabled, and IGMP Snooping must be enabled globally and for each relevant VLAN.

With IGMP Snooping the switch forwards Multicast frames to ports that have registered Multicast clients.



**NOTE:** The switch supports IGMP Snooping only on static VLANs. It does not support IGMP Snooping on dynamic VLANs.

When IGMP Snooping is enabled globally or on a VLAN, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets, and determines the following:

- ◆ Which ports are asking to join which Multicast groups on what VLAN.
- ◆ Which ports are connected to Multicast routers (Mrouter) that are generating IGMP queries.
- ◆ Which ports are receiving PIM, DVMRP, or IGMP query protocols.

These are displayed on the [IGMP Snooping Page](#).

Ports asking to join a specific Multicast group issue an IGMP report that specifies which group(s) the host wants to join. This results in the creation of a forwarding entry in the Multicast forwarding database.

The speed of IGMP Querier activity should be aligned with the IGMP-snooping-enabled switches. Queries should be sent at a rate that is aligned to the snooping table aging time. If queries are sent at a rate lower than the aging time, the subscriber cannot receive the Multicast packets.

To enable IGMP Snooping and identify the switch as an IGMP Snooping Querier on a VLAN:

1. Click **Multicast > IGMP Snooping**. The [IGMP Snooping Page](#) is displayed.

**Figure 101: IGMP Snooping Page**

The screenshot shows the IGMP Snooping configuration page. At the top, there is a section for 'IGMP Snooping Status' with a dropdown menu set to 'Disable' and 'Apply' and 'Cancel' buttons. Below this is the 'IGMP Snooping Table' which contains the following data:

VLAN ID	IGMP Snooping Operational Status	Router IGMP Version	MRouter Ports Auto Learn	Query Robustness	Query Interval (sec.)	Query Max Response Interval (sec.)	Last Member Query Counter	Last Member Query Interval (mSec.)	Immediate Leave	IGMP Querier Status	IGMP Querier Version	Querier IP Address
1	Disabled	v3	Enabled	2	125	10	2	1000	Disabled	Disabled	v2	192.168.1.5

There is an 'Edit...' button at the bottom right of the table.

The IGMP Snooping Table displays the IGMP snooping information for the VLANs on the switch. The columns are described in 3.

Enable or disable **IGMP Snooping Status**. IGMP Snooping Status globally enables the device monitoring network traffic to determine which hosts have requested to receive Multicast traffic. The switch performs IGMP Snooping if IGMP snooping and Bridge Multicast filtering are both enabled.

2. Select a VLAN, and click **Edit**. The [Edit IGMP Snooping Page](#) is displayed.

Figure 102: Edit IGMP Snooping Page

VLAN ID	1		
IGMP Snooping Status	Disable	Operational IGMP Snooping Status	Disabled
MRouter Ports Auto Learn	Enable		
Query Robustness	2 (1 - 7, Default: 2)	Operational Query Robustness	2
Query Interval	125 sec. (30 - 18000, Default: 125)	Operational Query Interval	125 (sec.)
Query Max Response Interval	10 sec. (5 - 20, Default: 10)	Operational Query Max Response Interval	10 (sec.)
Last Member Query Counter	(1 - 7, Default: Query Robustness) <input checked="" type="checkbox"/> Use default	Operational Last Member Query Counter	Query Robustness
Last Member Query Interval	1000 mS (100 - 25500, Default: 1000)	Operational Last Member Query Interval	1000 (mS)
Immediate leave	<input type="checkbox"/> Enable		
IGMP Querier Status	Disable		
Administrative Querier Source IP Address	192.168.1.5	Operational Querier Source IP Address	192.168.1.5
IGMP Querier Version	IGMPv2		

There should be only one IGMP Querier in a network. The switch supports standards-based IGMP Querier election. The following values are used when the querier message does not supply them (for IGMPv1/v2).

3. Enter the parameters.

- **VLAN ID**—Select the VLAN ID where IGMP snooping is defined.
- **IGMP Snooping Status**—Enable or disable the monitoring of network traffic to determine which hosts have asked to be sent Multicast traffic. The switch performs IGMP snooping only if IGMP snooping and Bridge Multicast filtering are both enabled.
- **Operational IGMP Snooping Status**—Displays the current status of the IGMP Snooping for the selected VLAN.
- **MRouter Ports Auto Learn**—Enable or disable auto learning of the ports to which the Mrouter is connected.
- **Query Robustness**—Enter the Robustness Variable value to be used.
- **Operational Query Robustness**—Displays the robustness variable sent by the elected querier.
- **Query Interval**—Enter the interval between the General Queries to be used.
- **Operational Query Interval**—The time interval in seconds between General Queries sent by the elected querier.
- **Query Max Response Interval**—Enter the delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
- **Operational Query Max Response Interval**—Displays the Query Max Response Interval included in the General Queries sent by the elected querier.

- **Last Member Query Counter**—Enter the number of IGMP Group-Specific Queries sent before the switch assumes there are no more members for the group.
  - **Operational Last Member Query Counter**—Displays the operational value of the Last Member Query Counter.
  - **Last Member Query Interval**—Enter the Maximum Response Delay to be used if the switch cannot read Max Response Time value from Group-Specific queries sent by the elected querier.
  - **Operational Last Member Query Interval**—Displays the Last Member Query Interval sent by the elected querier.
  - **Immediate Leave**—Enable Immediate Leave to decrease the time it takes to block a Multicast stream sent to a member port when an IGMP Group Leave message is received on that port.
  - **IGMP Querier Status**—Enable or disable the IGMP Querier.
  - **Administrative Querier Source IP Address**—Select the source IP address of the IGMP Querier. This can be the IP address of the VLAN or it can be the management IP address.
  - **Operational Querier Source IP Address**—Displays the source IP address of the elected querier.
  - **IGMP Querier Version**—Select the IGMP version used if the switch becomes the elected querier. Select IGMPv3 if there are switches and/or Multicast routers in the VLAN that perform source-specific IP Multicast forwarding.
4. Click **Apply**. The Running Configuration file is updated with the settings.

---

## CONFIGURING MLD SNOOPING

When IGMP/MLD snooping is enabled in a switch on a VLAN, it analyzes all of the IGMP/MLD packets it receives from the VLAN connected to the switch and Multicast routers in the network.

When a switch learns that a host is using IGMP/MLD messages to register to receive a Multicast stream, optionally from a specific source, the switch adds the registration in its Multicast forwarding data base.

IGMP/MLD snooping can effectively reduce Multicast traffic from streaming bandwidth-intensive IP applications. A switch using IGMP/MLD snooping only forwards Multicast traffic to the hosts interested in that traffic. This reduction of Multicast traffic reduces the packet processing at the switch, and also reduces the workload at the end hosts since they do not have to receive and filter all of the Multicast traffic generated in the network.

The following versions are supported:

- ◆ IGMP v1/v2/ v3
- ◆ MLD v1/v2

To support selective Multicast forwarding (IPv6), Bridge Multicast filtering must be enabled, and MLD Snooping must be enabled globally and for each relevant VLAN.



---

**NOTE:** The switch supports MLD Snooping only on static VLANs. It does not support MLD Snooping on dynamic VLANs.

---

The switch uses this feature to build Multicast membership lists. It uses the lists to forward Multicast packets only to switch ports where there are host nodes that are members of the Multicast groups. The switch does not support MLD Querier.

Hosts use the MLD protocol to report their participation in Multicast sessions.

The switch supports two versions of MLD snooping:

- ◆ MLDv1 snooping detects MLDv1 control packets, and sets up traffic bridging based on IPv6 destination Multicast addresses.
- ◆ MLDv2 snooping uses MLDv2 control packets to forward traffic based on the source IPv6 address, and the destination IPv6 Multicast address.

The actual MLD version is selected by the Multicast router in the network.

In an approach similar to IGMP snooping, MLD frames are snooped as they are forwarded by the switch from stations to an upstream Multicast router and vice versa. This facility enables a switch to conclude the following:

- ◆ On which ports stations interested in joining a specific Multicast group are located
- ◆ On which ports Multicast routers sending Multicast frames are located

This knowledge is used to exclude irrelevant ports (ports on which no stations have registered to receive a specific Multicast group) from the forwarding set of an incoming Multicast frame.

If you enable MLD snooping in addition to the manually-configured Multicast groups, the result is a union of the Multicast groups and port memberships derived from the manual setup and the dynamic discovery by MLD snooping. However, only the static definitions are preserved when the system is rebooted.

To enable MLD Snooping:

1. Click **Multicast > MLD Snooping**. The [MLD Snooping Page](#) is displayed.

**Figure 103: MLD Snooping Page**

VLAN ID	MLD Snooping Operational Status	Router MLD Version	MRouter Ports Auto Learn	Query Robustness	Query Interval (sec.)	Query Max Response Interval (sec.)	Last Member Query Counter	Last Member Query Interval (mSec.)	Immediate Leave
1	Disabled	v2	Enabled	2	125	10	2	1000	Disabled

The MLD Snooping Table block lists the operational MLD snooping information for the VLANs on the switch. For a description of the table columns, see 3.

2. Enable or disable **MLD Snooping Status**. MLD Snooping Status globally enables the device monitoring network traffic to determine which hosts have requested to receive Multicast traffic. The switch performs MLD Snooping if MLD snooping and Bridge Multicast filtering are both enabled.
3. Select a VLAN, and click **Edit**. The [Edit MLD Snooping Page](#) is displayed.

**Figure 104: Edit MLD Snooping Page**

VLAN ID	1		
MLD Snooping Status	Disable	Operational MLD Snooping Status	Disabled
MRouter Ports Auto Learn	Enable		
Query Robustness *	2 (1 - 7, Default: 2)	Operational Query Robustness	2
Query Interval *	125 sec. (30 - 18000, Default: 125)	Operational Query Interval	125 (sec.)
Query Max Response Interval *	10 sec. (5 - 20, Default: 10)	Operational Query Max Response Interval	10 (sec.)
Last Member Query Counter *	1 (1 - 7, Default: Query Robustness) <input checked="" type="checkbox"/> Use default	Operational Last Member Query Counter	Query Robustness
Last Member Query Interval *	1000 mS (100 - 25500, Default: 1000)	Operational Last Member Query Interval	1000 (mS)
Immediate leave	<input type="checkbox"/> Enable		

4. Enter the parameters.
  - **VLAN ID**—Select the VLAN ID.
  - **MLD Snooping Status**—Enable or disable MLD snooping on the VLAN. The switch monitors network traffic to determine which hosts have asked to be sent Multicast traffic. The switch performs MLD snooping only when MLD snooping and Bridge Multicast filtering are both enabled.
  - **Operational MLD Snooping Status**—Displays the current status of MLD Snooping for the selected VLAN.

- **MRouter Ports Auto Learn**—Enable or disable Auto Learn for the Multicast router.
  - **Query Robustness**—Enter the Robustness Variable value to be used if the switch cannot read this value from messages sent by the elected querier.
  - **Operational Query Robustness**—Displays the robustness variable sent by the elected querier.
  - **Query Interval**—Enter the Query Interval value to be used by the switch if the switch cannot derive the value from the messages sent by the elected querier.
  - **Operational Query Interval**—The time interval in seconds between General Queries received from the elected querier.
  - **Query Max Response Interval**—Enter Query Max Response delay to be used if the switch cannot read the Max Response Time value from General Queries sent by the elected querier.
  - **Operational Query Max Response Interval**—Displays the delay used to calculate the Maximum Response Code inserted into the General Queries.
  - **Last Member Query Counter**—Enter the Last Member Query Count to be used if the switch cannot derive the value from the messages sent by the elected querier.
  - **Operational Last Member Query Counter**—Displays the operational value of the Last Member Query Counter.
  - **Last Member Query Interval**—Enter the Maximum Response Delay to be used if the switch cannot read Max Response Time value from Group-Specific queries sent by the elected querier.
  - **Operational Last Member Query Interval**—The Last Member Query Interval sent by the elected querier.
  - **Immediate Leave**—When enabled, reduces the time it takes to block unnecessary MLD traffic sent to a switch port.
5. Click **Apply**. The Running Configuration file is updated with the settings.

## VIEWING IGMP/MLD IP MULTICAST GROUPS

The IGMP/MLD IP Multicast Group Page displays the IPv4 and IPv6 group address the switch learned from the IGMP/MLD messages it snoops.

There might be a difference between information on this page and, for example, information displayed in the [MAC Group Address Page](#). Assuming that the system is in MAC-based groups and a port that requested to join the following Multicast groups 224.1.1.1 and 225.1.1.1, both are mapped to the same MAC Multicast address 01:00:5e:01:01:01. In this case, there is a single entry in the MAC Multicast page, but two entries on this page.

To query for a IP Multicast group:

1. Click **Multicast > IGMP/MLD IP Multicast Group**. The [IGMP/MLD IP Multicast Group Page](#) is displayed.

**Figure 105: IGMP/MLD IP Multicast Group Page**

**IGMP IP Multicast Group Table**

Group Address   
 Source Address   
 VLAN ID

VLAN	Group Address	Source Address	Included Ports	Excluded Ports	Compatibility Mode
Table is empty					

2. Set the type of snooping group for which to search: IGMP or MLD.
3. Enter some or all of following query filter criteria:
  - **Group Address**—Defines the Multicast group MAC address or IP address to query.
  - **Source Address**—Defines the sender address to query.
  - **VLAN ID**—Defines the VLAN ID to query.
  - Click **Go**. The following fields are displayed for each Multicast group:
    - **VLAN**—The VLAN ID.
    - **Group Address**—The Multicast group MAC address or IP address.
    - **Source Address**—The sender address for all of the specified group ports.

- **Included Ports**—The list of ports to where the corresponding Multicast stream is forwarded.
- **Excluded Ports**—The list of ports not included in the group.
- **Compatibility Mode**—The oldest IGMP/MLD version of registration from the hosts the switch receives on the IP group address.

## DEFINING MULTICAST ROUTER PORTS

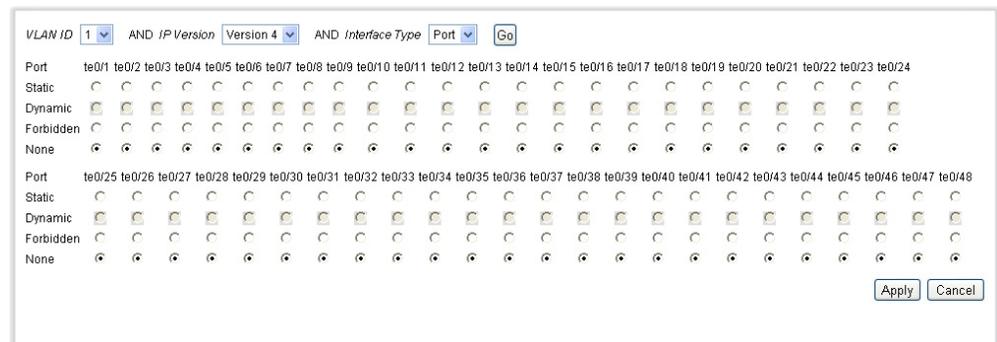
A Multicast router (Mrouter) port is a port that connects to a Multicast router. The switch includes the Multicast router port(s) when it forwards the Multicast streams and IGMP/MLD registration messages. This is required in order for all the Multicast routers can in turn forward the Multicast streams and propagate the registration messages to other subnets.

On this page, it is possible to statically configure or dynamically detect which ports are connected to Mrouters.

To define Multicast router ports:

1. Click **Multicast > Multicast Router Port**. The [Multicast Router Port Page](#) is displayed.

**Figure 106: Multicast Router Port Page**



2. Enter some or all of following query filter criteria:
  - **VLAN ID**—Select the VLAN ID for the router ports that are described.
  - **IP Version**—Select the IP version that the Multicast router supports.
  - **Interface**—Select whether to display ports or LAGs.
3. Click **Go**. The interfaces matching the query criteria are displayed.

4. For each interface, select its association type. The options are as follows:
  - *Static*—The port is statically configured as a Multicast router port.
  - *Dynamic*—The port is dynamically configured as a Multicast router port by a MLD/IGMP query. To enable the dynamic learning of Multicast router ports, go to the **Multicast > IGMP Snooping Page**, and the **Multicast > MLD Snooping Page**
  - *Forbidden*—This port is not to be configured as a Multicast router port, even if IGMP or MLD queries are received on this port. If **Auto Detect Mrouter Ports** is enabled on this port, the configuration does not succeed.
  - *None*—The port is not currently a Multicast router port.
5. Click **Apply**. The Running Configuration file is updated with the settings..

---

## DEFINING FORWARD ALL MULTICAST

The [Forward All Page](#) enables and displays the configuration of the ports and/or LAGs that are to receive all of the Multicast stream from a specific VLAN. This feature requires that the Bridge Multicast filtering in the [Properties Page](#) be enabled. If it is disabled, then all Multicast traffic is flooded to all ports in the switch.

You can statically configure a port to Forward All, if the devices connecting to the port does not support IGMP and/or MLD.

IGMP or MLD messages are not forwarded to the ports are defined as *Forward All*.



**NOTE:** The configuration affects only the ports that are members of the selected VLAN.

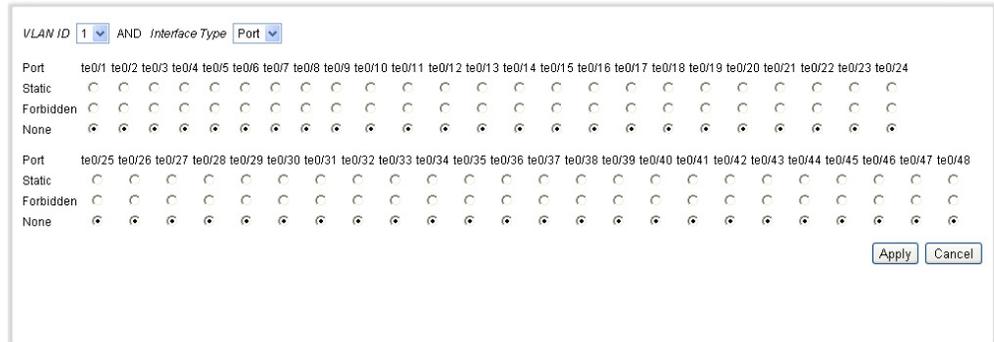
---

The configuration affects only the ports that are members of the selected VLAN.

To define Forward All Multicast:

1. Click **Multicast > Forward All**. The [Forward All Page](#) is displayed.

**Figure 107: Forward All Page**



2. Define the following:
  - **VLAN ID**—The VLAN ID the ports/LAGs are to be displayed.
  - **Interface Type**—Define whether to display ports or LAGs.
3. Click **Go**. The status of all ports/LAGs are displayed.
4. Select the interface that is to be defined as forward all by using the following methods:
  - *Static*—The port receives all Multicast streams.
  - *Dynamic*—Not applicable.
  - *Forbidden*—Ports cannot receive any Multicast streams, even if IGMP/MLD snooping designated the port to join a Multicast group.
  - *None*—The port is not currently a Forward All port.
5. Click **Apply**. The Running Configuration file is updated with the settings.

## DEFINING UNREGISTERED MULTICAST SETTINGS

Multicast frames are generally forwarded to all ports in the VLAN. If IGMP/MLD Snooping is enabled, the switch learns about the existence of Multicast groups, and monitors which ports have joined which Multicast group. Multicast groups can also be statically configured. Multicast groups that were either dynamically learned or statically configured, are considered registered. This enables the switch to forward the Multicast frames (from a registered Multicast group) only to ports that are joined to that Multicast group. The switch forwards Multicast frames (from a registered Multicast group) only to ports that are registered to that Multicast group.

The *Unregistered Multicast Page* enables handling Multicast frames that belong to groups that are not known to the switch (unregistered Multicast groups). Unregistered Multicast frames are usually forwarded to all ports on the VLAN.

You can select a port to receive or filter unregistered Multicast streams. The configuration is valid for any VLAN of which it is a member (or will be a member).

This feature ensures that the customer receives only the Multicast groups requested and not others that may be transmitted in the network.

To define unregistered Multicast settings:

1. Click **Multicast > Unregistered Multicast**. The *Unregistered Multicast Page* is displayed.

**Figure 108: Unregistered Multicast Page**

The screenshot shows a web interface titled "Unregistered Multicast Table". At the top, there is a dropdown menu for "Interface Type" set to "Port". Below this is a table with the following data:

Entry No.	Interface	Unregistered Multicast
1	te0/1	Forwarding
2	te0/2	Forwarding
3	te0/3	Forwarding
4	te0/4	Forwarding
5	te0/5	Forwarding
6	te0/6	Forwarding
7	te0/7	Forwarding
8	te0/8	Forwarding
9	te0/9	Forwarding
10	te0/10	Forwarding

This page displays information either for all ports or for all LAGs, depending on which interface type is selected.

2. Select an interface to be modified, and click **Edit**. The [Edit Unregistered Multicast Page](#) is displayed.

**Figure 109: Edit Unregistered Multicast Page**



The screenshot shows a configuration page with the following elements:

- Interface** section:
  - Radio button for **Port** (selected) with a dropdown menu showing `te0/3`.
  - Radio button for **LAG** with a dropdown menu showing `1`.
- Unregistered Multicast** section:
  - Dropdown menu showing `Forwarding`.
- An **Apply** button in the bottom right corner.

3. Define the Unregistered Multicast field.
  - **Interface**—Select the interface to be modified.
  - **LAG**—Select the LAG to be modified.
  - **Unregistered Multicast**—Define the forwarding status of the interface. The options are as follows:
    - *Forwarding*—Enables forwarding of unregistered Multicast frames to the selected interface.
    - *Filtering*—Enables filtering of unregistered Multicast frames to the selected interface.
4. Click **Apply**. The settings are saved, and the Running Configuration file is updated with the settings.

IP interface addresses are configured manually by the user, or auto-configured by a DHCP server. This chapter provides information for defining the switch IP addresses.

It includes the following topics:

- ◆ [Management and IP Interfaces](#)
- ◆ [Defining IPv4 Static Routing](#)
- ◆ [Configuring ARP](#)
- ◆ [Defining UDP Relay](#)
- ◆ [Domain Name Systems](#)

---

## MANAGEMENT AND IP INTERFACES

**IP ADDRESSING** The factory default setting of the IP address configuration is *DHCP*. This means that the switch acts as a DHCP client, and sends out a DHCP request during boot up.

If the switch receives a DHCP response from the DHCP server with an IP address, it sends Address Resolution Protocol (ARP) packets to confirm that the IP address is unique. If the ARP response shows that the IP address is in use, the switch sends a DHCPDECLINE message to the offering DHCP server, and sends another DHCPDISCOVER packet that restarts the process.

If the switch does not receive a DHCP response in 60 seconds, it continues to send DHCPDISCOVER queries, and adopts the default IP address: 10.5.235.3.

IP address collisions occur when the same IP address is used in the same IP subnet by more than one device. Address collisions require administrative actions on the DHCP server and/or the devices that collide with the switch.

When a VLAN is configured to use dynamic IP addresses, the switch issues DHCP requests until it is assigned an IP address from a DHCP server. Up to 32 interfaces (ports, LAGs, and/or VLAN) on the switch can be configured

with a static or dynamic IP address. The IP subnets where these IP addresses belong to are known as directly connected/attached IP subnets.

The IP address assignment rules for the switch are as follows:

- ◆ If the IP address on the switch is changed, the switch issues gratuitous ARP packets to the corresponding VLAN to check IP address collisions.
- ◆ The same rules apply when a client must renew the lease, prior to its expiration date through a DHCPREQUEST message.

The Internet Protocol version 6 (IPv6) is a network-layer protocol for packet-switched internetworks. IPv6 was designed to replace IPv4, the predominantly deployed Internet protocol.

IPv6 introduces greater flexibility in assigning IP addresses because the address size increases from 32-bit to 128-bit addresses. IPv6 addresses are written as eight groups of four hexadecimal digits, for example FE80:0000:0000:0000:9C00:876A:130B. The abbreviated form, in which a group of zeroes can be left out, and replaced with '::', is also acceptable, for example, ::-FE80::9C00:876A:130B.

IPv6 nodes require an intermediary mapping mechanism to communicate with other IPv6 nodes over an IPv4-only network. This mechanism, called a tunnel, enables IPv6-only hosts to reach IPv4 services, and allows isolated IPv6 hosts and networks to reach an IPv6 node over the IPv4 infrastructure.

The tunneling mechanism uses the ISATAP mechanism. This protocol treats the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link local IPv6 address.

The switch detects IPv6 frames by the IPv6 Ethertype.

The switch can have multiple IP addresses. Each IP address can be assigned to specified ports, LAGs, or VLANs. These IP addresses are configured in the [IPv4 Interface Page](#). The switch can be reached at all its IP addresses from the corresponding interfaces.

A predefined, default route is not provided. To remotely manage the switch, a default route must be defined. Any DHCP-assigned default gateways are stored as default routes. In addition, you can manually define default routes. This is defined in the [IPv4 Static Routes](#).

## DEFINING AN IPv4 INTERFACE

The IP address can be configured on a port, a LAG, or VLAN interface.

The switch routes traffic between the directly attached IP subnets configured at the switch. The switch continues to bridge traffic between devices in the same VLAN. Additional IPv4 routes for routing to non-directly attached subnets can be configured in the [IPv4 Static Routes](#).



**NOTE:** The switch software consumes one VLAN ID (VID) for every IP address configured on a port or LAG. The switch takes the first VID that is not used starting from 4094.

To configure the IPv4 addresses:

1. Click **IP Configuration > Management and IP Interface > IPv4 Interface**. The [IPv4 Interface Page](#) is displayed.

**Figure 110: IPv4 Interface Page**

<input type="checkbox"/>	Interface	IP Address Type	IP Address	Mask	Status
<input type="checkbox"/>	VLAN 1	Static	192.168.1.5	255.255.255.0	Valid

This page displays the following fields:

- ◆ **Interface**—Interface for which the IP address is defined.
- ◆ **IP Address Type**—IP address defined as static or DHCP.
  - *Static*—Entered manually.
  - *DHCP*—Received from DHCP server.
- ◆ **IP Address**—Configured IP address for the interface.
- ◆ **Mask**—Configured IP address mask.
- ◆ **Status**—Results of the IP address duplication check.
  - *No Entry*—The IP address is unknown.
  - *Tentative*—There is no final result for the IP address duplication check.
  - *Valid*—The IP address collision check was completed, and no IP address collision was detected.
  - *Valid-Duplicated*—The IP address duplication check was completed, and a duplicate IP address was detected.
  - *Duplicated Without Valid*—A duplicated IP address was detected for the default IP address.

2. Click **Add**. The [Add IPv4 Interface Page](#) is displayed.

Figure 111: Add IPv4 Interface Page

The screenshot shows a configuration page for adding an IPv4 interface. At the top, there are three radio buttons for 'Interface': 'Port' (selected), 'LAG', and 'VLAN'. Below 'Port' is a dropdown menu showing 'te0/1'. Below 'LAG' is a dropdown menu showing '1'. Below 'VLAN' is a dropdown menu showing '1'. Underneath, there is a dropdown menu for 'IP Address Type' set to 'Dynamic'. Below that is a text input field for 'IP Address'. Under the 'Mask' section, there are two radio buttons: 'Network Mask' (selected) and 'Prefix Length'. The 'Prefix Length' option has a range '(0 - 32)' next to it. At the bottom right, there are two buttons: 'Apply' and 'Close'.

3. Select one of the following fields:
  - **Interface**—Select Port, LAG, or VLAN as the interface associated with this IP configuration, and select a value for the interface from the list.
  - **IP Address Type**—Select one of the following options:
    - **Dynamic IP Address**—Receive the IP address from a DHCP server.
    - **Static IP Address**—Enter the IP address.
4. If Static Address was selected, enter the **IP Address** for this interface.
5. Enter the Network Mask or Prefix Length for this IP address.
  - **Network Mask**—IP mask for this address.
  - **Prefix Length**—Length of the IPv4 prefix.
6. Click **Apply**. The IPv4 address settings are defined, and the Running Configuration file is updated with the settings.

## DEFINING IPv6 GLOBAL CONFIGURATION

The [IPv6 Global Configuration Page](#) defines the frequency of the IPv6 ICMP error messages generated by the switch.

To define IPv6 global parameters:

1. Click **IP Configuration > Management and IP Interface > IPv6 Global Configuration**.

The [IPv6 Global Configuration Page](#) is displayed.

**Figure 112: IPv6 Global Configuration Page**

ICMPv6 Rate Limit Interval \*  ms (0 - 2147483647, Default: 100)

ICMPv6 Rate Limit Bucket Size \*  messages (1 - 200, Default: 10)

2. Enter the values for the following fields:
  - ◆ **ICMPv6 Rate Limit Interval**—Enter the time limit.
  - ◆ **ICMPv6 Rate Limit Bucket Size**—Enter the maximum number of ICMP error message that can be sent by the switch per interval.
3. Click **Apply**. The IPv6 global parameters are defined, and the Running Configuration file is updated with the settings.

## DEFINING AN IPv6 INTERFACE

The [IPv6 Interfaces Page](#) displays the switch’s IPv6 interface parameters and *enables* configuring this interface. An IPv6 interface can be configured on a port, a LAG, VLAN, or ISATAP tunnel interface. The switch supports one IPv6 interface as an IPv6 end device.

A tunnel interface is configured with an IPv6 address based on the settings defined in the [IPv6 Tunnel Page](#).

To configure IPv6 interfaces:

1. Click **IP Configuration > Management and IP Interface > IPv6 Interfaces**.

The [IPv6 Interfaces Page](#) is displayed.

**Figure 113: IPv6 Interfaces Page**

**IPv6 Interface Table**

<input type="checkbox"/>	Interface	DAD Attempts	Auto Configuration	Send ICMPv6 Messages
Table is empty				

This page displays the IPv6 interfaces already configured.

2. Click **Add** to add a new IPv6 interface, that is to define on which interface IPv6 is enabled. The [Add IPv6 Interface Page](#) is displayed.

Figure 114: Add IPv6 Interface Page

The screenshot shows a configuration page for an IPv6 interface. At the top, there are radio buttons for selecting the interface type: Port (selected), LAG, VLAN, and ISATAP Tunnel. Below these are input fields for LAG (1), VLAN (1), and ISATAP Tunnel. The 'Number of DAD Attempts' is set to 1, with a note '(0 - 600, Default: 1)'. The 'IPv6 Address Auto Configuration' and 'Send ICMPv6 Messages' are both set to 'Enable'. An 'Apply' button is located in the bottom right corner.

3. Enter the values.

- **IPv6 Interface**—Select a specific port, LAG, VLAN, or ISATAP tunnel.
- **Number of DAD Attempts**—Enter the number of consecutive neighbor solicitation messages that are sent while Duplicate Address Detection (DAD) is performed on the interface’s Unicast IPv6 addresses. DAD verifies the uniqueness of new Unicast IPv6 addresses before the addresses are assigned. New addresses remain in a tentative state during DAD verification. Entering **0** in this field disables duplicate address detection processing on the specified interface. Entering **1** in this field indicates a single transmission without follow-up transmissions.
- **IPv6 Address Auto Configuration**—Enable automatic address configuration from the DHCP server. If enabled, the switch supports IPv6 stateless address auto configuration of site local and global IP address from the IPv6 router advertisement received on the interface. The switch does not support stateful address auto configuration.
- **Send ICMPv6 Messages**—Enable generating unreachable destination messages.

4. Click **Apply** to enable IPv6 processing on the selected interface. Regular IPv6 interfaces have the following addresses automatically configured:

- Link local address using EUI-64 format interface ID based on a device’s MAC address
- All node link local Multicast addresses (FF02::1)
- Solicited-Node Multicast address (format FF02::1:FFXX:XXXX)

5. Click **IPv6 Address Table** to manually assign IPv6 addresses to the interface, if required. This page is described in the [Defining IPv6 Addresses](#) section.

**DEFINING IPv6 ADDRESSES** To assign an IPv6 address to an IPv6 Interface:

1. Click **IP Configuration > Management and IP Interface > IPv6 Addresses**.

The [IPv6 Address Page](#) is displayed.

**Figure 115: IPv6 Address Page**

2. Select an interface. The interface is displayed in the IPv6 Address table.
3. Click **Add**. The [Add IPv6 Address Page](#) is displayed.

**Figure 116: Add IPv6 Address Page**

4. Enter the values for the fields.
  - **IPv6 Interface**—Displays the interface where the address is automatically completed, based on the filter.
  - **IPv6 Address Type**—Select Link Local or Global as the type of IPv6 address to add.
    - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.

- *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **IPv6 Address**—The switch supports one IPv6 interface. In addition to the default link local and Multicast addresses, the device also automatically adds global addresses to the interface based on the router advertisements it receives. The device supports a maximum of 128 addresses at the interface. Each address must be a valid IPv6 address that is specified in hexadecimal format by using 16-bit values separated by colons.



**NOTE:** You cannot configure any IPv6 addresses directly on a ISATAP tunnel interface.

- **Prefix Length**—The length of the Global IPv6 prefix as a decimal value from 0-128 indicating the number of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
  - **EUI-64**—Select to use the EUI-64 parameter to identify the interface ID portion of the Global IPv6 address by using the EUI-64 format based on a device MAC address.
5. Click **Apply**. The Running Configuration file is updated with the settings.

## VIEWING THE IPv6 DEFAULT ROUTER LIST

The [IPv6 Default Router List Page](#) enables configuring and viewing the default IPv6 router addresses. This list contains 0 or more routers that are candidates to become the switch default router for non-local traffic. The switch randomly selects a router from the list. The switch supports one static IPv6 default router. Dynamic default routers are routers that have sent router advertisements to the switch IPv6 interface.

When adding or deleting IP addresses, the following events occur:

- ◆ When removing an IP interface, all the default router IP addresses are removed.
- ◆ Dynamic IP addresses cannot be removed.
- ◆ An alert message is displayed after an attempt is made to insert more than a single user-defined address.
- ◆ An alert message is displayed when attempting to insert a non-link local type address, meaning 'fe80:'.

To define a default router:

1. Click **IP Configuration > Management and IP Interface > IPv6 Default Router List**.

The [IPv6 Default Router List Page](#) is displayed.

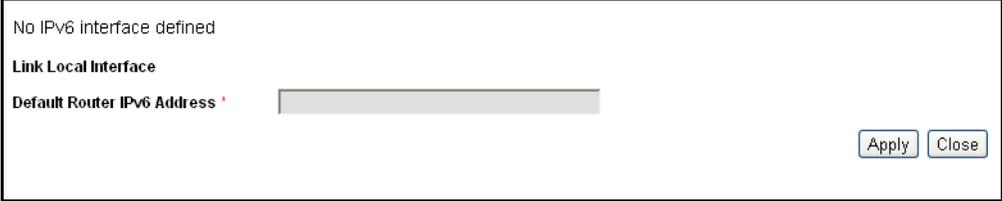
**Figure 117: IPv6 Default Router List Page**

<input type="checkbox"/>	Default Router IPv6 Address	Interface	Type	State
Table is empty				
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>				

This page displays the following fields for each default router:

- ◆ **Default Router IPv6 Address**—Link local IP address of the default router.
  - ◆ **Interface**—Outgoing IPv6 interface where the default router resides.
  - ◆ **Type**—The default router configuration that includes the following options:
    - *Static*—The default router was manually added to this table through the **Add** button.
    - *Dynamic*—The default router was dynamically configured.
    - **State**—The default router status options are:
      - *Incomplete*—Address resolution is in process. Default router has not yet responded.
      - *Reachable*—Positive confirmation was received within the *Reachable Time*.
      - *Stale*—Previously-known neighboring network is unreachable, and no action is taken to verify its reachability until it is necessary to send traffic.
      - *Delay*—Previously-known neighboring network is unreachable. The switch is in Delay state for a predefined *Delay Time*. If no confirmation is received, the state changes to Probe.
      - *Probe*—Neighboring network is unavailable, and Unicast Neighbor Solicitation probes are being sent to verify the status.
2. Click **Add** to add a static default router. The [Add Default Router Page](#) is displayed.

**Figure 118: Add Default Router Page**



The window displays the Link Local Interface. The interface can be a port, LAG, VLAN, or tunnel.

3. Enter the static default router IP address in the Default Router IPv6 Address field.
4. Click **Apply**. The default router is defined, and the Running Configuration file is updated with the settings.

## CONFIGURING IPv6 TUNNELS

The ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) enables encapsulating IPv6 packets within IPv4 packets for transmission over IPv4 networks. You must first manually enable and configure an ISATAP tunnel. Then you manually define an IPv6 interface at the ISATAP tunnel. Then the switch automatically configures the link local IPv6 address to the IPv6 interface.

When defining ISATAP tunnels, note the following:

- ◆ An IPv6 link local address is assigned to the ISATAP interface. The initial IP address is assigned to the interface, which is then activated.
- ◆ If an ISATAP interface is active, the ISATAP router IPv4 address is resolved via DNS by using ISATAP-to-IPv4 mapping. If the ISATAP DNS record is not resolved, ISATAP host name-to-address mapping is searched in the host mapping table.
- ◆ When the ISATAP router IPv4 address is not resolved via the DNS process, the ISATAP IP interface remains active. The system does not have a default router for ISATAP traffic until the DNS process is resolved.

To configure an IPv6 Tunnel:

1. Click **IP Configuration > Management and IP Interface > IPv6 Tunnel**.

The [IPv6 Tunnel Page](#) is displayed.

Figure 119: IPv6 Tunnel Page

<b>Tunnel Number</b>	1	
<b>Tunnel Type</b>	ISATAP	
<b>Source IPv4 Address *</b>	None <input type="button" value="v"/>	<input type="text"/>
<b>Tunnel Router's Domain Name *</b>	ISATAP <input type="text"/>	(Default: ISATAP) <input checked="" type="checkbox"/> Use default
<b>Parameters</b>		
<b>Query Interval *</b>	<input type="text" value="10"/>	sec. (10 - 3600, Default: 10) <input checked="" type="checkbox"/> Use default
<b>ISATAP Solicitation Interval *</b>	<input type="text" value="10"/>	sec. (10 - 3600, Default: 10) <input checked="" type="checkbox"/> Use default
<b>ISATAP Robustness *</b>	<input type="text" value="3"/>	(1 - 20, Default: 3) <input checked="" type="checkbox"/> User defined
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

2. Enter the values for the following fields:

- **Tunnel Number**—Displays the automatic tunnel router domain number.
- **Tunnel Type**—Always displayed as ISATAP.
- **Source IPv4 Address**—Disable the ISATAP tunnel, or enable the ISATAP tunnel over an IPv4 interface. The IPv4 address of the selected IPv4 interface used to form part of the IPv6 address over the ISATAP tunnel interface. The IPv6 address has a 64-bit network prefix of fe80::, with the rest of the 64-bit formed by concatenating 0000:5EFE and the IPv4 address.
  - *Auto*—Automatically selects the lowest IPv4 address from among all of its configured IPv4 interfaces.
  - *None*—Disable the ISATAP tunnel.
  - *Manual*—Manually configure an IPv4 address. The IPv4 address configured must be one of the IPv4 addresses at the switch IPv4 interfaces.
- **Tunnel Router's Domain Name**—A global string that represents a specific automatic tunnel router domain name. The name can either be the default name (ISATAP) or a user defined name.
- **Query Interval**—The number of seconds from 10-3600 between DNS queries (before the IP address of the ISATAP router is known) for this tunnel. The interval can be the default value (10 seconds) or a user defined interval.
- **ISATAP Solicitation Interval**—The number of seconds from 10-3600 between ISATAP router solicitations messages, when there is no active ISATAP router. The interval can be the default value (10 seconds) or a user defined interval.

- **ISATAP Robustness**—Used to calculate the interval for the DNS or router solicitation queries. The bigger the number, the more frequent the queries. The default value is 3. The range is 1-20.



**NOTE:** The ISATAP tunnel is not operational if the underlying IPv4 interface is not in operation.

3. Click **Apply**. The tunnel is defined, and the Running Configuration file is updated with the settings.

### DEFINING IPv6 NEIGHBORS INFORMATION

The *IPv6 Neighbors Page* enables configuring and viewing the list of IPv6 neighbors on the IPv6 interface. The IPv6 Neighbor Table (also known as IPv6 Neighbor Discovery Cache) displays the MAC addresses of the IPv6 neighbors that are in the same IPv6 subnet as the switch. This is used to verify the reachability of this neighbor. This is the IPv6 equivalent of the IPv4 ARP Table. When the switch needs to communicate with its neighbors, the switch uses the IPv6 Neighbor Table to determine the MAC addresses based on their the IPv6 addresses.

This page displays the neighbors that were automatically detected or manually configured entries. Each entry displays to which interface the neighbor is connected, the neighbor’s IPv6 and MAC addresses, the entry type (static or dynamic), and the state of the neighbor.

#### TO DEFINE IPv6 NEIGHBORS:

1. Click **IP Configuration > Management and IP Interface > IPv6 Neighbors**.

The IPv6 Neighbors Page is displayed.

**Figure 120: IPv6 Neighbors Page**



2. Select a **Clear Table** option to clear some or all of IPv6 addresses in the IPv6 Neighbors Table.
  - *Static Only*—Deletes the static IPv6 address entries.
  - *Dynamic Only*—Deletes the dynamic IPv6 address entries.

- *All Dynamic & Static*—Deletes the static and dynamic address entries IPv6 address entries.
  - The following fields are displayed for the neighboring interfaces:
    - **Interface**—Neighboring IPv6 interface type.
    - **IPv6 Address**—IPv6 address of a neighbor.
    - **MAC Address**—MAC address mapped to the specified IPv6 address.
    - **Type**—Neighbor discovery cache information entry type (static or dynamic).
    - **State**—Specifies the IPv6 neighbor status. The values are:
      - *Incomplete*—Address resolution is working. The neighbor has not yet responded.
      - *Reachable*—Neighbor is known to be reachable.
      - *Stale*—Previously-known neighbor is unreachable. No action is taken to verify its reachability until traffic must be sent.
      - *Delay*—Previously-known neighbor is unreachable. The interface is in Delay state for a predefined Delay Time. If no reachability confirmation is received, the state changes to Probe.
      - *Probe*—Neighbor is no longer known to be reachable, and Unicast Neighbor Solicitation probes are being sent to verify the reachability.
3. Click **Add**. The [Add IPv6 Neighbors Page](#) is displayed.
  4. The [Add IPv6 Neighbors Page](#) provides information for adding a neighbor to be monitored.

**Figure 121: Add IPv6 Neighbors Page**

The screenshot shows a web form titled "Add IPv6 Neighbors Page". At the top, it says "No IPv6 interface defined". Below this, there are three input fields: "Interface", "IPv6 Address", and "MAC Address". Each field has a small red asterisk to its right. The "Interface" field is currently empty. The "IPv6 Address" and "MAC Address" fields contain placeholder text. In the bottom right corner of the form, there is an "Apply" button.

5. Enter the values for the following fields:
  - **Interface**—The neighboring IPv6 interface to be added.
  - **IPv6 Address**—Enter the IPv6 network address assigned to the interface. The address must be a valid IPv6 address.

- **MAC Address**—Enter the MAC address mapped to the specified IPv6 address.
6. Click **Apply**, and the Running Configuration file is updated with the settings.

## VIEWING IPv6 ROUTE TABLES

The *IPv6 Routes Table Page* displays the IPv6 Routes Table. The table contains a single default route (IPv6 address::0) that uses the default router selected from the IPv6 Default Router List to send packets to destination devices that are not in the same IPv6 subnet as the switch. In addition to the default route, the table also contains dynamic routes which are ICMP redirect routes received from IPv6 routers by using ICMP redirect messages. This could happen when the default router the switch uses is not the router for traffic to the IPv6 subnets that the switch wants to communicate to.

1. Click **IP Configuration > Management and IP Interface > IPv6 Routes**.

The IPv6 Routes Table Page is displayed.

**Figure 122: IPv6 Routes Table Page**



The screenshot shows a web interface titled "IPv6 Routing Table". Below the title is a table with the following headers: IPv6 Address, Prefix Length, Interface, Next Hop, Metric, Life Time, and Route Type. The table body is empty, and the text "Table is empty" is displayed in the center.

IPv6 Address	Prefix Length	Interface	Next Hop	Metric	Life Time	Route Type
Table is empty						

This page displays the following fields:

- ◆ **IPv6 Address**—The IPv6 subnet address.
- ◆ **Prefix Length**—IP route prefix length for the destination IPv6 subnet address. It is preceded by a forward slash.
- ◆ **Interface**—Interface used to forward the packet.
- ◆ **Next Hop**—Address where the packet is forwarded. Typically, this is the address of a neighboring router. This must be a link local address.
- ◆ **Metric**—Value used for comparing this route to other routes with the same destination in the IPv6 router table. All default routes have the same value.
- ◆ **Life Time**—Time period that the packet can be sent, and resent, before being deleted.

- ◆ **Route Type**—How the destination is attached, and the method used to obtain the entry. The following values are:
  - *Local*—The manually configured switch IPv6 address.
  - *Dynamic*—The destination is indirectly attached IPv6 subnet address. The entry was obtained dynamically via the ICMP protocol.

## DEFINING IPv4 STATIC ROUTING

This page enables configuring and viewing IPv4 static routes on the switch. When routing traffic, the next hop is decided based on the longest prefix match (LPM algorithm). A destination IPv4 address may match multiple routes in the IPv4 Static Route Table. The switch uses the matched route with the highest subnet mask, that is, the longest prefix match.

To define an IP static route:

1. Click **IP Configuration > IPv4 Static Routes**.

The [IPv4 Static Routes](#) is displayed.

**Figure 123: IPv4 Static Routes**

IPv4 Static Routing Table						
<input type="checkbox"/>	Destination IP Address	Prefix Length	Next Hop Router IP Address	Route Type	Route Owner	Metric
<input type="checkbox"/>	192.168.1.0	24		Local		

2. Click **Add**. The [Add IPv4 Static Routes](#) is displayed.

**Figure 124: Add IPv4 Static Routes**

**Destination IP Prefix \***   
**Mask \***  Network mask   Prefix length   
**Next Hop Router IP Address \***   
**Route Type**    
**Metric \***  (1 - 255, Default: 1)

3. Enter the values for the following fields:

- **Destination IP Prefix**—Enter the destination IP address prefix.

- **Mask**—Select and enter information for one of the following:
  - **Network Mask**—The IP route prefix for the destination IP.
  - **Prefix Length**—The IP route prefix for the destination IP.
- **Next Hop Router IP Address**—Enter the next hop IP address or IP alias on the route.



**NOTE:** You cannot configure a static route through a directly-connected IP subnet where the switch gets its IP address from a DHCP server.

- **Route Type**—Select the route type.
    - *Reject*—Rejects the route and stops routing to the destination network via all gateways. This ensures that if a frame arrives with the destination IP of this route, it is dropped.
    - *Remote*—Indicates that the route is a remote path.
  - **Metric**—Enter the administrative distance to the next hop. The range is 1–255.
4. Click **Apply**. The IP Static route is added, and the Running Configuration file is updated with the settings.

---

## CONFIGURING ARP

The switch maintains an ARP (Address Resolution Protocol) Table for all the known devices that reside in its directly connected IP subnets. A directly connected IP subnet is the subnet that a IPv4 interface of the switch is connected to. When the switch needs to send/route a packet to a local device, it searches the ARP Table to obtain the MAC address of the device. The ARP Table contains both static and dynamic addresses. Static addresses are manually configured and do not age out. The switch creates dynamic addresses from the ARP packets it receives. Dynamic addresses age out after a configured time.

The [ARP Table Page](#) enables viewing dynamic ARP entries that the switch has learned, changing the ARP entry aging time, clearing ARP entries, and adding or deleting static ARP entries.

To define the ARP tables:

1. Click **IP Configuration** > **ARP**. The [ARP Table Page](#) is displayed.

Figure 125: ARP Table Page

ARP Entry Age Out <sup>\*</sup>  sec. (1 - 40000000, Default: 60000)

Clear ARP Table Entries

**ARP Table**

<input type="checkbox"/>	Interface	IP Address	MAC Address	Status
<input type="checkbox"/>	VLAN 1	192.168.1.9	00:30:f1:2f:be:30	Dynamic

- Enter the parameters.
  - ARP Entry Age Out**—Enter the number of seconds that dynamic addresses can remain in the ARP Table. A dynamic address ages out after the time it is in the table exceeds the ARP Entry Age Out time. When a dynamic address ages out, it is deleted from the table, and needs to be relearned to be entered into the table again.
  - Clear ARP Table Entries**—Select the type of ARP entries to be cleared the system.
    - All*—Deletes all of the static and dynamic addresses immediately.
    - Dynamic*—Deletes all of the dynamic addresses immediately.
    - Static*—Deletes all of the static addresses immediately.
    - Normal Age Out*—Deletes dynamic addresses based on the configured ARP Entry Age Out time.
- Click **Apply**. The ARP global settings are modified, and the Running Configuration file is updated with the settings.

The ARP Table displays the following fields:

- Interface**—The IPv4 Interface of the directly connected IP subnet where the IP device resides.
  - IP Address**—The IP address of the IP device.
  - MAC Address**—The MAC address of the IP device.
  - Status**—Whether the entry was manually entered or dynamically learned.
- Click **Add**. The [Add ARP Page](#) is displayed.

Figure 126: Add ARP Page

The screenshot shows a configuration page for adding an ARP entry. It features the following elements:

- IP Version:** A dropdown menu currently set to "Version 4".
- Interface:** Three radio buttons labeled "Port", "LAG", and "VLAN". The "VLAN" radio button is selected. To the right of the "VLAN" radio button is a dropdown menu showing the value "1".
- IP Address:** A text input field with a red asterisk to its left, indicating it is a required field.
- MAC Address:** A text input field with a red asterisk to its left, indicating it is a required field.
- Apply:** A button located in the bottom right corner of the form.

5. Enter the parameters.

- **IP Version**—The IP address format supported by the host. Only IPv4 is supported.
- **Interface**—IPv4 interface on the switch. An IPv4 interface can be configured on a port, LAG or VLAN
  - For devices in Layer 2 mode, there is only one directly connected IP subnet which is always in the management VLAN. All the static and dynamic addresses in the ARP Table reside in the management VLAN.
  - For devices in Layer 3 mode, an IPv4 interface can be configured on a port, LAG or VLAN. Select the desired interface from the list of configured IPv4 interfaces on the switch.
- **IP Address**—Enter the IP address of the local device.
- **MAC Address**—Enter the MAC address of the local device.

6. Click **Apply**. The ARP entry is defined, and the Running Configuration file is updated with the settings.

---

## DEFINING UDP RELAY

Switches do not typically route IP broadcast packets between IP subnets. However, if configured, the switch can relay specific UDP broadcast packets received from its IPv4 interfaces to specific destination IP addresses.

To configure the relaying of UDP packets received from a specific IPv4 interface with a specific destination UDP port, add a UDP Relay:

1. Click **IP Configuration > UDP Relay**. The [UDP Relay Page](#) is displayed.

Figure 127: UDP Relay Page

Source IP Interface	UDP Destination Port	Destination IP Address
Table is empty		

Add... Delete

- Click **Add**. The [Add UDP Relay Page](#) is displayed.

Figure 128: Add UDP Relay Page

Source IP Interface \*

UDP Destination Port  (1 - 65535)

Destination IP Address \*

Apply Close

- Select the **Source IP Interface** to where the switch is to relay UDP broadcast packets based on a configured UDP Destination Port. The interface must be one of the IPv4 interfaces configured on the switch.
- Enter the **UDP Destination Port** number for the packets that the switch is to relay. The range is from 1-65535.
- Enter the **Destination IP Address** that receives the UDP packet relays. If this field is 0.0.0.0, UDP packets are discarded. If this field is 255.255.255.255, UDP packets are flooded to all IP interfaces.
- Click **Apply**. The UDP relay settings are defined, and the Running Configuration file is updated with the settings.

---

## DOMAIN NAME SYSTEMS

The Domain Name System (DNS) translates user-defined domain names into IP addresses for the purpose of locating and addressing these objects.

As a DNS client the switch resolves domain names to IP addresses through one or more configured DNS servers.

### DEFINING DNS SERVERS

The *DNS Servers Page* enables configuring the DNS servers and the default domain used by the switch.

To configure DNS servers:

1. Click **IP Configuration > Domain Name System > DNS Servers**. The [DNS Servers Page](#) is displayed.

**Figure 129: DNS Servers Page**

DNS  Enable

---

**Default Parameters**

Default Domain Name

Type N/A

Remove

**DNS Server Table**

DNS Server	Server state
Table is empty	

2. Enter the parameters.
  - **DNS**—Select to enable the switch as a DNS client to resolve DNS names into IP addresses through one or more configured DNS servers.
  - **Default Domain Name**—Enter the default DNS domain name (1–158 characters). The switch appends to all non-fully qualified domain names (FQDN) turning them into FQDNs.
  - **Type**—Displays the default domain type options:
    - *DHCP*—The default domain name is dynamically assigned by the DHCP server.
    - *Static*—The default domain name is user-defined.
    - *N/A*—No default domain name.

DNS Server Table:

- **DNS Server**—The IP addresses of the DNS servers. Up to eight DNS servers can be defined.
- **Server State**—The active DNS server. There can be only one active server. Each static server has a priority, a lower value means a higher priority. When first time the request is sent, static server with lowest priority is chosen. If after two retries there is no response from this server, the next server with the next lowest priority is selected. If none of the static servers respond, the first dynamic server on the table, sorted by IP address (low to high), is selected.

3. Click **Add**. The [Add DNS Server Page](#) is displayed.

**Figure 130: Add DNS Server Page**

4. Enter the parameters.

- ◆ **IP Version**—Select Version 6 for IPv6 or Version 4 for IPv4.
  - ◆ **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:
    - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
    - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
  - ◆ **Link Local Interface**—If the IPv6 address type is Link Local, select whether it is received through VLAN2 or ISATAP.
  - ◆ **DNS Server IP Address**—Enter the DNS server IP address.
  - ◆ **Set DNS Server Active**—Select to activate the new DNS server.
5. Click **Apply**. The DNS server is added, and the Running Configuration file is updated with the settings.

**MAPPING DNS HOSTS** The switch saves the frequently-queried domain names acquired from the DNS servers into the local DNS cache. The cache can hold up to 64 static entries, 64 dynamic entries, and one entry for each IP address configured on the switch by DHCP. Name resolution always begins by checking these static entries, continues by checking the local DNS cache, and ends by sending requests to the external DNS server.

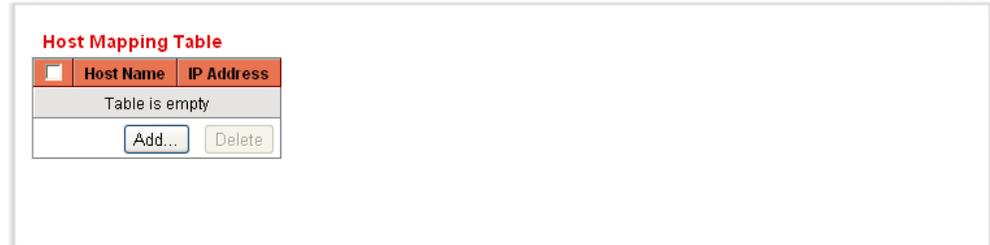
The [Host Mapping Page](#) enables configure static mappings between a DNS host name and an IP address.

Several IP addresses are supported per DNS per host name.

To add a domain name and its IP address:

1. Click **IP Configuration > Domain Name System > Host Mapping**. The [Host Mapping Page](#) is displayed.

**Figure 131: Host Mapping Page**

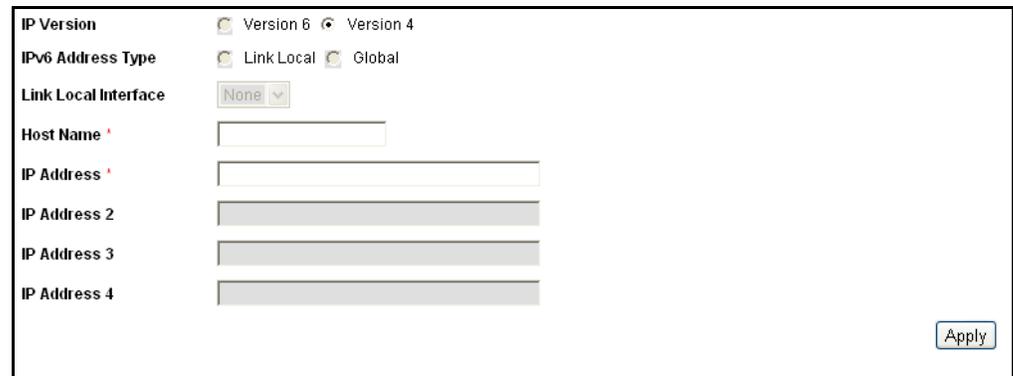


This page displays the following fields:

- ◆ **Host Name**—User-defined domain name, up to 158 characters.
- ◆ **IP Address**—The host name IP address.

2. Click **Add**. The [Add Host Mapping Page](#) is displayed.

**Figure 132: Add Host Mapping Page**



3. Enter the parameters.

- **IP Version**—Select Version 6 for IPv6 or Version 4 for IPv4.
- **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:
  - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.

- *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
  - **Link Local Interface**—If the IPv6 address type is Link Local, select whether it is received through VLAN2 or ISATAP.
  - **Host Name**—Enter a domain name, up to 158 characters.
  - **IP Address**—Enter an IP v4 IP address or enter up to four IPv6 host IP addresses. Addresses 2–4 are backup addresses.
4. Click **Apply**. The DNS host is added, and the Running Configuration file is updated with the settings.



This chapter describes various aspects of security and access control. The system handles various types of security. Some features are used for more than a single type of security or control, and so they appear twice in the list of topics below. The following list of topics describes the various types of security features described in this chapter:

Permission to administer the switch is detailed in the following sections:

- ◆ [Configuring TACACS+](#)
- ◆ [Configuring RADIUS Parameters](#)
- ◆ [Configuring Management Access Authentication](#)
- ◆ [Defining Access Profiles](#)

Protection from attacks directed at the switch CPU is detailed in the following sections:

- ◆ [Defining Storm Control](#)

Access control of end-users to the network through the switch is detailed in the following sections:

- ◆ [Configuring Management Access Authentication](#)
- ◆ [Defining Access Profiles](#)
- ◆ [Configuring TACACS+](#)
- ◆ [Configuring RADIUS Parameters](#)
- ◆ [Configuring Port Security](#)
- ◆ [Configuring 802.1X](#)

Protection from other network users is detailed in the following sections. These are attacks that pass through, but are not directed at, the switch.

- ◆ [Defining Storm Control](#)
- ◆ [Configuring Port Security](#)
- ◆ [Defining DHCP Snooping](#)
- ◆ [Defining Dynamic ARP Inspection](#)

---

## CONFIGURING TACACS+

The switch is a *Terminal Access Controller Access Control System* (TACACS+) client that relies on a TACACS+ server to provide centralized security, authorizing and authenticating users attempting to access and administer the switch.

TACACS+ provides the following services:

- ◆ **Authentication**—Provides authentication of administrators logging onto the switch by using usernames and user-defined passwords.
- ◆ **Authorization**—Performed at login. After the authentication session is completed, an authorization session starts using the authenticated username. The TACACS+ server then checks user privileges.

The TACACS+ protocol ensures network integrity, through encrypted protocol exchanges between the device and the TACACS+ server.

TACACS+ is supported only with IPv4.

TACACS+ servers cannot be used as 802.1X authentication servers to verify credentials of network users trying to join the networks through the switch.

Some TACACS+ servers support a single connection that enables the device to receive all information in a single connection. If the TACACS+ server does not support this, the device reverts back to multiple connections.

### CONFIGURING DEFAULT TACACS+ PARAMETERS

The [TACACS+ Page](#) enables adding, removing, and editing the TACACS+ servers. You can define the default parameters, such as the key string used to encrypt communications with the TACACS+ server. A user must be configured on the TACACS+ to have privilege level 15 to be granted permission to administer the switch.

To define a TACACS+ server and default TACACS+ server authentication parameters:

1. Click **Security** > **TACACS+**. The [TACACS+ Page](#) is displayed.

Figure 133: TACACS+ Page

**Use Default Parameters**

IP Version            Version 4

Key String           

Timeout for Reply \*     sec. (1 - 30)

**TACACS+ Server Table**

	Server	Priority	Key String	Timeout for Reply	Authentication IP Port	Single Connection	Status
Table is empty							
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>							

The TACACS+ Server Table displays the default parameters and the previously-defined TACACS+ servers.

2. Enter the default **Key String**. This is the authentication and encryption key used for communicating with the TACACS+ servers. The switch can be configured to use this key or to use a key for an individual server (described in the [Adding a TACACS+ Server](#) section). If you do not enter a key string in this field, the individual server key must match the encryption key used by the TACACS+ server. If you enter a key string here and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.
3. In the **Timeout for Reply** field, enter the amount of time that passes before the connection between the switch and the TACACS+ server times out. If a value is not entered in the [Add TACACS+ Server Page](#) for a specific server, the value is taken from this field.
4. Click **Apply**. The TACACS+ settings and the Running Configuration file is updated with the settings.

#### ADDING A TACACS+ SERVER

1. Click **Security > TACACS+**. The [TACACS+ Page](#) is displayed.
2. Click **Add**. The [Add TACACS+ Server Page](#) is displayed.

Figure 134: Add TACACS+ Server Page

The screenshot shows a configuration form for adding a TACACS+ server. The fields are as follows:

- Server IP Address**: An empty text input field.
- Priority**: An empty text input field with a range of (0 - 65535).
- Source IP Address**: Two radio buttons. The first is selected and labeled "Use default". The second is labeled "User defined" and has a dropdown menu showing "192.168.1.5" with the text "(Default: Set using the routing table.)" below it.
- Key String**: A text input field containing "Default" with "(Default: )" and a checked "Use default" checkbox.
- Timeout for Reply**: A text input field containing "Default" with "sec. (1 - 30, Default: 5)" and a checked "Use default" checkbox.
- Authentication IP Port**: A text input field containing "49" with "(0 - 65535)" next to it.
- Single Connection**: A dropdown menu currently set to "Enable".
- An **Apply** button is located in the bottom right corner of the form.

3. Enter the parameters.

- **Server IP Address**—Enter the TACACS+ server IP address.
- **Priority**—Enter the order that this TACACS+ server is used. Zero is the highest priority TACACS+ server and is the first server used. If it cannot establish a session with the high priority server, the switch will try the next highest priority server.
- **Key String**—Enter the authentication and encryption key for the TACACS+ server. The key must match the encryption key configured on the TACACS+ server. Select **Use Default** to use the key string defined under the TACACS+ Default Parameters.
- **Timeout for Reply**—Enter the amount of time that passes before the connection between the switch and the TACACS+ server times out. Select **Use Default** to use the default value displayed on the page.
- **Authentication IP Port**—Enter the port number through which the TACACS+ session occurs. The default is port 49.
- **Single Connection**—Select to enable a single open connection between the switch and the TACACS+ server.

4. Click **Apply**. The TACACS+ server is added, and the Running Configuration file is updated with the settings.

## CONFIGURING RADIUS PARAMETERS

Remote Authorization Dial-In User Service (RADIUS) servers provide a centralized 802.1X or MAC-based network access control. The switch is a RADIUS client that relies on a RADIUS server to provide centralized security, authorizing and authenticating users attempting to access and administer the switch.

For the RADIUS server to grant access to the web-based switch configuration utility, the RADIUS server must return `cisco-avpair = shell:priv-lvl=15`.

Use this page to enable the configuration of the RADIUS server parameters the switch uses to communicate with the servers.

To set the default RADIUS parameters:

1. Click **Security** > **RADIUS**. The **RADIUS Page** is displayed.

**Figure 135: RADIUS Page**

The screenshot shows the RADIUS configuration interface. At the top, there is a 'RADIUS Accounting' dropdown menu set to 'None'. Below this is a section titled 'Use Default Parameters' with several input fields: 'IP Version' (radio buttons for Version 6 and Version 4), 'Retries' (input field with '3', range 1-10, default 3), 'Timeout for Reply' (input field with '3', range 1-30, default 3), 'Dead Time' (input field with '0', range 0-2000, default 0), and 'Key String' (input field, ASCII Alphanumeric). 'Apply' and 'Cancel' buttons are to the right. Below is a 'RADIUS Table' with columns: Server, Priority, Key String, Timeout for Reply, Authentication Port, Accounting Port, Number of Retries, Dead Time, and Usage Type. The table is currently empty, with a message 'Table is empty' and 'Add...', 'Edit...', and 'Delete' buttons at the bottom right.

The RADIUS table displays the specific parameters for each defined RADIUS server.

2. Enter the default RADIUS parameters. Values entered in the *Default Parameters* are applied to all servers. If a value is not entered for a specific server the switch uses the values in these fields.
  - **IP Version**—Displays the supported IP version: IPv6 and/or IPv4 subnet.
  - **Number of Retries**—Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred.

- **Timeout for Reply**—Enter the number of seconds that the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server.
- **Dead Time**—Enter the number of minutes that elapse before a non-responsive RADIUS server is bypassed for service requests. If the value is 0, the server is not bypassed.
- **Key String**—Enter the default key string used for authenticating and encrypting the RADIUS attributes communicated between the switch and the RADIUS server. This key must match the key configured on the RADIUS server. A key string is used to encrypt communications by using MD5. A key configured for an individual RADIUS server has precedence over the default key that is used if there is no key provided for an individual server.

3. Click **Apply**. The RADIUS settings for the switch are updated.

To add a RADIUS Server:

1. Click **Security > RADIUS**. The [RADIUS Page](#) is displayed.
2. Click **Add**. The [Add RADIUS Server Page](#) is displayed.

**Figure 136: Add RADIUS Server Page**

The screenshot shows the 'Add RADIUS Server Page' configuration form. It includes the following fields and options:

- Host Definition:** Radio buttons for 'By IP address' (selected) and 'By name'.
- IP Version:** Radio buttons for 'Version 6' and 'Version 4' (selected).
- IPv6 Address Type:** 'Global'.
- Server IP Address:** Text input field.
- Priority:** Text input field with a range of '(0 - 65535)'. A red asterisk is next to the label.
- Source IP Address:** Radio buttons for 'Use default' (selected) and 'User defined'. The 'User defined' option has a dropdown menu showing '192.168.1.5' and a note '(Default: Set using the routing table)'. A red asterisk is next to the label.
- Key String:** Text input field with 'Default' and a dropdown menu for 'ASCII Alphanumeric (Default:)' with a checked 'Use default' checkbox. A red asterisk is next to the label.
- Timeout for Reply:** Text input field with 'Default' and a dropdown menu for 'sec. (1 - 30, Default: 3)' with a checked 'Use default' checkbox. A red asterisk is next to the label.
- Authentication Port:** Text input field with '1812' and a range of '(0 - 65535, Default: 1812)'. A red asterisk is next to the label.
- Accounting Port:** Text input field with '1813' and a range of '(0 - 65535, Default: 1813)'. A red asterisk is next to the label.
- Number of Retries:** Text input field with 'Default' and a range of '(1 - 10, Default: 3)' with a checked 'Use default' checkbox. A red asterisk is next to the label.
- Dead Time:** Text input field with 'Default' and a range of 'min. (0 - 2000, Default: 0)' with a checked 'Use default' checkbox. A red asterisk is next to the label.
- Usage Type:** Dropdown menu with 'All' selected.
- Apply:** Button in the bottom right corner.

This page provides fields that must be entered individually for a server.

3. Enter the values in the fields for each server.
  - **Host Definition**—Select whether to define the host by IP address or name.
  - **IP Version**—Select the IP version of the RADIUS server IP address.
  - **IPv6 Address Type**—Select Link Local or Global as the type of IPv6 address to enter.

- *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **Link Local Interface**—If the IPv6 address type is Link Local, select from where it is received.
  - **Server IP Address**—Enter the address of the RADIUS server.
  - **Priority**—Enter the priority of the server. The priority determines the order the switch attempts to contact the servers to authenticate a user. The switch will start with the highest priority RADIUS server first. Zero is the highest priority.
  - **Key String**—Enter the key string used for authenticating and encrypting the RADIUS attributes communicated between the switch and the RADIUS server. This key must match the key configured on the individual RADIUS server. If this field is left blank, the switch attempts to authenticate to the RADIUS server by using the default Key String.
  - **Timeout for Reply**—Enter the number of seconds the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server. If there is no value entered in this field, the switch uses the default timeout value.
  - **Authentication Port**—Enter the UDP port number of the RADUS server for authentication requests.
  - **Accounting Port**—Enter the UDP port number of the RADUS server for accounting requests.
  - **Number of Retries**—Enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred. Select **Use Default** to use the default value for the number of retries.
  - **Dead Time**—Enter the number of minutes that must pass before a non-responsive RADIUS server is bypassed for service requests. Select **Use Default** to use the default value for the dead time. If you enter 0 minutes, there is no dead time.
  - **Usage Type**—Enter the RADIUS server authentication type. The options are:
    - *Login*—RADIUS server is used for authenticating users that want to administer the switch.

- *802.1X*—RADIUS server is used for authentication in 802.1x Access Control.
  - *All*—RADIUS server is used for authenticating user that wants to administer the switch and for authentication in 802.1X Access Control.
4. Click **Apply**. The RADIUS server is added, and the Running Configuration file is updated with the settings.

## CONFIGURING MANAGEMENT ACCESS AUTHENTICATION

You can assign authentication methods to management access methods, such as SSH, console, Telnet, HTTP, and HTTPS. This authentication can be performed locally or on an external server, such as a TACACS+ or a RADIUS server.

User authentication occurs in the order that the authentication methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and all configured RADIUS servers are queried in priority order and do not reply, the user is authenticated locally.

If an authentication method fails or the user has insufficient privilege level, the user is denied access to the switch. In other words, if authentication fails at an authentication method, the switch stops; it does not continue and does not attempt to use the next authentication method.

To define authentication methods for an access method:

1. Click **Security > Management Access Authentication**. The [Management Access Authentication Page](#) is displayed.

**Figure 137: Management Access Authentication Page**

The screenshot shows a configuration interface for 'Management Access Authentication'. At the top, there is a dropdown menu labeled 'Application' with 'Console' selected. Below this, there are two columns: 'Optional Methods' and 'Selected Methods'. The 'Optional Methods' column contains a list with 'RADIUS', 'TACACS+', and 'None'. The 'Selected Methods' column contains a list with 'Local'. Between these two columns are two arrow buttons: a right-pointing arrow (>) and a left-pointing arrow (<). At the bottom right of the interface, there are two buttons: 'Apply' and 'Cancel'.

2. Select an access method from the **Application** list.

3. Use the arrows to move the authentication method between the **Optional Methods** column and the **Selected Methods** column. The first method selected is the first method that is used.
  - *RADIUS*—User is authenticated on a RADIUS server. You must have configured one or more RADIUS servers.
  - *TACACS+*—User authenticated on the TACACS+ server. You must have configured one or more TACACS+ servers.
  - *None*—User is allowed to access the switch without authentication.
  - *Local*—Username and password is checked against the data stored on the local switch. These username and password pairs are defined in the [User Accounts Page](#).



---

**NOTE:** The **Local** or **None** authentication method must always be selected last. All authentication methods selected after **Local** or **None** are ignored.

---

4. Click **Apply**. The selected authentication methods are associated with the access method.

---

## DEFINING ACCESS PROFILES

Management Access Authentication configures the authentication methods to be used to authenticate and authorize users from different management access methods. Management Access Profiles limit management access from specific interfaces and/or sources.

Only users who pass both the active access profile and management access authentication are given management access to the switch.

### ACCESS PROFILE RULES, FILTERS, AND ELEMENTS

Access profiles consist of rules for allowing access to the switch. Each access profile can consist of one or more rules. The rules are executed in order of their priority within the access profile (top to bottom).

Rules are composed of filters that include the following elements:

- ◆ **Access Methods**—Methods for accessing and managing the switch:
  - Telnet
  - Secure Telnet (SSH)
  - Hypertext Transfer Protocol (HTTP)
  - Secure HTTP (HTTPS)

- Simple Network Management Protocol (SNMP)
- All of the above
- ◆ **Action**—Permit or deny access to an interface or source address.
- ◆ **Interface**—Which ports, LAGs, or VLANs are permitted to access or denied access to the web-based switch configuration utility.
- ◆ **Source IP Address**—IP addresses or subnets. Access to management methods might differ among user groups. For example, one user group might be able to access the switch module only by using an HTTPS session, while another user group might be able to access the switch module by using both HTTPS and Telnet sessions.

### ACTIVE ACCESS PROFILE

The [Access Profiles Page](#) displays the active access profile and all access profiles created by users. Only one access profile can be active on the switch and any attempt to access the switch must fit the rules in the active access profile.

The lookup in the active access profile is done by using a first-match method. The switch looks to see if the active access profile explicitly permits management access to the switch. If no match is found, access is denied.

When an attempt to access the switch is in violation of the active access profile, the switch generates a SYSLOG message to alert the system administrator of the attempt.

If a console-only access profile has been activated, the only way to deactivate it is through a direct connection from the management station to the physical console port on the switch.

After an access profile has been defined, additional rules can be added or edited by using the [Profiles Rules Page](#).

### DISPLAYING, ADDING, OR ACTIVATING AN ACCESS PROFILE

To display, add, or select a different active access profile:

1. Click **Security > Mgmt Access Method > Access Profiles**. The [Access Profiles Page](#) is displayed.

**Figure 138: Access Profiles Page**

Active Access Profile: None

Apply Cancel

**Access Profile Table**

<input type="checkbox"/>	Access Profile Name
<input type="checkbox"/>	Console Only

Add... Delete

Profile Rules Table

This page displays all of the access profiles, active and inactive.

- To change the active access profile, select a profile from the **Active Access Profile** drop down menu and click **Apply**. This makes the chosen profile the active access profile.

A caution message is displayed if you selected Console Only. If you continue, you are immediately disconnected from the web-based switch configuration utility and can access the switch only through the console port. This only applies to device types that offer a console port.

A caution message displays if you selected any other access profile, warning you that, depending on the selected access profile, you might be disconnected from the web-based switch configuration utility.

**Figure 139: Caution Message**

This action will disconnect your session and enable access only from console. Do you want to continue?

OK Cancel

- Click **OK** to select the active access profile or click **Cancel** to discontinue the action.
- Click **Add** to open the [Add Access Profile Page](#). The page allows you to configure a new profile and one rule. Go to the [Defining Profile Rules](#) section for instructions on how to construct a rule.

Figure 140: Add Access Profile Page

The screenshot shows a configuration page for adding an access profile. It contains several sections with input fields and dropdown menus:

- Access Profile Name**: A text input field.
- Rule Priority**: A text input field with a range of (1 - 65535).
- Management Method**: A dropdown menu set to "All".
- Action**: A dropdown menu set to "Permit".
- Applies to Interface**: Radio buttons for "All" (selected) and "User defined".
- Interface**: Radio buttons for "Port" (selected), "LAG", and "VLAN". Below "Port" are dropdowns for "te0/1", "LAG" is "1", and "VLAN" is "1".
- Applies to Source IP Address**: Radio buttons for "All" (selected) and "User defined".
- IP Version**: Radio buttons for "Version 6" (selected) and "Version 4".
- IP Address**: A text input field.
- Mask**: Radio buttons for "Network Mask" and "Prefix Length". Below "Prefix Length" is a text input field with a range of (0 - 32).
- Apply**: A button in the bottom right corner.

5. Enter the parameters.

- **Access Profile Name**—Enter an access profile name. The access profile name can contain up to 32 characters.
- **Rule Priority**—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the switch. The rule priority is essential to matching packets to rules, as packets are matched on a first-match basis. One is the highest priority.
- **Management Method**—Select the management method for which the rule is defined. Users with this access profile can only access the switch by using the management method selected. The options are:
  - *All*—Assigns all management methods to the rule.
  - *Telnet*—Users requesting access to the switch who meet the Telnet access profile criteria are permitted or denied access.
  - *Secure Telnet (SSH)*—Users requesting access to the switch who meet the SSH access profile criteria, are permitted or denied access.
  - *HTTP*—Assigns HTTP access to the rule. Users requesting access to the switch who meet the HTTP access profile criteria, are permitted or denied.
  - *Secure HTTP (HTTPS)*—Users requesting access to the switch who meet the HTTPS access profile criteria, are permitted or denied.
  - *SNMP*—Users requesting access to the switch who meet the SNMP access profile criteria are permitted or denied.

- **Action**—Select the action attached to the rule. The options are:
    - *Permit*—Permits access to the switch if the user matches the settings in the profile.
    - *Deny*—Denies access to the switch if the user matches the settings in the profile.
  - **Applies to Interface**—Select the interface attached to the rule. The options are:
    - *All*—Applies to all ports, VLANs, and LAGs.
    - *User Defined*—Applies only to the port, VLAN or LAG selected.
  - **Applies to Source IP Address**—Select the type of source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnetwork. Select one of the following values:
    - *All*—Applies to all types of IP addresses.
    - *User Defined*—Applies to only those types of IP addresses defined in the fields.
  - **IP Version**—Select the supported IP version of the source address, IPv6 or IPv4.
  - **IP Address**—Enter the source IP address.
  - **Mask**—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
    - **Network Mask**—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
    - **Prefix Length**—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.
6. Click **Apply**. The access profile is created, and the Running Configuration file is updated with the settings. You can now select this access profile as the active access profile.

## DEFINING PROFILE RULES

Access profiles can contain up to 128 rules to determine who is permitted to manage and access the switch, and the access methods that may be used.

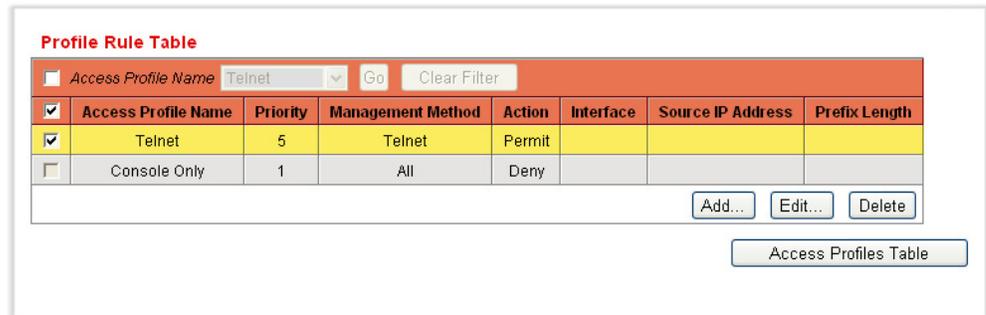
Each rule in an access profile contains an action and a criteria (one or more parameters) to match. Each rule has a priority; rules with the lowest priority are checked first. If the incoming packet matches a rule, the action associated with the rule is performed. If no matching rule is found within the active access profile, the packet is dropped.

For example, you can limit access to the switch from all IP addresses except IP addresses that are allocated to the IT management center. In this way, the switch can still be managed and has gained another layer of security.

To define profile rules:

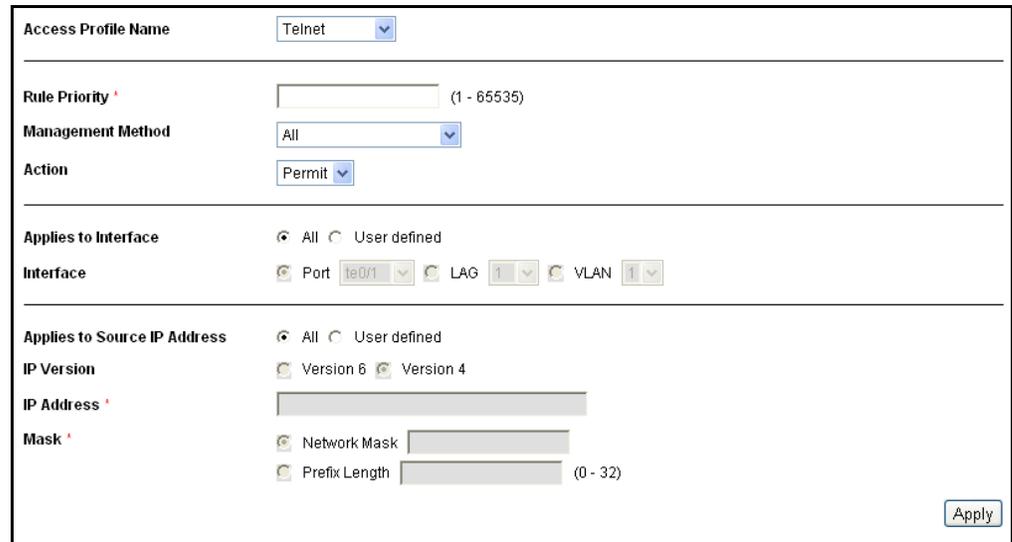
1. Click **Security > Mgmt Access Method > Profile Rules**. The [Profiles Rules Page](#) is displayed.

**Figure 141: Profiles Rules Page**



2. Select the Filter field, and an access profile. Click **Go**.
3. The selected access profile is displayed in the Profile Rule Table.
4. Click **Add** to add a rule to it. The [Add Profile Rule Page](#) is displayed.

**Figure 142: Add Profile Rule Page**



5. Enter the parameters.
  - **Access Profile Name**—Select an access profile.

- **Rule Priority**—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the switch. The rule priority is essential to matching packets to rules, as packets are matched on a first-fit basis.
- **Management Method**—Select the management method for which the rule is defined. The options are:
  - *All*—Assigns all management methods to the rule.
  - *Telnet*—Users requesting access to the switch who meet the Telnet access profile criteria are permitted or denied access.
  - *Secure Telnet (SSH)*—Users requesting access to the switch who meet the Telnet access profile criteria, are permitted or denied access.
  - *HTTP*—Assigns HTTP access to the rule. Users requesting access to the switch who meet the HTTP access profile criteria, are permitted or denied.
  - *Secure HTTP (HTTPS)*—Users requesting access to the switch who meet the HTTPS access profile criteria, are permitted or denied.
  - *SNMP*—Users requesting access to the switch who meet the SNMP access profile criteria are permitted or denied.
- **Action**—Select **Permit** to permit the users that attempt to access the switch by using the configured access method from the interface and IP source defined in this rule. Or select **Deny** to deny access.
- **Applies to Interface**—Select the interface attached to the rule. The options are:
  - *All*—Applies to all ports, VLANs, and LAGs.
  - *User Defined*—Applies only to the port, VLAN, or LAG selected.
- **Applies to Source IP Address**—Select the type of source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnetwork. Select one of the following values:
  - *All*—Applies to all types of IP addresses.
  - *User Defined*—Applies to only those types of IP addresses defined in the fields.
- **IP Version**—Select the supported IP version of the source address: IPv6 or IPv4.
- **IP Address**—Enter the source IP address.

- **Mask**—Select the format for the subnet mask for the source IP address, and enter a value in one of the field:
    - *Network Mask*—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
    - *Prefix Length*—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.
6. Click **Apply**, and the rule is added to the access profile.

## DEFINING STORM CONTROL

When Broadcast, Multicast, or Unknown Unicast frames are received, they are duplicated, and a copy is sent to all possible egress ports. This means that in practice they are sent to all ports belonging to the relevant VLAN. In this way, one ingress frame is turned into many, creating the potential for a storm.

Storm protection enables you to limit the number of frames entering the switch and to define the types of frames that are counted towards this limit.

When a threshold (limit) is entered in the system, the port discards traffic after that threshold is reached. The port remains blocked until the traffic rate drops below this threshold. It then resumes normal forwarding.

To define Storm Control:

1. Click **Security > Storm Control**. The [Storm Control Page](#) is displayed.

**Figure 143: Storm Control Page**

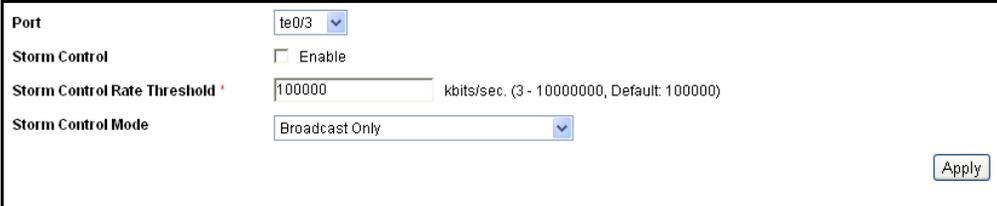
Storm Control Table						
	Entry No.	Port	Storm Control	Storm Control Rate Threshold (Kbits/sec.)	Storm Control Rate Threshold (%)	Storm Control Mode
<input type="radio"/>	1	te0/1	Disabled	100000	10.0	Broadcast Only
<input type="radio"/>	2	te0/2	Disabled	100000	1.0	Broadcast Only
<input type="radio"/>	3	te0/3	Disabled	100000	1.0	Broadcast Only
<input type="radio"/>	4	te0/4	Disabled	100000	1.0	Broadcast Only
<input type="radio"/>	5	te0/5	Disabled	100000	1.0	Broadcast Only
<input type="radio"/>	6	te0/6	Disabled	100000	1.0	Broadcast Only
<input type="radio"/>	7	te0/7	Disabled	100000	1.0	Broadcast Only
<input type="radio"/>	8	te0/8	Disabled	100000	1.0	Broadcast Only
<input type="radio"/>	9	te0/9	Disabled	100000	1.0	Broadcast Only
<input type="radio"/>	10	te0/10	Disabled	100000	1.0	Broadcast Only

This page displays storm control parameters for all ports.

All the fields on this page are described in the [Edit Storm Control Page](#) except for the **Storm Control Rate Threshold (%)**. It displays the percent of the total available bandwidth for unknown Unicast, Multicast, and Broadcast packets before storm control is applied at the port. The default value is 10% of the maximum rate of the port and is set in the [Edit Storm Control Page](#).

2. Select a port and click **Edit**. The [Edit Storm Control Page](#) is displayed.

**Figure 144: Edit Storm Control Page**



The screenshot shows a configuration form for storm control on a specific port. The form includes the following fields and options:

- Port:** A dropdown menu with "te0/3" selected.
- Storm Control:** A checkbox labeled "Enable" which is currently unchecked.
- Storm Control Rate Threshold:** A text input field containing "100000" with a unit of "kbits/sec. (3 - 10000000, Default: 100000)".
- Storm Control Mode:** A dropdown menu with "Broadcast Only" selected.
- Apply:** A button located at the bottom right of the form.

3. Enter the parameters.
  - **Port**—Select the port for which storm control is enabled.
  - **Storm Control**—Select to enable Storm Control.
  - **Storm Control Rate Threshold**—Enter the maximum rate at which unknown packets can be forwarded. The default for this threshold is 10,000 for FE devices and 100,000 for GE devices.
  - **Storm Control Mode**—Select one of the modes:
    - *Unknown Unicast, Multicast & Broadcast*—Counts unknown Unicast, Broadcast, and Multicast traffic together towards the bandwidth threshold.
    - *Multicast & Broadcast*—Counts Broadcast and Multicast traffic together towards the bandwidth threshold.
    - *Broadcast Only*—Counts only Broadcast traffic towards the bandwidth threshold.
4. Click **Apply**. Storm control is modified, and the Running Configuration file is updated with the settings.

---

## CONFIGURING PORT SECURITY

Network security can be increased by limiting access on a port to users with specific MAC addresses. The MAC addresses can be either dynamically learned or statically configured.

Port security monitors received and learned packets. Access to locked ports is limited to users with specific MAC addresses.

Port Security has two modes:

- ◆ **Classic Lock**—All learned MAC addresses on the port are locked, and the port does not learn any new MAC addresses. The learned addresses are not subject to aging or re-learning.
- ◆ **Limited Dynamic Lock**—The switch learns MAC addresses up to the configured limit of allowed addresses. After the limit is reached the switch does not learn additional addresses. In this mode, the addresses are subject to aging and re-learning.

When a frame from a new MAC address is detected on a port where it is not authorized (the port is classically locked, and there is a new MAC address, or the port is dynamically locked, and the maximum number of allowed addresses has been exceeded), the protection mechanism is invoked, and one of the following actions can take place:

- ◆ Frame is discarded
- ◆ Frame is forwarded
- ◆ Port is shut down

When the secure MAC address is seen on another port, the frame is forwarded, but the MAC address is not learned on that port.

In addition to one of these actions, you can also generate traps, and limit their frequency and number to avoid overloading the devices.



**NOTE:** If you want to use 802.1X on a port, it must be multiple host mode (see the 802.1x, [Host and Session Authentication Page](#)).

---

The [Port Security Page](#) displays security parameters for all ports and LAGs, and enables their modification.

To configure port security:

1. Click **Security > Port Security**. The [Port Security Page](#) is displayed.

Figure 145: Port Security Page

**Port Security Table**

Interface Type: Port

Entry No.	Interface	Interface Status	Learning Mode	Max No. of Address Allowed	Action on Violation	Trap	Trap Frequency (sec.)
1	te0/1	Unlocked	Classic Lock	1		Disabled	10
2	te0/2	Unlocked	Classic Lock	1		Disabled	10
3	te0/3	Unlocked	Classic Lock	1		Disabled	10
4	te0/4	Unlocked	Classic Lock	1		Disabled	10
5	te0/5	Unlocked	Classic Lock	1		Disabled	10
6	te0/6	Unlocked	Classic Lock	1		Disabled	10
7	te0/7	Unlocked	Classic Lock	1		Disabled	10
8	te0/8	Unlocked	Classic Lock	1		Disabled	10
9	te0/9	Unlocked	Classic Lock	1		Disabled	10
10	te0/10	Unlocked	Classic Lock	1		Disabled	10

This page displays information either for all ports or for all LAGs, depending on which interface type is selected.

2. Select an interface to be modified, and click **Edit**. The [Edit Port Security Interface Settings Page](#) is displayed.

Figure 146: Edit Port Security Interface Settings Page

Interface:  Port te0/3  LAG 1

Interface Status:  Lock

Learning Mode: Classic Lock

Max No. of Address Allowed: 1 (0 - 128, Default: 1)

Action on Violation: Discard

Trap:  Enable

Trap Frequency: 10 sec. (1 - 1000000, Default: 10)

Apply

3. Enter the parameters.
  - **Interface**—Select the interface name.
  - **Interface Status**—Select to lock the port.
  - **Learning Mode**—Select the type of port locking. To configure this field, the Interface Status must be unlocked. The Learning Mode field is enabled only if the *Interface Status* field is locked. To change the Learning Mode, the Lock Interface must be cleared. After the mode is changed, the Lock Interface can be reinstated. The options are:
    - *Classic Lock*—Locks the port immediately, regardless of the number of addresses that have already been learned.

- *Limited Dynamic Lock*—Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both re-learning and aging of MAC addresses are enabled.
  - **Max No. of Addresses Allowed**—Enter the maximum number of MAC addresses that can be learned on the port if *Limited Dynamic Lock* learning mode is selected. The range is 0-256 and the default is 1. The number 0 indicates that only static addresses are supported on the interface.
  - **Action on Violation**—Select an action to be applied to packets arriving on a locked port. The options are:
    - *Discard*—Discards packets from any unlearned source.
    - *Forward*—Forwards packets from an unknown source without learning the MAC address.
    - *Shutdown*—Discards packets from any unlearned source, and shuts down the port. The port remains shut down until reactivated, or until the switch is rebooted.
  - **Trap**—Select to enable traps when a packet is received on a locked port. This is relevant for lock violations. For Classic Lock, this is any new address received. For Limited Dynamic Lock, this is any new address that exceeds the number of allowed addresses.
  - **Trap Frequency**—Enter minimum time (in seconds) that elapses between traps.
4. Click **Apply**. Port security is modified, and the Running Configuration file is updated with the settings.

---

## CONFIGURING 802.1X

Port-based access control has the effect of creating two types of access on the switch ports. One point of access enables uncontrolled communication, regardless of the authorization state (*uncontrolled port*). The other point of access authorizes communication between the host and the switch.

The 802.1x is an IEEE standard for port based network access control. The 802.1x framework enables a device (the supplicant) to request port access from a remote device (authenticator) to which it is connected. Only when the supplicant requesting port access is authenticated and authorized is the supplicant permitted to send data to the port. Otherwise, the authenticator discards the supplicant data unless the data is sent to a Guest VLAN and/or non-authenticated VLANs.

Authentication of the supplicant is performed by an external RADIUS server through the authenticator. The authenticator monitors the result of the authentication.

In the 802.1x standard, a device can be a supplicant and an authenticator at a port simultaneously, requesting port access and granting port access. However, this device is only the authenticator, and does not take on the role of a supplicant.

The following varieties of 802.1X exist:

◆ **Single session 802.1X:**

- **A1**—Single-session/single host. In this mode, the switch, as an authenticator supports one 802.1x session and grants permission to use the port to the authorized supplicant at a port. All the access by the other devices received from the same port are denied until the authorized supplicant is no longer using the port or the access is to the unauthenticated VLAN or guest VLAN.
- Single session/multiple hosts—This follows the 802.1x standard. In this mode, the switch as an authenticator allows any device to use a port as long as it has been granted permission to a supplicant at the port.

- ◆ **Multi-Session 802.1X**—Every device (supplicant) connecting to a port must be authenticated and authorized by the switch (authenticator) separately in a different 802.1x session. This is the only mode that supports Dynamic VLAN Assignment (DVA).

### DYNAMIC VLAN ASSIGNMENT (DVA)

Dynamic VLAN Assignment (DVA) is also referred as RADIUS VLAN Assignment in this guide. When a port is in Multiple Session mode and is DVA-enabled, the switch automatically adds the port as an untagged member of the VLAN that is assigned by the RADIUS server during the authentication process. The switch classifies untagged packets to the assigned VLAN if the packets are originated from the devices or ports that are authenticated and authorized.

For a device to be authenticated and authorized at a port with DVA enabled:

- ◆ The RADIUS server must authenticate the device and dynamically assign a VLAN to the device.
- ◆ The assigned VLAN must not be the default VLAN and must have been created at the switch.
- ◆ The switch must not be configured to use both a DVA and a MAC-based VLAN group together.
- ◆ A RADIUS server must support DVA with RADIUS attributes tunnel-type (64) = VLAN (13), tunnel-media-type (65) = 802 (6), and tunnel-private-group-id = a VLAN ID.

## AUTHENTICATION METHODS

The authentication methods can be:

- ◆ 802.1x—The switch supports the authentication mechanism as described in the standard to authenticate and authorize 802.1x supplicants.
- ◆ MAC-based—The switch can be configured to use this mode to authenticate and authorized devices that do not support 802.1x. The switch emulates the supplicant role on behalf of the non 802.1x capable devices, and uses the MAC address of the devices as the username and password when communicating with the RADIUS servers. MAC addresses for username and password must be entered in lower case and with no delimiting characters (for example: aaccbb55ccff). To use MAC-based authentication at a port:
  - A Guest VLAN must be defined
  - The port must be Guest VLAN enabled.
  - The packets from the first supplicant at the port before it is authorized must be untagged packets.

You can configure a port to use 802.1x, MAC-based, or 802.1x and MAC-based authentication. If a port is configured to use both 802.1x and MAC-based authentication, 802.1x supplicant has precedence over non-802.1x device. The 802.1x supplicant preempts an authorized but non-802.1x device at a port that is configured with a single session.

## UNAUTHENTICATED VLANS AND THE GUEST VLAN

Unauthenticated VLANs and Guest VLAN provide access to services that do not require the subscribing devices or ports to be 802.1x or MAC-Based authenticated and authorized.

An unauthenticated VLAN is a VLAN that allows access by both authorized and unauthorized devices or ports. You can configure one or more VLAN to be an unauthenticated in the [Creating VLANs](#) section. An unauthenticated VLAN has the following characteristics:

- ◆ It must be a static VLAN, and cannot be the Guest VLAN or the Default VLAN.
- ◆ The member ports must be manually configured as tagged members.
- ◆ The member ports must be trunk and/or general ports. An access port cannot be member of an unauthenticated VLAN.

The Guest VLAN, if configured, is a static VLAN with the following characteristics.

- ◆ Must be manually defined from an existing static VLAN.
- ◆ Is automatically available only to unauthorized devices or ports of devices that are connected and Guest VLAN enabled.

- ◆ If a port is Guest VLAN enabled, the switch automatically adds the port as untagged member of the Guest VLAN when the port is not authorized, and remove the port from the Guest VLAN when the first supplicant of the port is authorized.
- ◆ The Guest VLAN cannot be used as the Voice VLAN and an unauthenticated VLAN.

The switch also uses the Guest VLAN for the authentication process at ports configured with Multiple Session mode and MAC-Based Authentication. Therefore, you must configure a Guest VLAN before you can use the MAC authentication mode.

### 802.1X PARAMETERS WORKFLOW

Define the 802.1X parameters as follows:

1. Define one or more static VLANs as unauthenticated VLANs as described in the [Defining 802.1X Properties](#) section. 802.1x authorized and unauthorized devices or ports can always send or receive packets to or from unauthenticated VLANs. *This is optional.*
2. Define 802.1X settings for each port by using the [Edit Port Authentication Page](#). Note the following:
  - a. On this page, DVA can be activated on a port by selecting the RADIUS VLAN Assignment field.
  - b. You can select the Guest VLAN field to have untagged incoming frames go to the guest VLAN.
3. Define host authentication parameters for each port using the [Port Authentication Page](#).

### DEFINING 802.1X PROPERTIES

The [Properties Page](#) is used to globally enable 802.1X. For 802.1X to function, it must be activated both globally and individually on each port.

To define port-based authentication:

1. Click **Security** > **802.1X** > **Properties**. The [Properties Page](#) is displayed.

Figure 147: Properties Page

Port-Based Authentication: Enable

Authentication Method: RADIUS

Guest VLAN: Disable

Guest VLAN ID: 1

Guest VLAN Timeout:  Immediate  User defined  sec. (30 - 180)

Apply Cancel

**VLAN Authentication Table**

VLAN ID	VLAN Name	Authentication
<input checked="" type="radio"/> 123	Test	Enabled
<input type="button" value="Edit..."/>		

2. Enter the parameters.

- **Port Based Authentication**—Enable or disable port-based, 802.1X authentication.
- **Authentication Method**—Select the user authentication methods. The options are:
  - *RADIUS, None*—Perform port authentication first by using the RADIUS server. If no response is received from RADIUS (for example, if the server is down), then no authentication is performed, and the session is permitted. If the server is available but the user credentials are incorrect, access will be denied and the session terminated.
  - *RADIUS*—Authenticate the user on the RADIUS server. If no authentication is performed, the session is not permitted
  - *None*—Do not authenticate the user. Permit the session.
- **Guest VLAN**—Select to enable the use of a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, all unauthorized ports automatically join the VLAN selected in the *Guest VLAN ID* field. If a port is later authorized, it is removed from the Guest VLAN.
- **Guest VLAN ID**—Select the guest VLAN from the list of VLANs.
- **Guest VLAN Timeout**—Define a time period:
  - After linkup, if the software does not detect the 802.1X supplicant, or the authentication has failed, the port is added to the Guest VLAN, only after the *Guest VLAN timeout* period has expired.

- If the port state changes from *Authorized* to *Not Authorized*, the port is added to the Guest VLAN only after the *Guest VLAN* timeout has expired.

The VLAN Authentication Table displays all VLANs, and indicates whether authentication has been enabled on them.

3. Click **Apply**. The 802.1X properties are modified, and the Running Configuration file is updated with the settings.

### CONFIGURING UNAUTHENTICATED VLANS

When a port is 802.1x-enabled, unauthorized ports or devices are not allowed to access a VLAN unless the VLAN is a Guest VLAN or unauthenticated VLAN. You can make a static VLAN an authenticated VLAN by using the procedure in the [Defining 802.1X Properties](#) section, allowing both 802.1x authorized and unauthorized devices or ports to send or receive packets to or from unauthenticated VLANs. You must manually add VLAN port membership by using the Port to VLAN page.

1. Click **Security > 802.1X > Properties**. The [Properties Page](#) is displayed.
2. Select a VLAN, and click **Edit**. The [Edit VLAN Authentication Page](#) is displayed.

**Figure 148: Edit VLAN Authentication Page**

VLAN ID	123
VLAN Name	Test
Authentication	Enable

3. Select a VLAN.
4. Optionally, disable **Authentication** to make the VLAN an unauthenticated VLAN.
5. Click **Apply**, and the Running Configuration file is updated with the settings.

### DEFINING 802.1X PORT AUTHENTICATION

The [Port Authentication Page](#) enables configuration of several of the 802.1X parameters for each port. Since some of the configuration changes are only possible while the port is in *Force Authorized* state, such as host authentication, it is recommended that you change the port control to *Force Authorized* before making changes. When the configuration is complete, return the port control to its previous state.



**NOTE:** A port with 802.1x defined on it cannot become a member of a LAG.

To define 802.1X authentication:

1. Click **Security > 802.1X > Port Authentication**. The [Port Authentication Page](#) is displayed.

**Figure 149: Port Authentication Page**

Port Authentication Table									
	Entry No.	Port	User Name	Current Port Control	RADIUS VLAN Assignment	Guest VLAN	Authentication Method	Periodic Reauthentication	Reauthentication Period
<input type="checkbox"/>	1	te0/1		Authorized	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	2	te0/2		N/A	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	3	te0/3		N/A	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	4	te0/4		N/A	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	5	te0/5		N/A	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	6	te0/6		N/A	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	7	te0/7		N/A	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	8	te0/8		N/A	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	9	te0/9		N/A	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	10	te0/10		N/A	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	11	te0/11		N/A	Disabled	Disabled	802.1x Only	Disabled	3600
<input type="checkbox"/>	12	te0/12		N/A	Disabled	Disabled	802.1x Only	Disabled	3600

This page displays authentication settings for all ports.

2. Select a port, and click **Edit**. The [Edit Port Authentication Page](#) is displayed.

**Figure 150: Edit Port Authentication Page**

Port	te0/4
User Name	
Current Port Control	Authorized
Administrative Port Control	Force Authorized
RADIUS VLAN Assignment	<input type="checkbox"/> Enable
Guest VLAN	<input type="checkbox"/> Enable
Authentication Method	802.1x Only
Periodic Reauthentication	<input type="checkbox"/> Enable
Reauthentication Period *	3600 sec. (300 - 4294967295, Default: 3600)
Reauthenticate Now	<input type="checkbox"/>
Authenticator State	Initialize
Quiet Period *	60 sec. (0 - 65535, Default: 60)
Resending EAP *	30 sec. (30 - 65535, Default: 30)
Max EAP Requests *	2 (1 - 10, Default: 2)
Supplicant Timeout *	30 sec. (1 - 65535, Default: 30)
Server Timeout *	30 sec. (1 - 65535, Default: 30)
Termination Cause	Port re-initialize

Enter the parameters.

- **Port**—Select a port.
- **User Name**—Displays the username of the port.
- **Current Port Control**—Displays the current port authorization state. If the state is *Authorized*, the port is either authenticated or the *Administrative Port Control* is *Force Authorized*. Conversely, if the state is *Unauthorized*, then the port is either not authenticated or the *Administrative Port Control* is *Force Unauthorized*.
- **Administrative Port Control**—Select the Administrative Port Authorization state. The options are:
  - *Force Unauthorized*—Denies the interface access by moving the interface into the unauthorized state. The switch does not provide authentication services to the client through the interface.
  - *Auto*—Enables port-based authentication and authorization on the switch. The interface moves between an authorized or unauthorized state based on the authentication exchange between the switch and the client.
  - *Force Authorized*—Authorizes the interface without authentication.
- **RADIUS VLAN Assignment**—Select to enable Dynamic VLAN assignment on the selected port. Dynamic VLAN assignment is possible only when the 802.1X mode is set to multiple session. (After authentication, the port joins the supplicant VLAN as an untagged port in that VLAN.)



**NOTE:** For the Dynamic VLAN Assignment feature to work, the switch requires the following VLAN attributes to be sent by the RADIUS server (as defined in RFC 3580):

[64] Tunnel-Type = VLAN (type 13)

[65] Tunnel-Medium-Type = 802 (type 6)

[81] Tunnel-Private-Group-Id = VLAN ID

- **Guest VLAN**—Select to indicate that the usage of a previously-defined Guest VLAN is enabled for the switch. The options are:
  - *Selected*—Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the *Guest VLAN ID* field in the *802.1X Port Authentication Page*. After an authentication failure and if Guest VLAN is activated globally and on a given port, the guest VLAN is automatically assigned to the unauthorized ports as an Untagged VLAN.
  - *Cleared*—Disables Guest VLAN on the port.

- **Authentication Method**—Select the authentication method for the port. The options are:
  - *802.1X Only*—802.1X authentication is the only authentication method performed on the port.
  - *MAC Only*—Port is authenticated based on the supplicant MAC address. Only 8 MAC-based authentications can be used on the port.
  - *802.1X and MAC*—Both 802.1X and MAC-based authentication are performed on the switch. The 802.1X authentication takes precedence.



---

**NOTE:** For MAC authentication to succeed, the RADIUS server supplicant username and password must be the supplicant MAC address. The MAC address must be in lower case letters and entered without the ":" or "-" separators; for example: 0020aa00bbcc.

---

- **Periodic Reauthentication**—Select to enable port re-authentication attempts after the specified Reauthentication Period.
- **Reauthentication Period**—Enter the number of seconds after which the selected port is reauthenticated.
- **Reauthenticate Now**—Select to enable immediate port re-authentication.
- **Authenticator State**—Displays the defined port authorization state. The options are:
  - *Force-Authorized*—Controlled port state is set to Force-Authorized (forward traffic).
  - *Force-Unauthorized*—Controlled port state is set to Force-Unauthorized (discard traffic).



---

**NOTE:** If the port is not in Force-Authorized or Force-Unauthorized, it is in Auto Mode and the authenticator displays the state of the authentication in progress. After the port is authenticated, the state is shown as Authenticated.

---

- **Quiet Period**—Enter the number of seconds that the switch remains in the quiet state following a failed authentication exchange.
- **Resending EAP**—Enter the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.

- **Max EAP Requests**—Enter the maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.
  - **Supplicant Timeout**—Enter the number of seconds that lapses before EAP requests are resent to the supplicant.
  - **Server Timeout**—Enter the number of seconds that lapses before the switch resends a request to the authentication server.
  - **Termination Cause**—Displays the reason for which the port authentication was terminated, if applicable.
3. Click **Apply**. The port settings are defined, and the Running Configuration file is updated with the settings.

## DEFINING HOST AND SESSION AUTHENTICATION

The [Host and Session Authentication Page](#) enables defining the mode in which 802.1X operates on the port and the action to perform if a violation has been detected.

The 802.1X modes are:

- ◆ *Single*—Only a single authorized host can access the port. (Port Security cannot be enabled on a port in single-host mode.)
- ◆ *Multiple Host (802.1X)*—Multiple hosts can be attached to a single 802.1X-enabled port. Only the first host must be authorized, and then the port is wide-open for all who want to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
- ◆ *Multiple Sessions*—Enables number of specific authorized hosts to access the port. Each host is treated as if it were the first and only user and must be authenticated. Filtering is based on the source MAC address.

To define 802.1X advanced settings for ports:

1. Click **Security > 802.1X > Host and Session Authentication**. The [Host and Session Authentication Page](#) is displayed.

Figure 151: Host and Session Authentication Page

Host and Session Authentication Table								
	Entry No.	Port	Host Authentication	Action on Violation	Traps	Trap Frequency	Status	Number of Violations
<input type="radio"/>	1	te0/1	Multiple Sessions	Discard	Disabled	10	No Single-host	0
<input type="radio"/>	2	te0/2	Multiple Sessions	Discard	Disabled	10	No Single-host	0
<input type="radio"/>	3	te0/3	Multiple Sessions	Discard	Disabled	10	No Single-host	0
<input checked="" type="radio"/>	4	te0/4	Multiple Sessions	Discard	Disabled	10	No Single-host	0
<input type="radio"/>	5	te0/5	Multiple Sessions	Discard	Disabled	10	No Single-host	0
<input type="radio"/>	6	te0/6	Multiple Sessions	Discard	Disabled	10	No Single-host	0
<input type="radio"/>	7	te0/7	Multiple Sessions	Discard	Disabled	10	No Single-host	0
<input type="radio"/>	8	te0/8	Multiple Sessions	Discard	Disabled	10	No Single-host	0
<input type="radio"/>	9	te0/9	Multiple Sessions	Discard	Disabled	10	No Single-host	0
<input type="radio"/>	10	te0/10	Multiple Sessions	Discard	Disabled	10	No Single-host	0

802.1X authentication parameters are described for all ports. All fields except the following are described in the [Edit Host and Session Authentication Page](#).

- ◆ **Status**—Displays the host status. An asterisk indicates that the port is either not linked or is down. The options are:
    - *Unauthorized*—Either the port control is *Force Unauthorized* and the port link is down, or the port control is *Auto* but a client has not been authenticated via the port.
    - *Force-Authorized*—Clients have full port access.
    - *Single-host Lock*—Port control is *Auto* and only a single client has been authenticated by using the port.
    - *No Single host*—Port control is *Auto* and Multiple Hosts mode is enabled. At least one client has been authenticated.
    - *Not in Auto Mode*—Auto port control is not enabled.
  - ◆ **Number of Violations**—Displays the number of packets that arrive on the interface in single-host mode, from a host whose MAC address is not the supplicant MAC address.
2. Select a port, and click **Edit**. The [Edit Host and Session Authentication Page](#) is displayed.

**Figure 152: Edit Host and Session Authentication Page**

The screenshot shows a configuration page with the following fields and values:

- Port:** te0/4
- Host Authentication:** Multiple Sessions
- Action on Violation:** Discard
- Traps:**  Enable
- Trap Frequency:** 10 sec. (1 - 1000000, Default: 10)

Buttons: Apply, Close

**3.** Enter the parameters.

- **Port**—Enter a port number for which host authentication is enabled.
- **Host Authentication**—Select one of the modes. These modes are described above in [Defining Host and Session Authentication](#).
- The following fields are only relevant if you select *Single* in the Host Authentication field.
- **Action on Violation**—Select the action to be applied to packets arriving in Single Session/Single Host mode, from a host whose MAC address is not the supplicant MAC address. The options are:
  - *Discard*—Discards the packets.
  - *Forward*—Forwards the packets.
  - *Shutdown*—Discards the packets and shuts down the port. The ports remains shut down until reactivated, or until the switch is rebooted.
- **Traps**—Select to enable traps.
- **Trap Frequency**—Defines how often traps are sent to the host. This field can be defined only if multiple hosts are disabled.

**4.** Click **Apply**. The settings are defined, and the Running Configuration file is updated with the settings.

## DEFINING DHCP SNOOPING

DHCP snooping is a feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database (table). DHCP snooping acts as a firewall between untrusted hosts and DHCP servers. DHCP snooping differentiates between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

The DHCP Snooping section contains the following topics:

- ◆ [Defining DHCP Snooping Properties](#)
- ◆ [Defining DHCP Snooping on VLANs](#)
- ◆ [Defining Trusted Interfaces](#)
- ◆ [Binding Addresses to the DHCP Snooping Database](#)

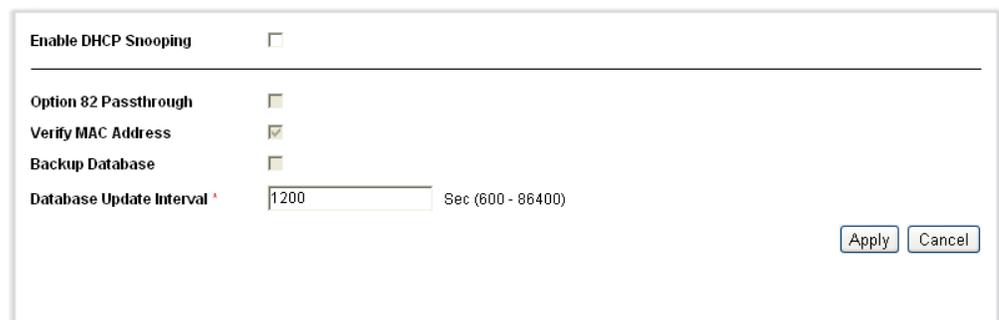
### DEFINING DHCP SNOOPING PROPERTIES

The [Properties Page](#) contains parameters for enabling DHCP Snooping on the device.

To define the DHCP Snooping general properties:

1. Click **Security > DHCP Snooping > Properties**. The [Properties Page](#) is displayed.

**Figure 153: Properties Page**



The screenshot shows a configuration window for DHCP Snooping properties. It includes the following fields and controls:

- Enable DHCP Snooping**: A checkbox that is currently unchecked.
- Option 82 Passthrough**: A checkbox that is currently unchecked.
- Verify MAC Address**: A checkbox that is currently checked.
- Backup Database**: A checkbox that is currently unchecked.
- Database Update Interval**: A text input field containing the value "1200". To the right of the field is the unit "Sec (600 - 86400)".
- Buttons**: "Apply" and "Cancel" buttons are located at the bottom right of the window.

The [Properties Page](#) contains the following fields:

- ◆ **Enable DHCP Snooping**—Indicates if DHCP Snooping is enabled on the device. The possible field values are:
  - *Checked*—Enables DHCP Snooping on the device.
  - *Unchecked*—Disables DHCP Snooping on the device. This is the default value.

- ◆ **Option 82 Passthrough**—Indicates if the device forwards or rejects packets that include Option 82 information, while DHCP Snooping is enabled.
    - *Checked*—Device forwards packets containing Option 82 information.
    - *Unchecked*—Device rejects packets containing Option 82 information.
  - ◆ **Verify MAC Address**—Indicates if the MAC address is verified. The possible field values are:
    - *Checked*—Verifies (on an untrusted port) that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header (part of the payload).
    - *Unchecked*—Disables verifying that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header. This is the default value.
  - ◆ **Backup Database**—Indicates if the DHCP Snooping Database learning and update is enabled. All changes to the binding storage file are implemented only if the device's system clock is synchronized with the SNTP Server. The possible field values are:
    - *Checked*—Enables backing up of the allotted IP address in the DHCP Snooping Database.
    - *Unchecked*—Disables backing up to the allotted IP address in the DHCP Snooping Database. This is the default value.
  - ◆ **Database Update Interval**—Indicates how often the DHCP Snooping Database is backed up. The possible field range is 600 – 86400 seconds. The field default is 1200 seconds.
2. Modify the relevant fields.
  3. Click **Apply**. The settings are defined, and the Running Configuration file is updated with the settings..

## DEFINING DHCP SNOOPING ON VLANS

The [VLAN Settings Page](#) allows network managers to enable DHCP snooping on VLANs. To enable DHCP Snooping on a VLAN, ensure DHCP Snooping is enabled on the device.

To define DHCP Snooping on VLANs:

1. Click **Security > DHCP Snooping > VLAN Settings**. The [VLAN Settings Page](#) is displayed.

Figure 154: VLAN Settings Page



The [VLAN Settings Page](#) contains the following fields:

- ◆ **VLAN ID**—Indicates the VLAN to be added to the Enabled VLAN list.
  - ◆ **Enabled VLANs**—Contains a list of VLANs for which DHCP Snooping is enabled.
2. Modify the relevant fields.
  3. Click **Apply**. The settings are defined, and the Running Configuration file is updated with the settings.

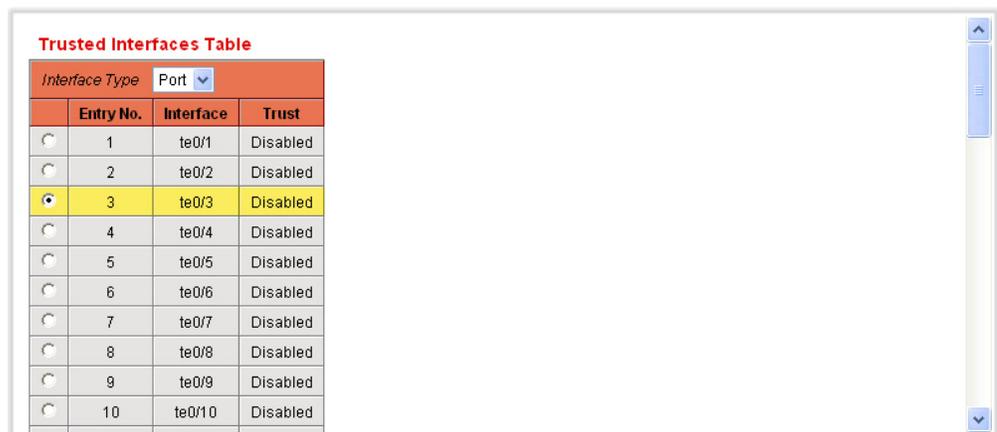
## DEFINING TRUSTED INTERFACES

The [Trusted Interfaces Page](#) allows network managers to define Trusted interfaces. The device transfers all DHCP requests to trusted interfaces.

To define trusted interfaces:

1. Click **Security > DHCP Snooping > Trusted Interfaces**. The [Trusted Interfaces Page](#) is displayed.

Figure 155: Trusted Interfaces Page



Trusted Interfaces Table			
Interface Type		Port	
Entry No.	Interface	Trust	
<input type="radio"/>	1	te0/1	Disabled
<input type="radio"/>	2	te0/2	Disabled
<input checked="" type="radio"/>	3	te0/3	Disabled
<input type="radio"/>	4	te0/4	Disabled
<input type="radio"/>	5	te0/5	Disabled
<input type="radio"/>	6	te0/6	Disabled
<input type="radio"/>	7	te0/7	Disabled
<input type="radio"/>	8	te0/8	Disabled
<input type="radio"/>	9	te0/9	Disabled
<input type="radio"/>	10	te0/10	Disabled

This page displays information either for all ports or for all LAGs, depending on which interface type is selected.

2. Select an interface to be modified, and click **Edit**. The [Edit Trusted Interface Page](#) is displayed.

**Figure 156: Edit Trusted Interface Page**

3. Enter the parameters.
  - **Interface**—Select the interface name.
  - **Trust Status**—Select whether the interface is a Trusted Interface. The possible field values are:
    - *Enable*—Interface is in trusted mode.
    - *Disable*—Interface is in untrusted mode.
4. Click **Apply**. The Trusted Interfaces configuration is defined and the Running Configuration file is updated with the settings..

## BINDING ADDRESSES TO THE DHCP SNOOPING DATABASE

The [Binding Database Page](#) contains parameters for querying and adding IP addresses to the DHCP Snooping Database.

To bind addresses to the DHCP Snooping database:

1. Click **Security > DHCP Snooping > Binding Database**. The [Binding Database Page](#) is displayed.

**Figure 157: Binding Database Page**

The [Binding Database Page](#) contains the following fields:

- ◆ **Supported IP Format**—Indicates only IPv4 is supported.
- 2. Define any of the following fields as a query filter:
  - **MAC Address**—Indicates the MAC addresses recorded in the DHCP Database. The Database can be queried by MAC address.
  - **IP Address**—Indicates the IP addresses recorded in the DHCP Database. The Database can be queried by IP address.
  - **Vlan**—Indicates the VLANs recorded in the DHCP Database. The Database can be queried by VLAN.
  - **Interface Type**—Contains a list of interface by which the DHCP Database can be queried. The possible field values are:
    - *Unit No.* and *Port*—Queries the VLAN database by a specific stacking member and port number.
    - *LAG*—Queries the VLAN database by LAG number.
- 3. Click **Query**. The results appear in the *Query Results* table.

The *Query Results* table contains the following fields:

- **MAC Address**—Indicates the MAC address found during the query.
- **VLAN ID**—Displays the VLAN ID to which the IP address is attached in the DHCP Snooping Database.
- **IP Address**—Indicates the IP address found during the query.
- **Interface**—Indicates the specific interface connected to the address found during the query.
- **Type**—Displays the IP address binding type. The possible field values are:
  - *Static*—Indicates the IP address is static.
  - *Dynamic*—Indicates the IP address is defined as a dynamic address in the DHCP database.
  - *Learned*—Indicates the IP address is dynamically defined by the DHCP server. (This field appears as a read-only field in the table).
- **Lease Time**—Displays the lease time. The Lease Time defines the amount of time the DHCP Snooping entry is active. Addresses whose lease times are expired are deleted from the database. The possible values are 10 – 4294967295 seconds. In the [Add Binding](#)

[Database Page](#), select **Infinite** if the DHCP Snooping entry never expires.

- To add an entry, click **Add**. The [Add Binding Database Page](#) is displayed.

**Figure 158: Add Binding Database Page**

The screenshot shows a configuration form for adding a binding to the database. The form is titled "Supported IP Format" and "Version 4". It contains the following fields and options:

- Type:** Radio buttons for "Dynamic" (selected) and "Static".
- MAC Address:** An empty text input field.
- Vlan ID:** A dropdown menu showing "1".
- IP Address:** An empty text input field.
- Interface:** Radio buttons for "Port" (selected) and "LAG". The "Port" dropdown shows "te0/1" and the "LAG" dropdown shows "LAG 1".
- Lease Time:** A text input field containing "10" and a checkbox for "(Sec) Infinite".
- Apply:** A button in the bottom right corner.

- Define the fields.
- Click **Apply**. The bound address is added to the database and the Running Configuration file is updated with the settings..
- Click **Delete** to delete the data from the *Query Results* table.
- To remove dynamic addresses from the *Query Results* table, click **Clear Dynamic**.

## DEFINING DYNAMIC ARP INSPECTION

*Dynamic Address Resolution Protocol (ARP)* is a TCP/IP protocol for translating IP addresses into MAC addresses. Classic ARP does the following:

- ◆ Permits two hosts on the same network to communicate and send packets.
- ◆ Permits two hosts on different networks to communicate via a gateway.
- ◆ Permits routers to send packets via a host to a different router on the same network.
- ◆ Permits routers to send packets to a destination host via a local host.

ARP Inspection intercepts, discards, and logs ARP packets that contain invalid IP-to-MAC address bindings. This eliminates man-in-the-middle attacks, where false ARP packets are inserted into the subnet. Packets are classified as:

- ◆ **Trusted**—Indicates that the interface IP and MAC address are recognized, and recorded in the ARP Inspection List. Trusted packets are forward without ARP Inspection.
- ◆ **Untrusted**—Indicates that the packet arrived from an interface that does not have a recognized IP and MAC addresses. The packet is checked for:
  - *Source MAC*—Compares the packet’s source MAC address in the Ethernet header against the sender’s MAC address in the ARP request. This check is performed on both ARP requests and responses.
  - *Destination MAC*—Compares the packet’s destination MAC address in the Ethernet header against the destination interface’s MAC address. This check is performed for ARP responses.
  - *IP Addresses*—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.

If the packet’s IP address was not found in the ARP Inspection List, and DHCP snooping is enabled for a VLAN, a search of the DHCP Snooping Database is performed. If the IP address is found, the packet is valid and is forwarded.



---

**NOTE:** ARP inspection is performed only on untrusted interfaces.

---

The ARP Inspection section contains the following topics:

- ◆ [Defining ARP Inspection Properties](#)
- ◆ [Defining ARP Inspection Trusted Interfaces](#)
- ◆ [Defining ARP Inspection List](#)
- ◆ [Assigning ARP Inspection VLAN Settings](#)

## DEFINING ARP INSPECTION PROPERTIES

The [ARP Inspection Properties Page](#) provides parameters for enabling and setting global Dynamic ARP Inspection parameters, as well as defining ARP Inspection Log parameters.

To define ARP Inspection properties:

1. Click **Security > ARP Inspection > Properties**. The [ARP Inspection Properties Page](#) is displayed.

**Figure 159: ARP Inspection Properties Page**

The screenshot shows a configuration window for ARP Inspection. It contains three main sections:

- Enable ARP Inspection:** A checkbox that is currently unchecked.
- ARP Inspection Validate:** A checkbox that is currently unchecked.
- Log Buffer Interval:** A section with two radio buttons:
  - Retry Frequency:** Selected with a radio button. It is followed by a text input field containing the number '5' and the label '(Sec)'.
  - Never:** Unselected with a radio button.

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

The [ARP Inspection Properties Page](#) contains the following fields:

- ◆ **Enable ARP Inspection**—Enables ARP Inspection on the device. The possible field values are:
    - *Checked*—Enables ARP Inspection on the device.
    - *Unchecked*—Disables ARP Inspection on the device. This is the default value.
  - ◆ **ARP Inspection Validate**—Enables ARP Inspection Validation on the device. The possible field values are:
    - *Checked*—Enables ARP Inspection Validation on the device. Source MAC, Destination MAC, and IP addresses are checked in ARP requests and responses.
    - *Unchecked*—Disable ARP Inspection Validation on the device. This is the default value.
  - ◆ **Log Buffer Interval**—Defines the minimal interval between successive Syslog messages. The possible field values are:
    - *Retry Frequency*—Frequency at which the log is updated. The possible range is 0-86400 seconds. 0 seconds specifies immediate transmissions of Syslog messages. The default value is 5 seconds.
    - *Never*—Log is never updated.
2. Define the relevant fields,
  3. Click **Apply**. The ARP Inspection Properties are defined, and the Running Configuration file is updated with the settings..

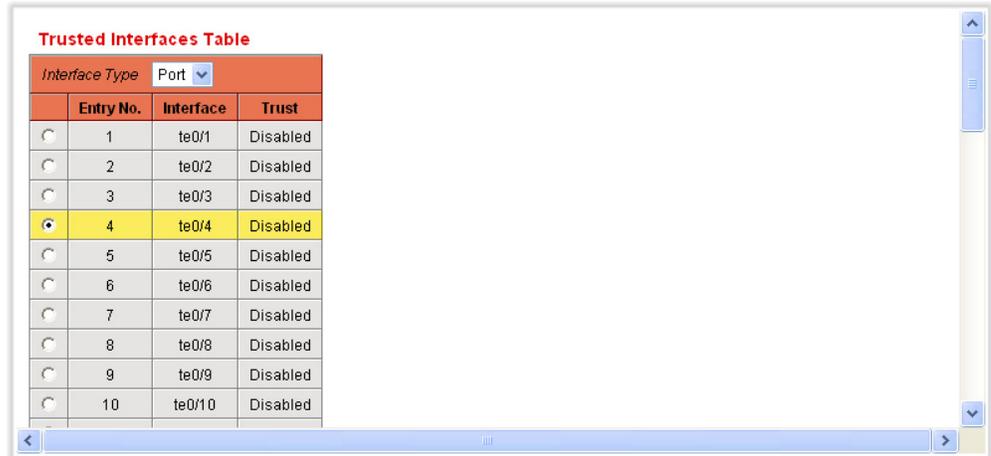
## DEFINING ARP INSPECTION TRUSTED INTERFACES

The [ARP Inspection Trusted Interfaces Page](#) allows network managers to define trusted and untrusted interfaces. These settings are independent of the trusted interface settings defined for DHCP snooping. ARP Inspection is enabled only on untrusted interfaces.

To define trusted interfaces:

1. Click **Security > ARP Inspection > Trusted Interfaces**. The [ARP Inspection Trusted Interfaces Page](#) is displayed.

**Figure 160: ARP Inspection Trusted Interfaces Page**



The screenshot shows a web interface titled "Trusted Interfaces Table". At the top, there is a dropdown menu for "Interface Type" set to "Port". Below this is a table with four columns: "Entry No.", "Interface", and "Trust". The table contains 10 rows, each representing an interface from te0/1 to te0/10. The "Trust" column for all entries is "Disabled". The row for te0/4 is highlighted in yellow, and a radio button next to the "Entry No." 4 is selected.

Interface Type	Port		
Entry No.	Interface	Trust	
<input type="radio"/>	1	te0/1	Disabled
<input type="radio"/>	2	te0/2	Disabled
<input type="radio"/>	3	te0/3	Disabled
<input checked="" type="radio"/>	4	te0/4	Disabled
<input type="radio"/>	5	te0/5	Disabled
<input type="radio"/>	6	te0/6	Disabled
<input type="radio"/>	7	te0/7	Disabled
<input type="radio"/>	8	te0/8	Disabled
<input type="radio"/>	9	te0/9	Disabled
<input type="radio"/>	10	te0/10	Disabled

This page displays information either for all ports or for all LAGs, depending on which interface type is selected.

2. Select an interface to be modified, and click **Edit**. The [Edit Trusted Interfaces Page](#) is displayed.

The [ARP Inspection Trusted Interfaces Page](#) contains the following fields:

**Figure 161: Edit Trusted Interfaces Page**



The screenshot shows a form with two main sections. The first section is labeled "Interface" and contains two radio buttons: "Port" (selected) and "LAG". The "Port" radio button is followed by a dropdown menu showing "te0/4". The "LAG" radio button is followed by a dropdown menu showing "LAG 1". The second section is labeled "Trust Status" and contains a dropdown menu showing "Disable". An "Apply" button is located at the bottom right of the form.

3. Enter the parameters.
  - **Interface**—Select the interface name.
  - **Trust Status**—Select whether the interface is a Trusted Interface. The possible field values are:
    - *Enabled*—Indicates the port or LAG is a trusted interface, and ARP inspection is not performed on the ARP requests/replies sent to/from the interface.

- *Disabled*—Indicates the port or LAG is not a trusted interface, and ARP inspection is performed on the ARP requests/replies sent to/from the interface. This is the default value.
4. Click **Apply**. The Trusted Interface's configuration is modified, and the Running Configuration file is updated with the settings..

## DEFINING ARP INSPECTION LIST

The [ARP Inspection List Page](#) provides information for creating static ARP Binding Lists. ARP Binding Lists contain the List Name, IP address and MAC address which are validated against ARP requests and replies.

To add an ARP Inspection List entry:

1. Click **Security > ARP Inspection > ARP Inspection List**. The [ARP Inspection List Page](#) is displayed.

**Figure 162: ARP Inspection List Page**

The screenshot shows a web interface titled "Static ARP Table". It features a table with a header "ARP Inspection Name" and a sub-header "Table is empty". Below the table are two buttons: "Add..." and "Delete". At the bottom of the interface is a button labeled "List Details".

2. Click **Add**. The [Add ARP List Page](#) is displayed.

**Figure 163: Add ARP List Page**

The screenshot shows a form titled "Add ARP List Page". It contains three input fields: "List Name", "IP Address", and "MAC Address", each with a red asterisk indicating a required field. To the right of the "MAC Address" field is an "Apply" button.

3. Enter the parameters.
  - **ARP Inspection List Name**—Name of the ARP Inspection List. The list's name can contain up to 32 characters.
  - **IP Address**—Specifies IP address included in ARP Binding Lists which is checked against ARP requests and replies.
  - **MAC Address**—Specifies MAC address included in ARP Binding Lists which is checked against ARP requests and replies.

4. Click **Apply**. The new ARP Inspection List is added, and the Running Configuration file is updated with the settings..
5. To view the *ARP Inspection List* details, click **List Details**.

### ASSIGNING ARP INSPECTION VLAN SETTINGS

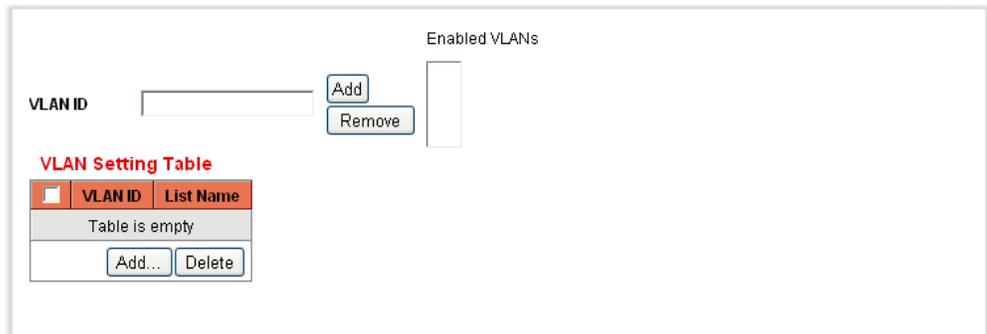
The [ARP Inspection VLAN Settings Page](#) contains fields for enabling ARP Inspection on VLANs. In the Enabled VLAN table, users assign static ARP Inspection Lists to enabled VLANs. When a packet passes through an untrusted interface which is enabled for ARP Inspection, the device performs the following checks in order:

- ◆ Determines if the packet’s IP address and MAC address exist in the static ARP Inspection list. If the addresses match, the packet passes through the interface.
- ◆ If the device does not find a matching IP address, but DHCP Snooping is enabled on the VLAN, the device checks the DHCP Snooping database for the IP address-VLAN match. If the entry exists in the DHCP Snooping database, the packet passes through the interface.
- ◆ If the packet’s IP address is not listed in the ARP Inspection List or the DHCP Snooping database, the device rejects the packet.

To define ARP Inspection on VLANs:

1. Click **Security > ARP Inspection > VLAN Settings**. The [ARP Inspection VLAN Settings Page](#) is displayed.

**Figure 164: ARP Inspection VLAN Settings Page**



The [ARP Inspection VLAN Settings Page](#) contains the following fields:

- ◆ **VLAN ID**—A user-defined VLAN ID to add to the Enabled VLANs list.
  - ◆ **Enabled VLANs**—Contains a list of VLANs in which ARP Inspection is enabled.
2. Select the VLAN name from the VLAN ID list and click **Add**. This VLAN name then appears in the list.

3. Click **Add**. The [Add VLAN Settings Page](#) is displayed.

**Figure 165: Add VLAN Settings Page**



The screenshot shows a configuration page with two dropdown menus. The first is labeled 'Bind List Name' and the second is labeled 'To VLAN'. Both dropdown menus have a downward-pointing arrow. To the right of these fields is a button labeled 'Apply'.

The [Add VLAN Settings Page](#) contains the following fields:

- ◆ **Bind List Name**—Select a static ARP Inspection List to assign to the VLAN. These lists are defined in the [ARP Inspection VLAN Settings Page](#).
  - ◆ **To VLAN**—Select the VLAN which includes the specified *ARP Inspection List*.
4. Define the fields.
  5. Click **Apply**. The VLAN Settings are modified, and the Running Configuration file is updated with the settings.



The Access Control List (ACL) feature is part of the security mechanism. ACL definitions serve as one of the mechanisms to define traffic flows that should be given a specific Quality of Service (QoS). For more information see the [Configuring QoS](#) section in the [Configuring Quality of Service](#) chapter.

ACLs enable network managers to define patterns (filter and actions) for ingress traffic. Packets, entering the switch on a port or LAG with an active ACL, are either admitted or denied entry.

This chapter contains the following topics:

- ◆ [Access Control Lists Overview](#)
- ◆ [Defining MAC-based ACLs](#)
- ◆ [Defining IPv4-based ACLs](#)
- ◆ [Defining IPv6-based ACLs](#)
- ◆ [Defining ACL Binding](#)

---

## ACCESS CONTROL LISTS OVERVIEW

An Access Control List (ACL) is an ordered list of classification filters and actions. Each single classification rule, together with its action, is called an Access Control Element (ACE).

Each ACE is made up of filters that determine traffic groups and associated actions. A single ACL may contain one or more ACEs, which are matched against the contents of incoming frames. Either a DENY or PERMIT action is applied to frames whose contents match the filter.

The switch support a maximum of 512 ACLs, and a maximum of 512 ACEs.

When a packet matches an ACE filter, the ACE action is taken and that ACL processing is stopped. If the packet does not match the ACE filter, the next ACE is processed. If all ACEs of an ACL have been processed without finding a match, and if another ACL exists, it is processed in a similar manner. If no match is found to any ACE in all relevant ACLs, the packet is dropped (as a default action). Because of this default drop action you must explicitly add ACEs into the ACL to permit all traffic, including management traffic, such as telnet, HTTP or SNMP that is directed to the switch itself.

If IGMP/MLD snooping is enabled at a port bound with an ACL, add ACE filters in the ACL to forward IGMP/MLD packets to the switch. Otherwise, IGMP/MLD snooping will fail at the port.

The order of the ACEs within the ACL is significant, since they are applied in a first-fit manner. The ACEs are processed sequentially, starting with the first ACE.

ACLs can be used for security, for example by permitting or denying certain traffic flows, and also for traffic classification and prioritization in the QoS Advanced mode.

A port can be either secured with ACLs or configured with advanced QoS policy, but not both.

There can only be one ACL per port, with the exception that it is possible to associate both an IP-based ACL and an IPv6-based ACL with a single port. To associate more than one ACL with a port, a policy with one or more class maps must be used (see *Configuring a Policy*). The following types of ACLs can be defined (depending on which part of the frame header is examined):

- ◆ MAC ACL—Examines Layer 2 fields only, as described in [Defining MAC-based ACLs](#)
- ◆ IP ACL—Examines the L3 layer of IP frames, as described in [Defining IPv4-based ACLs](#)
- ◆ IPv6 ACL—Examines the L3 layer of IPv6 frames as described in [Defining IPv6-Based ACL](#)

If a frame matches the filter in an ACL, it is defined as a flow with the name of that ACL. In advanced QoS, these frames can be referred to using this Flow name, and QoS can be applied to these frames (see [QoS Advanced Mode](#)).

## CREATING ACLS WORKFLOW

To create ACLs and associate them with an interface, perform the following:

1. Create one or more of the following types of ACLs:
  - a. MAC-based ACL by using the [MAC-Based ACL Page](#) and the [MAC-Based ACE Page](#)
  - b. IP-based ACL by using the [IPv4-Based ACL Page](#) and the [IPv4-Based ACE Page](#)
  - c. IPv6-based ACL by using the [IPv6-Based ACL Page](#) and the [IPv6-Based ACE Page](#)
2. Associate the ACL with interfaces by using the [ACL Binding Page](#).

## MODIFYING ACLS WORKFLOW

An ACL can only be modified if it is not in use. The following describes the process of unbinding an ACL in order to modify it:

- ◆ If the ACL does not belong to a QoS Advanced Mode class map, but it has been associated with an interface, unbind it from the interface using the [ACL Binding Page](#).
- ◆ If the ACL is part of the class map and not bound to an interface, then it can be modified.
- ◆ If the ACL is part of a class map contained in a policy bound to an interface, you must perform the chain of unbinding as follows:
  - Unbind the policy containing the class map from the interface by using [Policy Binding](#).
  - Delete the class map containing the ACL from the policy using the [Configuring a Policy \(Edit\)](#).
  - Delete the class map containing the ACL, by using [Defining Class Mapping](#).

Only then can the ACL be modified, as described in the sections of this chapter.

---

## DEFINING MAC-BASED ACLS

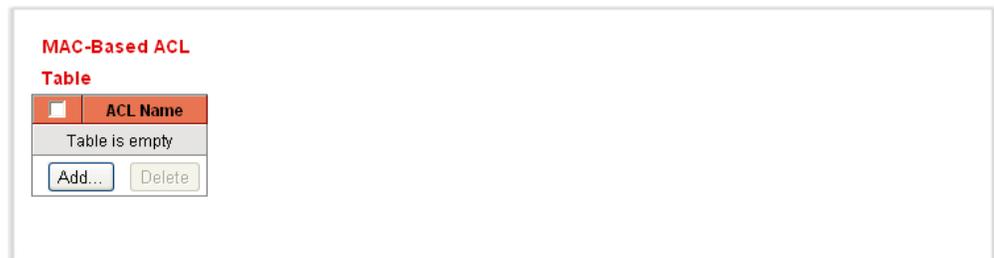
MAC-based ACLs are used to filter traffic based on Layer 2 fields. MAC-based ACLs check all frames for a match.

MAC-based ACLs are defined in the [MAC-Based ACL Page](#). The rules are defined in the [MAC-Based ACE Page](#).

To define a MAC-based ACL:

1. Click **Access Control** > **MAC-Based ACL**. The [MAC-Based ACL Page](#) is displayed.

**Figure 166: MAC-Based ACL Page**



This page displays a list of all currently defined MAC-based ACLs.

2. Click **Add**. The [Add MAC-Based ACL Page](#) is displayed.

**Figure 167: Add MAC-Based ACL Page**



The screenshot shows a form titled "Add MAC-Based ACL Page". It features a text input field labeled "ACL Name" with the value "Test1" entered. To the right of the input field is a button labeled "Apply".

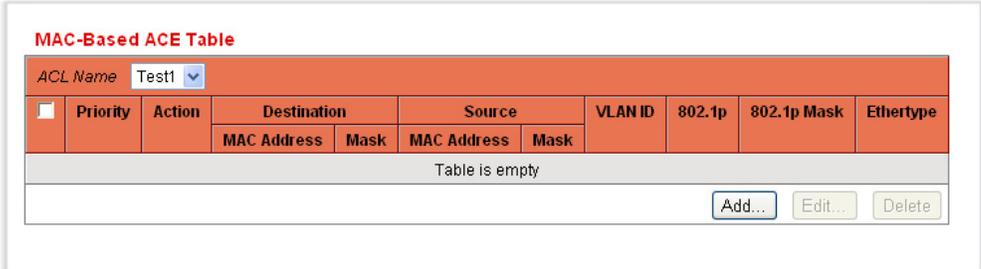
3. Enter the name of the new ACL in the **ACL Name** field. ACL names are case-sensitive.
4. Click **Apply**. The MAC-based ACL is added, and the Running Configuration file is updated with the settings.

### ADDING RULES TO A MAC-BASED ACL

To add rules (ACEs) to an ACL:

1. Click **Access Control > MAC-Based ACE**. The [MAC-Based ACE Page](#) is displayed.

**Figure 168: MAC-Based ACE Page**



The screenshot shows the "MAC-Based ACE Table" interface. At the top, there is a dropdown menu for "ACL Name" set to "Test1". Below this is a table with the following columns: Priority, Action, Destination (subdivided into MAC Address and Mask), Source (subdivided into MAC Address and Mask), VLAN ID, 802.1p, 802.1p Mask, and Ethertype. The table is currently empty, with the text "Table is empty" displayed in the center. At the bottom right of the table, there are three buttons: "Add...", "Edit...", and "Delete".

2. Select an ACL. The ACEs in the ACL are listed.
3. Click **Add**. The [Add MAC-Based ACE Page](#) is displayed.

Figure 169: Add MAC-Based ACE Page

ACL Name	Test1
Priority *	<input type="text"/> (Range: 1 - 2147483647)
Action	<input type="button" value="Permit"/> ▾
Destination MAC Address	<input checked="" type="radio"/> Any <input type="radio"/> User defined
Destination MAC Address Value *	<input type="text"/>
Destination MAC Wildcard Mask *	<input type="text"/>
Source MAC Address	<input checked="" type="radio"/> Any <input type="radio"/> User defined
Source MAC Address Value *	<input type="text"/>
Source MAC Wildcard Mask *	<input type="text"/>
VLAN ID	<input type="text"/> (1 - 4094)
802.1p	<input type="checkbox"/> Include
802.1p Value *	<input type="text"/> (0 - 7)
802.1p Mask *	<input type="text"/> (0 - 7)
Ethertype	<input type="text"/> (1501 - 65535)

4. Enter the parameters.

- **ACL Name**—Displays the name of the ACL to which an ACE is being added.
- **Priority**—Enter the priority of the ACE. ACEs with higher priority are processed first. One is the highest priority.
- **Action**—Select the action taken upon a match. The options are:
  - *Permit*—Forward packets that meet the ACE criteria.
  - *Deny*—Drop packets that meet the ACE criteria.
  - *Shutdown*—Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the *Port Settings Page*.
- **Destination MAC Address**—Select *Any* if all destination addresses are acceptable or *User defined* to enter a destination address or a range of destination addresses.
- **Destination MAC Address Value**—Enter the MAC address to which the destination MAC address will be matched and its mask (if relevant).
- **Destination MAC Wildcard Mask**—Enter the mask to define a range of MAC addresses. Note that this mask is different than in other uses, such as subnet mask. Here, setting a bit as **1** indicates don't care and **0** indicates to mask that value. For example, the value: "FFFFFF000000" indicates that only the first three bytes of the destination MAC address are used.

- **Source MAC Address**—Select *Any* if all source address are acceptable or *User defined* to enter a source address or range of source addresses.
  - **Source MAC Address Value**—Enter the MAC address to which the source MAC address will be matched and its mask (if relevant).
  - **Source MAC Wildcard Mask**—Enter the mask to define a range of MAC addresses.
  - **VLAN ID**—Enter the VLAN ID section of the VLAN tag to match.
  - **802.1p**—Select **Include** to use 802.1p.
  - **802.1p Value**—Enter the 802.1p value to be added to the VPT tag.
  - **802.1p Mask**—Enter the wildcard mask to be applied to the VPT tag.
  - **Ethertype**—Enter the frame Ether type to be matched.
5. Click **Apply**. The Add MAC Based ACE is defined, and the Running Configuration file is updated with the settings.

---

## DEFINING IPv4-BASED ACLS

IPv4-based ACLs are used to check IPv4 packets, while other types of frames, such as ARPs, are not checked.

The following fields can be matched:

- ◆ IP protocol (by name for well-known protocols, or directly by value)
- ◆ Source/destination ports for TCP/UDP traffic
- ◆ Flag values for TCP frames
- ◆ ICMP and IGMP type and code
- ◆ Source/destination IP addresses (including wildcards)
- ◆ DSCP/IP-precedence value

ACLs are also used as the building elements of flow definitions for per-flow QoS handling (see [QoS Advanced Mode](#)).

The [IPv4-Based ACL Page](#) enables adding ACLs to the system. The rules are defined in the [IPv4-Based ACE Page](#).

IPv6 ACLs are defined in the [IPv6-Based ACL Page](#).

**DEFINING AN IPv4-BASED ACL** To define an IPv4-based ACL:

1. Click **Access Control > IPv4 Based ACL**. The *IPv4-Based ACL Page* is displayed.

**Figure 170: IPv4-Based ACL Page**



This page displays all currently defined IPv4-based ACLs.

2. Click **Add**. The [Add IPv4-Based ACL Page](#) is displayed.

**Figure 171: Add IPv4-Based ACL Page**



3. Enter the name of the new ACL in the **ACL Name** field. The names are case-sensitive.
4. Click **Apply**. The IPv4-based ACL is defined, and the Running Configuration file is updated with the settings.

**ADDING RULES (ACEs) TO AN IPv4-BASED ACL** To add rules (ACEs) to an IPv4-based ACL:

1. Click **Access Control > IPv4 Based ACE**. The *IPv4-Based ACE Page* is displayed.

**Figure 172: IPv4-Based ACE Page**



2. Select an ACL, and click **Go**. All currently-defined IP ACEs for the selected ACL are displayed.
3. Click **Add**. The [Add IPv4-Based ACE Page](#) is displayed.

Figure 173: Add IPv4-Based ACE Page

The screenshot shows the 'Add IPv4-Based ACE Page' configuration form. The form is divided into several sections:

- ACL Name:** Test-ipv4
- Priority:** (Range: 1 - 2147483647)
- Action:** Permit
- Protocol:** Any (IP)
- Source IP Address:** Any
- Source IP Address Value:**
- Source IP Wildcard Mask:**
- Destination IP Address:** Any
- Destination IP Address Value:**
- Destination IP Wildcard Mask:**
- Source Port:** Any
- Destination Port:** Any
- TCP Flags:** Urg, Ack, Psh, Rst, Syn, Fin (all set to 'Don't care')
- Type of Service:** Any
- ICMP:** Any
- ICMP Code:** Any
- IGMP:** Any

An 'Apply' button is located in the bottom right corner of the form.

4. Enter the parameters.
  - **ACL Name**—Displays the name of the ACL.
  - **Priority**—Enter the priority. ACEs with higher priority are processed first.
  - **Action**—Select the action assigned to the packet matching the ACE. The options are as follows:
    - *Permit*—Forward packets that meet the ACE criteria.
    - *Deny*—Drop packets that meet the ACE criteria.
    - *Shutdown*—Drop packet that meets the ACE criteria and disable the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.
  - **Protocol**—Select to create an ACE based on a specific protocol or protocol ID. Select *Any (IPv4)* to accept all IP protocols. Otherwise select one of the following protocols from the drop-down list:
    - *ICMP*—*Internet Control Message Protocol*
    - *IGMP*—*Internet Group Management Protocol*

- *IP in IP*—IP in IP encapsulation
- *TCP*—Transmission Control Protocol
- *EGP*—Exterior Gateway Protocol
- *IGP*—Interior Gateway Protocol
- *UDP*—User Datagram Protocol
- *HMP*—Host Mapping Protocol
- *RDP*—Reliable Datagram Protocol.
- *IDPR*—Inter-Domain Policy Routing Protocol
- *IPV6*—IPv6 over IPv4 tunneling
- *IPV6:ROUT*—Matches packets belonging to the *IPv6 over IPv4 route through a gateway*
- *IPV6:FRAG*—Matches packets belonging to the *IPv6 over IPv4 Fragment Header*
- *IDRP*—Inter-Domain Routing Protocol
- *RSVP*—ReSerVation Protocol
- *AH*—Authentication Header
- *IPV6:ICMP*—Internet Control Message Protocol
- *EIGRP*—Enhanced Interior Gateway Routing Protocol
- *OSPF*—Open Shortest Path First
- *IPIP*—IP in IP
- *PIM*—Protocol Independent Multicast
- *L2TP*—Layer 2 Tunneling Protocol
- *ISIS*—IGP-specific protocol
- **Protocol ID to match**—Instead of selecting the name, enter the protocol ID.
- **Source IP Address**—Select *Any* if all source address are acceptable or *User defined* to enter a source address or range of source addresses.
- **Source IP Address Value**—Enter the IP address to which the source IP address will be matched.

- **Source IP Wildcard Mask**—Enter the mask to define a range of IP addresses.
- **Destination IP Address**—Select *Any* if all destination address are acceptable or *User defined* to enter a destination address or range of destination addresses.
- **Destination IP Address Value**—Enter the IP address to which the destination MAC address will be matched.
- **Destination IP Wildcard Mask**—Enter the mask to define a range of IP addresses.
- **Source Port**—Select one of the following:
  - *Any*—Match to all source ports.
  - *Single*—Enter a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the Select from List drop-down menu.
  - *Range*—Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- **Destination Port**—Select one of the available values that are the same as for the Source Port field described above.



---

**NOTE:** You must specify the IP protocol for the ACE before you can enter the source and/or destination port.

---

- **TCP Flags**—Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security.
- **Type of Service**—The service type of the IP packet.
  - **Any**—Any service type
  - **DSCP to match**—Differentiated Services Code Point (DSCP) to match
  - **IP Precedence to match**—Check to enable matching IP-precedence with the packet IP-precedence value. IP precedence enables marking frames that exceed the CIR threshold. In a congested network, frames containing a higher DP value are discarded before frames with a lower DP value. If this field is checked, enter a value to be matched.

- **ICMP**—If the IP protocol of the ACL is ICMP, select the ICMP message type used for filtering purposes. Either select the message type by name or enter the message type number:
    - *Any*—All message types are accepted.
    - *Select from list*—Select message type by name.
    - *ICMP Type to Match*—Number of message type to be used for filtering purposes.
  - **ICMP Code**—The ICMP messages can have a code field that indicates how to handle the message. Select one of the following options to configure whether to filter on this code:
    - *Any*—Accept all codes.
    - *User defined*—Enter an ICMP code for filtering purposes.
  - **IGMP**—If the ACL is based on IGMP, select the IGMP message type to be used for filtering purposes. Either select the message type by name or enter the message type number:
    - *Any*—All message types are accepted.
    - *Select from list*—Select message type by name.
    - *IGMP Type to match*—Number of message type that will be used for filtering purposes.
5. Click **Apply**. The IPv4-based ACE is defined, and the Running Configuration file is updated with the settings.

---

## DEFINING IPV6-BASED ACLS

The [IPv6-Based ACL Page](#) displays and enables the creation of IPv6 ACLs, which check pure IPv6-based traffic. IPv6 ACLs do not check IPv6-over-IPv4 or ARP packets.

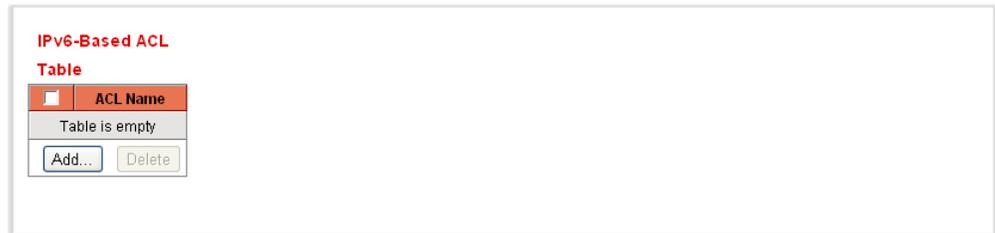
ACLs are also used as the building elements of flow definitions for per-flow QoS handling (see [QoS Advanced Mode](#)).

### DEFINING AN IPV6-BASED ACL

To define an IPv6-based ACL:

1. Click **Access Control > IPv6 Based ACL**. The [IPv6-Based ACL Page](#) is displayed.

**Figure 174: IPv6-Based ACL Page**



This window displays the list of defined ACLs and their contents

2. Click **Add**. The *Add IPv6-based ACL Page* is displayed.

**Figure 175: Add IPv6-based ACL Page**



3. Enter the name of a new ACL in the **ACL Name** field. The names are case-sensitive.
4. Click **Apply**. The IPv6-based ACL is defined, and the Running Configuration file is updated with the settings.

**DEFINING A RULE (ACE) FOR AN IPv6-BASED ACL**

1. Click **Access Control > IPv6 Based ACE**. The *IPv6-Based ACE Page* is displayed.

**Figure 176: IPv6-Based ACE Page**



This window displays the ACE (rules) for a specified ACL (group of rules).

2. Select an ACL, and click **Go**. All currently-defined IP ACEs for the selected ACL are displayed.
3. Click **Add**. The *Add IPv6-Based ACE Page* is displayed.

Figure 177: Add IPv6-Based ACE Page

The screenshot shows a configuration page for adding an IPv6-based ACE. The form is organized into several sections:

- ACL Name:** Test-ipv6
- Priority:** (1 - 2147483647)
- Action:** Permit
- Protocol:** Any (IPv6)
- Source IP Address:** Any
- Source IP Address Value:** [Text Field]
- Source IP Prefix Length:** (0 - 128)
- Destination IP Address:** Any
- Destination IP Address Value:** [Text Field]
- Destination IP Prefix Length:** (0 - 128)
- Source Port:** Any
- Destination Port:** Any
- TCP Flags:** Urg, Ack, Psh, Rst, Syn, Fin (each with a 'Set' dropdown)
- Type of Service:** Any
- ICMP:** Any

An 'Apply' button is located at the bottom right of the form.

4. Enter the parameters.

- **ACL Name**—Displays the name of the ACL to which an ACE is being added.
- **Priority**—Enter the priority. ACEs with higher priority are processed first.
- **Action**—Select the action assigned to the packet matching the ACE. The options are as follows:
  - *Permit*—Forward packets that meet the ACE criteria.
  - *Deny*—Drop packets that meet the ACE criteria.
  - *Shutdown*—Drop packets that meet the ACE criteria, and disable the port to which the packets were addressed. Ports are reactivated from the *Port Management* page.
- **Protocol**—Select to create an ACE based on a specific protocol. Select *Any (IPv6)* to accept all IP protocols. Otherwise select one of the following protocols:
  - *TCP*—*Transmission Control Protocol*. Enables two hosts to communicate and exchange data streams. TCP guarantees

packet delivery, and guarantees that packets are transmitted and received in the order they were sent.

- *UDP—User Datagram Protocol*. Transmits packets but does not guarantee their delivery.
- *ICMP—Matches packets to the Internet Control Message Protocol (ICMP)*.
- **Protocol ID to match**—Enter the ID of the protocol to be matched.
- **Source IP Address**—Select *Any* if all source address are acceptable or *User defined* to enter a source address or range of source addresses.
- **Source IP Address Value**—Enter the IP address to which the source IP address will be matched and its mask (if relevant).
- **Source IP Prefix Length**—Enter the prefix length of the source IP address.
- **Destination IP Address**—Select *Any* if all destination address are acceptable or *User defined* to enter a destination address or a range of destination addresses.
- **Destination IP Address Value**—Enter the IP address to which the destination MAC address will be matched and its mask (if relevant).
- **Destination IP Prefix Length**—Enter the prefix length of the IP address.
- **Source Port**—Select one of the following:
  - *Any*—Match to all source ports.
  - *Single*—Enter a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the IP Protocol drop-down menu.
  - *Range*—Select a range of TCP/UDP source ports to which the packet is matched.
- **Destination Port**—Select one of the available values. (They are the same as for the Source Port field described above).



**NOTE:** You must specify the IPv6 protocol for the ACL before you can configure the source and/or destination port.

---

- **TCP Flags**—Select one of more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security.

- Set—Match if the flag is SET.
  - Unset—Match if the flag is Not SET.
  - Don't care—Ignore the TCP flag.
  - **Type of Service**—The service type of the IP packet.
    - **Any**—Any service type
    - **DSCP to match**—Differentiated Services Code Point (DSCP) to match
    - **IP Precedence to match**—Specifies the IP precedence value.
  - **ICMP**—If the ACL is based on ICMP, select the ICMP message type that will be used for filtering purposes. Either select the message type by name or enter the message type number. If all message types are accepted, select *Any*.
    - *Any*—All message types are accepted.
    - *Select from list*—Select message type by name from the drop-down list.
    - *ICMP Type to Match*—Number of message type that will be used for filtering purposes.
  - **ICMP Code**—The ICMP messages may have a code field that indicates how to handle the message. Select one of the following options, to configure whether to filter on this code:
    - *Any*—Accept all codes.
    - *User defined*—Enter an ICMP code for filtering purposes.
5. Click **Apply**.

---

## DEFINING ACL BINDING

When an ACL is bound to an interface, its ACE rules are applied to packets arriving at that interface. Packets that do not match any of the ACEs in the ACL are matched to a default rule, whose action is to drop unmatched packets.

Although each interface can be bound to only one ACL, multiple interfaces can be bound to the same ACL by grouping them into a policy-map, and binding that policy-map to the interface.

After an ACL is bound to an interface, it cannot be edited, modified, or deleted until it is removed from all the ports to which it is bound or in use.

To bind an ACL to an interface:

1. Click **Access Control > ACL Binding**. The [ACL Binding Page](#) is displayed.

**Figure 178: ACL Binding Page**

ACL Binding Table					
Interface Type		Port			
<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	1	te0/1			
<input type="checkbox"/>	2	te0/2			
<input type="checkbox"/>	3	te0/3			
<input checked="" type="checkbox"/>	4	te0/4			
<input type="checkbox"/>	5	te0/5			
<input type="checkbox"/>	6	te0/6			
<input type="checkbox"/>	7	te0/7			
<input type="checkbox"/>	8	te0/8			
<input type="checkbox"/>	9	te0/9			

2. Select an interface type **Ports/LAGs** (Port or LAG). The list of ports/LAGs is displayed. For each type of interface selected, all interfaces of that type are displayed with a list of their current ACLs:
  - **Interface**—Identifier of interface.
  - **MAC ACL**—ACLs of type MAC that are bound to the interface (if any).
  - **IPv4 ACL**—ACLs of type IPv4 that are bound to the interface (if any).
  - **IPv6 ACL**—ACLs of type IPv6 that are bound to the interface (if any).



**NOTE:** To unbind all ACLs from an interface, select the interface, and click **Clear**.

3. Select an interface, and click **Edit**. The [Edit ACL Binding Page](#) is displayed.

**Figure 179: Edit ACL Binding Page**

Interface Port **te0/4** LAG **1**

Select MAC-Based ACL Test1

Select IPv4-Based ACL Test-ipv4

Select IPv6-Based ACL Test-ipv6

4. Select the **Interface** to which the ACLs are to be bound.
5. Select one of the following:
  - **Select MAC-Based ACL**—Select a MAC-based ACL to be bound to the interface.
  - **Select IPv4-Based ACL**—Select an IPv4-based ACL to be bound to the interface.
  - **Select IPv6-Based ACL**—Select an IPv6-based ACL to be bound to the interface.
6. Click **Apply**. The ACL binding is modified, and the Running Configuration file is updated with the settings.



**NOTE:** If no ACL is selected, the ACL(s) that is previously bound to the interface is unbound.

---



The Quality of Service feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and the desired traffic receives preferential treatment.

This chapter contains the following topics:

- ◆ [QoS Features and Components](#)
- ◆ [Configuring QoS](#)
- ◆ [QoS Basic Mode](#)
- ◆ [QoS Advanced Mode](#)

---

## QoS FEATURES AND COMPONENTS

The QoS feature is used to optimize network performance.

QoS provides the following:

- ◆ Classification of incoming traffic to traffic classes, based on attributes, including:
  - *Device Configuration*
  - *Ingress interface*
  - *Packet content*
  - *Combination of these attributes*

QoS includes the following:

- ◆ **Traffic Classification**—Classifies each incoming packet as belonging to a specific traffic flow, based on the packet contents and/or the port. The classification is done by ACL (Access Control List), and only traffic that meets the ACL criteria is subject to CoS or QoS classification.
- ◆ **Assignment to Hardware Queues**—Assigns incoming packets to forwarding queues. Packets are sent to a particular queue for handling as a function of the traffic class to which they belong.

- ◆ **Other Traffic Class-Handling Attribute**—Applies QoS mechanisms to various classes, including *bandwidth management*.

The QoS mode that is selected applies to all interfaces in the system.

- ◆ **Basic Mode**—Class of Service (CoS).

All traffic of the same class receives the same treatment, which is the single QoS action of determining the egress queue on the egress port, based on the indicated QoS value in the incoming frame. This is the VLAN Priority Tag (VPT) 802.1p value in Layer 2 and the Differentiated Service Code Point (DSCP) value for IPv4 or Traffic Class (TC) value for IPv6 in Layer 3. When operating in Basic Mode, the switch trusts this external assigned QoS value. The external assigned QoS value of a packet determines its traffic class and QoS.

The header field to be trusted is entered in the *Global Settings Page*. For every value of that field, an egress queue is assigned where the frame is sent in the *CoS/802.1p to Queue Page* or the *DSCP to Queue Page* (depending on whether the trust mode is CoS/802.1p or DSCP, respectively).

- ◆ **Advanced Mode**—Per-flow Quality of Service (QoS).

In advanced mode, a per flow QoS consists of a class map and a policer:

- A class map defines the kind of traffic in a flow, and contains one or more ACLs. Packets that match the ACLs belong to the flow.
- A policer applies the configured QoS to a flow. The QoS configuration of a flow may consist of egress queue, the DSCP or CoS/802.1p value, and actions on out of profile (excess) traffic.

- ◆ **Disable Mode**

In this mode all traffic is mapped to a single best effort queue, so that no type of traffic is prioritized over another.

Only a single mode can be active at a time. When the system is configured to work in QoS Advanced mode, settings for QoS Basic mode are not active and vice versa.

When the mode is changed, the following occurs:

- ◆ When changing from QoS Advanced mode to any other mode, policy profile definitions and class maps are deleted. ACLs bonded directly to interfaces remain bonded.
- ◆ When changing from QoS Basic mode to Advanced mode, the QoS Trust mode configuration in Basic mode is not retained.
- ◆ When disabling QoS, the shaper and queue setting (WRR/SP bandwidth setting) are reset to default values.

All other user configurations remain intact.

### QoS WORKFLOW

To configure general QoS parameters, perform the following:

1. Choose the QoS mode (Basic, Advanced, or Disabled, as described in [QoS Basic Mode](#) and [QoS Advanced Mode](#)) for the system by using the [QoS Properties Page](#). The following steps in the workflow, assume that you have chosen to enable QoS.
2. Assign each interface a default CoS/802.1p priority by using the [QoS Properties Page](#).
3. Assign the schedule method (Strict Priority or WRR) and bandwidth allocation for WRR to the egress queues by using the [Queue Page](#).
4. Designate an egress queue to each IP DSCP/TC value with the [DSCP to Queue Page](#). If the switch is in DSCP trusted mode, incoming packets are put into the egress queues based on the their DSCP/TC value.
5. Designate an egress queue to each CoS/802.1p priority. If the switch is in CoS/802.1 trusted mode, all incoming packets will be put into the designated egress queues according to the CoS/802.1p priority in the packets. This is done by using the [CoS/802.1p to Queue Page](#).
6. If required for Layer 3 traffic only, assign a queue to each DSCP/TC value, by using the [DSCP to Queue Page](#).
7. Set ingress rate limit and egress shaping rate per port by using the [Bandwidth Page](#).
8. Configure the selected mode by performing one of the following:
  - a. Configure Basic mode, as described in [QoS Basic Mode](#)
  - b. Configure Advanced mode, as described in [QoS Advanced Mode](#).

---

## CONFIGURING QoS

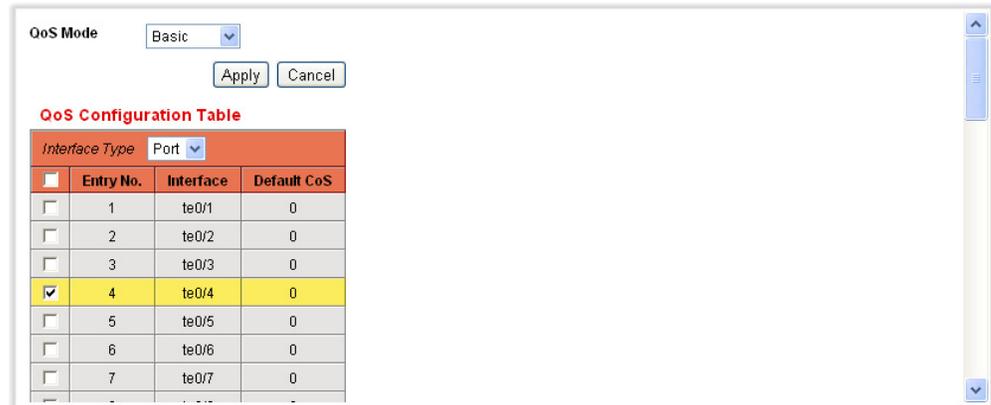
### DISPLAYING QoS PROPERTIES

The *QoS Properties Page* contains fields for setting the QoS mode for the system (Basic, Advanced, or Disabled, as described in [QoS Basic Mode](#) and [QoS Advanced Mode](#)). In addition, the default CoS priority for each interface can be defined.

To select the QoS mode:

1. Click **Quality of Service > General > QoS Properties**. The [QoS Properties Page](#) is displayed.

**Figure 180: QoS Properties Page**



2. Select the **QoS Mode** (Disable, Basic, or Advanced) that will be active on the switch and click **Apply**.
3. Select **Port/LAG** to display/modify all ports/LAGs and their CoS information.

The following fields are displayed for all ports/LAGs:

- **Interface**—Type of interface.
  - **Default CoS**—Default VPT value for incoming packets that do not have a VLAN Tag. The default CoS is 0. The default is only relevant for untagged frames and only if the system is in Basic mode and *Trust CoS* is selected in the *Global Settings Page*.
4. Select **Restore CoS Defaults** to restore the factory CoS default setting for this interface.

### MODIFYING INTERFACE DEFAULT CoS VALUE

1. Click **Quality of Service > General > QoS Properties**. The [QoS Properties Page](#) is displayed.
2. Select an interface, and click **Edit**. The [Edit Interface CoS Configuration Page](#) is displayed.

**Figure 181: Edit Interface CoS Configuration Page**



3. Enter the parameters.
  - **Interface**—Select the interface.

- **Default CoS**—Select the default CoS (Class-of-Service) value to be assigned for incoming packets (that do not have a VLAN tag). The range is 0-7.
4. Click **Apply**. The interface default CoS value is set, and the Running Configuration file is updated with the settings.

## CONFIGURING QoS QUEUES

The switch supports four queues for each interface. Queue number four is the highest priority queue. Queue number one is the lowest priority queue.

There are two ways of determining how traffic in queues is handled, Strict Priority and Weighted Round Robin (WRR).

**Strict Priority**—Egress traffic from the highest-priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, thus providing the highest level of priority of traffic to the highest numbered queue.

**Weighted Round Robin (WRR)**—In WRR mode, the number of packets sent from the queue is distributed evenly among the queues. If all eight queues are WRR, each queue receives the following percentage of the traffic by default:

- ◆ 1 - 12%
- ◆ 2 - 12%
- ◆ 3 - 12%
- ◆ 4 - 12%
- ◆ 5 - 13%
- ◆ 6 - 13%
- ◆ 7 - 13%
- ◆ 8 - 13%

The WRR weights can be changed as long as the total adds up to 100%.

The queuing modes can be selected in the *Queue Page*. When the queuing mode is by strict priority, the priority sets the order in which queues are serviced, starting with queue\_8 (the highest priority queue) and going to the next lower queue when each queue is completed.

When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced.

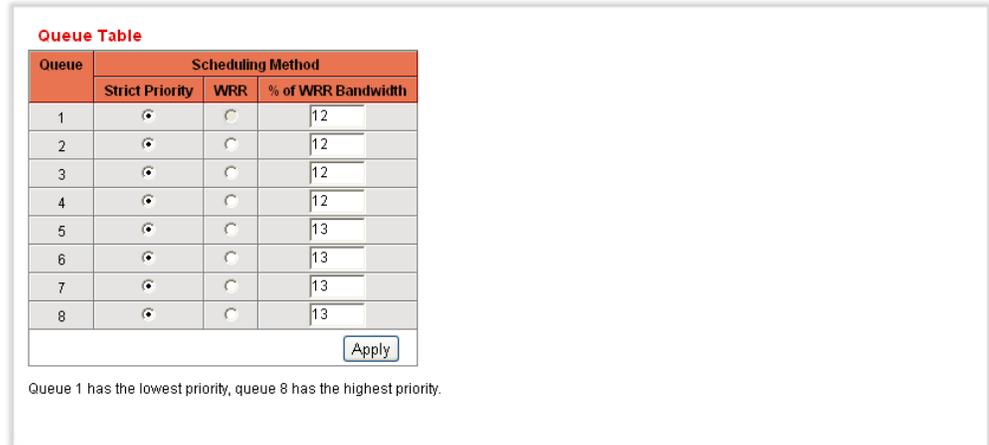
It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in strict priority. In this case traffic for the strict priority queues is always sent before traffic from the WRR queues. Only after the strict priority queues have been emptied is traffic

from the WRR queues forwarded. (The relative portion from each WRR queue depends on its weight).

To select the priority method and enter WRR data.

1. Click **Quality of Service > General > Queue**. The [Queue Page](#) is displayed.

**Figure 182: Queue Page**



Queue	Scheduling Method		
	Strict Priority	WRR	% of WRR Bandwidth
1	<input checked="" type="radio"/>	<input type="radio"/>	12
2	<input checked="" type="radio"/>	<input type="radio"/>	12
3	<input checked="" type="radio"/>	<input type="radio"/>	12
4	<input checked="" type="radio"/>	<input type="radio"/>	12
5	<input checked="" type="radio"/>	<input type="radio"/>	13
6	<input checked="" type="radio"/>	<input type="radio"/>	13
7	<input checked="" type="radio"/>	<input type="radio"/>	13
8	<input checked="" type="radio"/>	<input type="radio"/>	13

Queue 1 has the lowest priority, queue 8 has the highest priority.

2. Enter the parameters.
  - **Queue**—Displays the queue number.
  - **Scheduling Method:** Select one of the following options:
    - **Strict Priority**—Traffic scheduling for the selected queue and all higher queues is based strictly on the queue priority.
    - **WRR**—Traffic scheduling for the selected queue is based on WRR. The period time is divided between the WRR queues that are not empty, meaning they have descriptors to egress. This happens only if strict priority queues are empty.
    - **WRR Weight**—If WRR is selected, enter the WRR weight assigned to the queue.
    - **% of WRR Bandwidth**—Displays the amount of bandwidth assigned to the queue. These values represent the percent of the WRR weight.
3. Click **Apply**. The queues are configured, and the Running Configuration file is updated with the settings.

**MAPPING CoS/802.1P TO A QUEUE** The *CoS/802.1p to Queue Page* maps 802.1p priorities to egress queues. The CoS/802.1p to Queue Table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN Tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports.

**Table 5: Default Mapping Queues**

802.1p Values (0-7, 7 being the highest)	Queue (8 queues 1-8, 8 being the highest priority)	Notes
0	3	Background
1	1	Best Effort
2	2	Excellent Effort
3	4	Critical Application LVS phone SIP
4	5	Video
5	6	Voice IP phone default
6	7	Interwork Control LVS phone RTP
7	8	Network Control

By changing the CoS/802.1p to Queue mapping and the Queue schedule method and bandwidth allocation, it is possible to achieve the desired quality of services in a network.

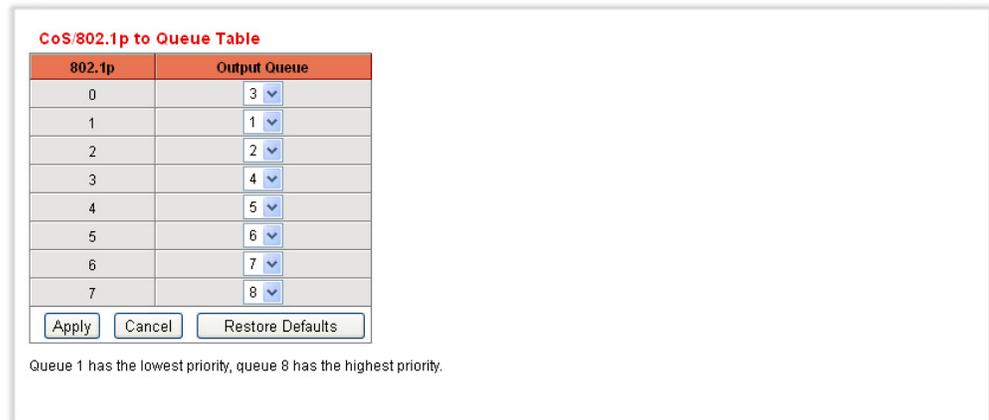
The CoS/802.1p to Queue mapping is applicable only if one of the following exists:

- ◆ The switch is in QoS Basic mode and CoS/802.1p trusted mode
- ◆ The switch is in QoS Advanced mode and the packets belong to flows that are CoS/802.1p trusted

To map CoS values to egress queues:

1. Click **Quality of Service > General > CoS/802.1p to Queue**. The [CoS/802.1p to Queue Page](#) is displayed.

Figure 183: CoS/802.1p to Queue Page



802.1p	Output Queue
0	3
1	1
2	2
3	4
4	5
5	6
6	7
7	8

Queue 1 has the lowest priority, queue 8 has the highest priority.

2. Enter the parameters.
  - **802.1p**—Displays the 802.1p priority tag values to be assigned to an egress queue, where 0 is the lowest and 7 is the highest priority.
  - **Output Queue**—Select the egress queue to which the 802.1p priority is mapped. Eight egress queues are supported, where Queue 8 is the highest priority egress queue and Queue 1 is the lowest priority.
  - **Restore Defaults**—Click to restore all queues to the factory default CoS/802.1p to Queue mapping.
3. For each 802.1p priority select the Output Queue to which it is mapped.
4. Click **Apply**. 802.1p priority values to queues are mapped, and the Running Configuration file is updated with the settings.

### MAPPING DSCP TO QUEUE

The DSCP (IP *Differentiated Services Code Point*) to Queue Page maps DSCP to egress queues. The DSCP to Queue Table determines the egress queues of the incoming IP packets based on their DSCP values. The original VPT (VLAN Priority Tag) of the packet is unchanged.

By simply changing the DSCP to Queue mapping and the Queue schedule method and bandwidth allocation, it is possible to achieve the desired quality of services in a network.

The DSCP to Queue mapping is applicable to IP packets if:

- ◆ The switch is in QoS Basic mode and DSCP is the trusted mode, or
- ◆ The switch is in QoS Advanced mode and the packets belongs to flows that is DSCP trusted

Non-IP packets are always classified to the best-effort queue.

To map DSCP to queues:

1. Click **Quality of Service** > **General** > **DSCP to Queue**. The [DSCP to Queue Page](#) is displayed.

**Figure 184: DSCP to Queue Page**

DSCP to Queue Table							
Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue
0 (BE)	1	16 (CS2)	3	32 (CS4)	5	48 (CS8)	7
1	1	17	3	33	5	49	7
2	1	18 (AF21)	3	34 (AF41)	5	50	7
3	1	19	3	35	5	51	7
4	1	20 (AF22)	3	36 (AF42)	5	52	7
5	1	21	3	37	5	53	7
6	1	22 (AF23)	3	38 (AF43)	5	54	7
7	1	23	3	39	5	55	7
8 (CS1)	2	24 (CS3)	4	40 (CS5)	6	56 (CS7)	8
9	2	25	4	41	6	57	8
10 (AF11)	2	26 (AF31)	4	42	6	58	8
11	2	27	4	43	6	59	8
12 (AF12)	2	28 (AF32)	4	44	6	60	8
13	2	29	4	45	6	61	8
14 (AF13)	2	30 (AF33)	4	46 (EF)	6	62	8
15	2	31	4	47	6	63	8

Queue 1 has the lowest priority, queue 8 has the highest priority.

The [DSCP to Queue Page](#) contains **Ingress DSCP**. It displays the DSCP value in the incoming packet and its associated class.

2. Select the **Output Queue** traffic forwarding queue) to which the DSCP value is mapped.
3. Click **Apply**. The Running Configuration file is updated with the settings.

## CONFIGURING BANDWIDTH

The [Bandwidth Page](#) enables network managers to define two sets of values that determine how much traffic the system can receive and send.

The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded.

The following values are entered for egress shaping:

- ◆ Committed Information Rate (CIR) sets the average maximum amount of data allowed to be sent on the egress interface, measured in bits per second
- ◆ Committed Burst Size (CBS) is the burst of data that is allowed to be sent, even though it is above the CIR. This is defined in number of bytes of data.

To enter bandwidth limitation:

1. Click **Quality of Service > General > Bandwidth**. The **Bandwidth Page** is displayed.

**Figure 185: Bandwidth Page**

Bandwidth Table								
Interface Type		Port	Ingress Rate Limit			Egress Shaping Rates		
Entry No.	Interface	Status	Rate Limit (KBits/sec)	%	Status	CIR (KBits/sec)	CBS (Bytes)	
<input type="checkbox"/>	1	te0/1	Disabled			Disabled		
<input type="checkbox"/>	2	te0/2	Disabled			Disabled		
<input type="checkbox"/>	3	te0/3	Disabled			Disabled		
<input type="checkbox"/>	4	te0/4	Disabled			Disabled		
<input type="checkbox"/>	5	te0/5	Disabled			Disabled		
<input type="checkbox"/>	6	te0/6	Disabled			Disabled		
<input type="checkbox"/>	7	te0/7	Disabled			Disabled		
<input type="checkbox"/>	8	te0/8	Disabled			Disabled		
<input type="checkbox"/>	9	te0/9	Disabled			Disabled		
<input type="checkbox"/>	10	te0/10	Disabled			Disabled		

The **Bandwidth Page** displays bandwidth information for each interface.

The **%** column is the ingress rate limit for the port divided by the total port bandwidth.

2. Select an interface, and click **Edit**. The **Edit Bandwidth Page** is displayed.

**Figure 186: Edit Bandwidth Page**

Interface: Port **te0/4** LAG **1**

Ingress Rate Limit: Disabled

Ingress Rate Limit:  KBits/sec. (3 - 10000000, Default: 100)

Egress Shaping Rate: Disabled

Committed Information Rate (CIR):  KBits/sec. (64 - 10000000, Default: 64)

Committed Burst Size (CBS):  Bytes (4096 - 12578880, Default: 128000)

3. Select the **Port/LAG** interface.
4. Enter the fields for the selected interface:
  - **Ingress Rate Limit**—Select to enable the ingress rate limit, which is defined in the field below.
  - **Ingress Rate Limit**—Enter the maximum amount of bandwidth allowed on the interface.



**NOTE:** The two **Ingress Rate Limit** fields do not appear when the interface type is LAG.

- **Egress Shaping Rate**—Select to enable egress shaping on the interface.
  - **Committed Information Rate (CIR)**—Enter the maximum bandwidth for the egress interface.
  - **Committed Burst Size (CBS)**—Enter the maximum burst size of data for the egress interface in bytes of data. This amount can be sent even if it temporarily increases the bandwidth beyond the allowed limit.
5. Click **Apply**. The bandwidth settings are modified, and the Running Configuration file is updated with the settings.

---

## QoS BASIC MODE

In QoS Basic mode, a specific domain in the network can be defined as trusted. Within that domain, packets are marked with 802.1p priority and/or DSCP to signal the type of service they require. Nodes within the domain use these fields to assign the packet to a specific output queue. The initial packet classification and marking of these fields is done in the ingress of the trusted domain.

To configure Basic QoS mode, perform the following:

1. Select Basic mode for the system by using the [QoS Properties Page](#).
2. Select the trust-behavior using the *Global Setting Page*. The switch supports CoS/802.1p trusted mode and DSCP trusted mode. CoS/802.1p trusted mode uses the 802.1p priority in the VLAN tag. DSCP trusted mode use the DSCP value in the IP header.
3. If there is any port that, as an exception, should not trust the incoming CoS mark, disable the QoS state on that port using the [Configuring QoS Queues](#).  
Enable or disable the global selected trusted mode at the ports by using the [Configuring QoS Queues](#). If a port is disabled without trusted mode, all its ingress packets are forward in best effort. It is recommended that you disable the trusted mode at the ports where the CoS/802.1p and/or DSCP values in the incoming packets are not trustworthy. Otherwise, it might negatively affect the performance of your network

### CONFIGURING GLOBAL SETTINGS

The [Global Settings Page](#) contains information for enabling Trust on the switch (see the *Trust Mode* field below). This configuration is active when the QoS mode is Basic mode. Packets entering a QoS domain are classified at the edge of the QoS domain.

To define the Trust configuration:

1. Click **Quality of Service > QoS Basic Mode > Global Settings**. The [Global Settings Page](#) is displayed.

**Figure 187: Global Settings Page**



The screenshot shows a configuration interface with two dropdown menus. The first is labeled 'Trust Mode' and is set to 'CoS/802.1p'. The second is labeled 'Override Ingress DSCP' and is set to 'Disabled'. To the right of these menus are three buttons: 'DSCP Override Table', 'Apply', and 'Cancel'.

2. Select the **Trust Mode** while the switch is in Basic mode. If a packet CoS level and DSCP tag are mapped to separate queues, the Trust mode determines the queue to which the packet is assigned:
  - **CoS/802.1p**—Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS/802.1p value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured in the mapping [CoS/802.1p to Queue Page](#).
  - **DSCP**—All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured in the [DSCP to Queue Page](#). If traffic is not IP traffic, it is mapped to the best effort queue.
  - **CoS/802.1p DSCP**—Traffic is mapped to queues based on the DSCP field in the IP Header, or based on the per-port default CoS/802.1p value (if there is no IP Header in the incoming packet), the actual mapping of the DSCP to queue can be configured in the mapping [DSCP to Queue Page](#).
3. If the trust mode is DSCP, select **Override Ingress DSCP** to override the original DSCP values in the incoming packets with the new values according to the DSCP Override Table. When Override Ingress DSCP is enabled, the switch will use the new DSCP values for egress queueing. It also replaces the original DSCP values in the packets with the new DSCP values.



**NOTE:** The frame is mapped to an egress queue using the new, rewritten value, and not by the original DSCP value.

4. If **Override Ingress DSCP** was enabled, click **DSCP Override Table** to reconfigure DSCP. The [Modifying Interface Default CoS Value](#) is displayed.

For more information about this page, see the [DSCP Remarking Page](#), which provides the same fields.

- Click **Apply**. The Running Configuration file is updated with the settings.

### INTERFACE QoS SETTINGS

The [Configuring QoS Queues](#) enables configuring QoS on each port of the switch, as follows:

- ◆ **QoS State Disabled on an Interface**—All inbound traffic on the port is mapped to the best effort queue and no classification/prioritization takes place.
- ◆ **QoS State of the Port is Enabled**—Port prioritize traffic on ingress is based on the system wide configured trusted mode, which is either CoS/802.1p trusted mode or DSCP trusted mode.

To enter QoS settings per interface:

- Select **Port** or **LAG** to display the list of ports or LAGs.

The list of ports/LAGs is displayed. **QoS State** displays whether QoS is enabled on the interface.

- Select an interface, and click **Edit**. The [Edit QoS Interface Settings Page](#) is displayed.

**Figure 188: Edit QoS Interface Settings Page**

**QoS Interface Setting Table**

Interface Type: Port

Entry No.	Port	QoS State
1	te0/1	Enabled
2	te0/2	Enabled
3	te0/3	Enabled
4	te0/4	Enabled
5	te0/5	Enabled
6	te0/6	Enabled
7	te0/7	Enabled
8	te0/8	Enabled
9	te0/9	Enabled
10	te0/10	Enabled

- Select **Port** or **LAG** the interface.
- Click to enable or disable **QoS State** for this interface.
- Click **Apply**. The Running Configuration file is updated with the settings.

---

## QoS ADVANCED MODE

Frames that match an ACL and were permitted entrance are implicitly labeled with the name of the ACL that permitted their entrance. Advanced mode QoS actions can then be applied to these flows.

In QoS advanced mode, the switch uses policies to support per flow QoS. A policy and its components have the following characteristics and relationships:

- ◆ A policy contains one or more class maps.
- ◆ A class map defines a flow with one or more associating ACLs. Packets that match only ACL rules (ACE) in a class map with Permit (forward) action are considered belonging to the same flow, and are subjected to the same quality of services. Thus, a policy contains one or more flows, each with a user defined QoS.
- ◆ The QoS of a class map (flow) is enforced by the associating policer. There are two type of policers, single policer and aggregate policer. Each policer is configured with a QoS specification. A single policer applies the QoS to a single class map, and thus to a single flow, based on the policer QoS specification. An aggregate policer applies the QoS to one or more class maps, and thus one or more flows. An aggregate policer can support class maps from different policies.
- ◆ Per flow QoS are applied to flows by binding the policies to the desired ports. A policy and its class maps can be bound to one or more ports, but each port is bound with at most one policy.



### NOTES:

- Single policer and aggregation policer are available when the switch is in Layer 2 mode
- An ACL can be configured to one or more class maps regardless of policies.
- A class map can belong to only one policy.
- When a class map using single policer is bound to multiple ports, each port has its own instance of single policer; each applying the QoS on the class map (flow) at a port independent of each other.
- An aggregate policer will apply the QoS to all its flow(s) in aggregation regardless of policies and ports.

Advanced QoS settings consist of three parts:

- Definitions of the rules to match. All frames matching a single group of rules are considered to be a *flow*.

- Definition of the actions to be applied to frames in each flow that match the rules.

Binding the combinations of rules and action to one or more interfaces.

---

To configure Advanced QoS mode, perform the following:

1. Select Advanced mode for the system by using the [QoS Properties Page](#).
2. Set global parameters in the [Advanced Global Settings Page](#).
3. If internal DSCP values are different from those used on incoming packets, map the external values to internal values by using the [DSCP Remarking Page](#).
4. Create ACLs, as described in [Defining Access Control](#).
5. If ACLs were defined, create class maps and associate the ACLs with them by using the [Class Mapping Page](#).
6. Create a policy using the Policy Table Page, and associate the policy with one or more class maps using the Policy Class Map Page. You can also specify the QoS, if needed, by assigning a policer to a class map when you associate the class map to the policy.

**Single Policer**—Create a policy that associates a class map with a single policer by using the [Policy Class Maps Page](#) and the [Policy Table Page](#). Within the policy, define the single policer.

**Aggregate Policer**—Create a QoS action for each flow that sends all matching frames to the same policer (aggregate policer) by using the [Aggregate Policer Page](#). Create a policy that associates a class map with the aggregate policer by using the [Policy Class Maps Page](#).

7. Bind the policy to an interface by using the [Policy Binding Page](#).

## CONFIGURING GLOBAL SETTINGS

The [Advanced Global Settings Page](#) contains information for enabling Trust on the switch (see the *Trust Mode* field below). This configuration is active when the QoS mode is Basic mode. Packets entering a QoS domain are classified at the edge of the QoS domain.

To define the Trust configuration:

1. Click **Quality of Service > QoS Advanced Mode > Global Settings**. The [Advanced Global Settings Page](#) is displayed.

Figure 189: Advanced Global Settings Page

The screenshot shows a configuration interface with three dropdown menus and three buttons. The first dropdown menu is labeled 'Trust Mode' and is set to 'CoS/802.1p-DSCP'. The second dropdown menu is labeled 'Advanced Mode Ports State' and is set to 'Not Trust'. The third dropdown menu is labeled 'Override Ingress DSCP' and is set to 'Disabled'. To the right of these menus are three buttons: 'DSCP Override Table', 'Apply', and 'Cancel'.

2. Select the **Trust Mode** while the switch is in Advanced mode. If a packet CoS level and DSCP tag are mapped to separate queues, the Trust mode determines the queue to which the packet is assigned:
  - **CoS/802.1p**—Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS/802.1p value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured in the mapping [CoS/802.1p to Queue Page](#).
  - **DSCP**—All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured in the [DSCP to Queue Page](#). If traffic is not IP traffic, it is mapped to the best effort queue.
  - **CoS/802.1p DSCP**—Traffic is mapped to queues based on the DSCP field in the IP Header, or based on the per-port default CoS/802.1p value (if there is no IP Header in the incoming packet), the actual mapping of the DSCP to queue can be configured in the mapping [DSCP to Queue Page](#).
3. If the trust mode is DSCP, select **Override Ingress DSCP** to override the original DSCP values in the incoming packets with the new values according to the DSCP Override Table. When Override Ingress DSCP is enabled, the switch will use the new DSCP values for egress queueing. It also replaces the original DSCP values in the packets with the new DSCP values.



**NOTE:** The frame is mapped to an egress queue using the new, rewritten value, and not by the original DSCP value.

4. If **Override Ingress DSCP** was enabled, click **DSCP Override Table** to reconfigure DSCP. The [Modifying Interface Default CoS Value](#) is displayed.

For more information about this page, see the [DSCP Remarking Page](#), which provides the same fields.

5. Click **Apply**. The Running Configuration file is updated with the settings.

**CONFIGURING OUT-OF-PROFILE DSCP REMARKING**

When a policer is assigned to a class maps (flows), you can specify the action to take when the amount of traffic in the flow(s) has exceed the QoS-specified limits. The portion of the traffic that causes the flow to exceed its QoS limit is referred to as *out-of-profile packets*.

If the exceed action is Out of Profile DSCP, the switch remaps the original DSCP value of the out-of-profile IP packets with a new value based on the Out of Profile DSCP Mapping Table. The switch uses the new values to assign resources and the egress queues to these packets. The switch also physically replaces the original DSCP value in the out of profile packets with the new DSCP value.

To use the out-of-profile DSCP exceed action, remap the DSCP value in the Out Of Profile DSCP Mapping Table. Otherwise the action is null, because the DSCP value in the table remaps the packets to itself by factory default.

The [DSCP Remarking Page](#) enables the *change-the-DSCP-value* of traffic entering or leaving the switch.

This feature changes the DSCP tags for incoming traffic switched between trusted QoS domains. Changing the DSCP values used in one domain, sets the priority of that type of traffic to the DSCP value used in the other domain to identify the same type of traffic.

These settings are active when the system is in the QoS basic mode, and once activated they are active globally.

For example: Assume that there are three levels of service: Silver, Gold, and Platinum and the DSCP incoming values used to mark these levels are 10, 20, and 30 respectively. If this traffic is forwarded to another service provider that has the same three levels of service, but uses DSCP values 16, 24, and 48, **DSCP Remarking** changes the incoming values as they are mapped to the outgoing values.

To map DSCP values:

1. Click **Quality of Service > QoS Advanced Mode > DSCP Remarking**. The Out of Profile [DSCP Remarking Page](#) is displayed.

Figure 190: DSCP Remarking Page

**DSCP Remarking Table**

DSCP In	DSCP Out						
0	0	16	16	32	32	48	48
1	1	17	17	33	33	49	49
2	2	18	18	34	34	50	50
3	3	19	19	35	35	51	51
4	4	20	20	36	36	52	52
5	5	21	21	37	37	53	53
6	6	22	22	38	38	54	54
7	7	23	23	39	39	55	55
8	8	24	24	40	40	56	56
9	9	25	25	41	41	57	57
10	10	26	26	42	42	58	58
11	11	27	27	43	43	59	59
12	12	28	28	44	44	60	60
13	13	29	29	45	45	61	61
14	14	30	30	46	46	62	62
15	15	31	31	47	47	63	63

Apply Cancel Restore Defaults

2. Select the **Trust Mode** while the switch is in Advanced mode. If a packet CoS level and DSCP tag
3. **DSCP In** displays the DSCP value of the incoming packet that needs to be remarked to an alternative value.
4. Select the **DSCP Out** value to where the incoming value is mapped.
5. Click **Apply**. The Running Configuration file is updated with the settings with the new DSCP remarking table.

**DEFINING CLASS MAPPING**

A Class Map defines a traffic flow with ACLs (Access Control Lists). A MAC ACL, IP ACL, and IPv6 ACL can be combined into a class map. Class maps are configured to match packet criteria on a match-all or match-any basis. They are matched to packets on a first-fit basis, meaning that the action associated with the first-matched class map is the action performed by the system. Packets that matches the same class map are considered to belong to the same flow.

Defining class maps does not have any effect on QoS; it is an interim step, enabling the class maps to be used later.

If more complex sets of rules are needed, several class maps can be grouped into a super-group called a policy (see the [Configuring a Policy](#) section).

The [Class Mapping Page](#) shows the list of defined class maps and the ACLs comprising each, and enables you to add/delete class maps.

To define a class map:

1. Click **Quality of Service > QoS Advanced Mode > Class Mapping**. The [Class Mapping Page](#) is displayed.

**Figure 191: Class Mapping Page**



This page displays the already-defined class maps.

2. Click **Add**. The [Add Class Mapping Page](#) is displayed.

**Figure 192: Add Class Mapping Page**



A new class map is added by selecting one or two ACLs and giving the class map a name. If a class map has two ACLs, you can specify that a frame must match both ACLs, or that it must match either one or both of the ACLs selected.

3. Enter the parameters.
  - **Class Map Name**—Enter the name of a new class map.
  - **Match ACL Type**—The criteria that a packet must match in order to be considered to belong to the flow defined in the class map. The options are:
    - **IP**—A packet must match either of the IP based ACLs in the class map.
    - **MAC**—A packet must match the MAC based ACL in the class map.
    - **IP and MAC**—A packet must match the IP based ACL and the MAC based ACL in the class map.

- **IP or MAC**—A packet must match either the IP based ACL or the MAC based ACL in the class map.
  - **IP**—Select the IPv4 based ACL or the IPv6 based ACL for the class map.
  - **MAC**—Select the MAC based ACL for the class map.
  - **Preferred ACL**—Select whether packets are first matched to an IP-based ACL or a MAC-based ACL.
4. Click **Apply**. The Running Configuration file is updated with the settings.

**QoS POLICERS** You can measure the rate of traffic that matches a pre-defined set of rules, and to enforce limits, such as limiting the rate of file-transfer traffic that is allowed on a port.

This can be done by using the ACLs in the class map(s) to match the desired traffic, and by using a policer to apply the QoS on the matching traffic.

QoS policers are not supported when the switch is in Layer 3 mode.

A policer is configured with a QoS specification. There are two kinds of policers:

- ◆ **Single (Regular) Policer**—A single policer applies the QoS to a single class map, and to a single flow based on the policer's QoS specification. When a class map using single policer is bound to multiple ports, each port has its own instance of single policer; each applying the QoS on the class map (flow) at ports that are otherwise independent of each other. A single policer is created in the [Policy Class Maps Page](#).
- ◆ **Aggregate Policer**—An aggregate policer applies the QoS to one or more class maps, and one or more flows. An aggregation policer can support class maps from different policies. An aggregate policer applies QoS to all its flow(s) in aggregation regardless of policies and ports. An aggregate policer is created in the [Aggregate Policer Page](#).

An aggregate policer is defined if the policer is to be shared with more than one class.

Each policer is defined with its own QoS specification with a combination of the following parameters:

- ◆ A maximum allowed rate, called a Committed Information Rate (CIR), measured in Kbps.
- ◆ An amount of traffic, measured in bytes, called a Committed Burst Size (CBS). This is traffic that is allowed to pass as a temporary burst even if it is above the defined maximum rate.

- ◆ An action to be applied to frames that are over the limits (called out-of-profile traffic), where such frames can be passed as is, dropped, or passed, but remapped to a new DSCP value that marks them as lower-priority frames for all subsequent handling within the device.

Assigning a policer to a class map is done when a class map is added to a policy. If the policer is an aggregate policer, you must create it using the [Aggregate Policar Page](#).

## DEFINING AGGREGATE POLICERS

An aggregate policer applies the QoS to one or more class maps, therefore one or more flows. An aggregation policer can support class maps from different policies and will apply the QoS to all its flow(s) in aggregation regardless of policies and ports.

The switch supports aggregate policers and single policers only when operating in Layer 2 mode.

To define an aggregate policer:

1. Click **Quality of Service > QoS Advanced Mode > Aggregate Policar**. The [Aggregate Policar Page](#) is displayed.

**Figure 193: Aggregate Policar Page**

<input type="checkbox"/>	Aggregate Policar Name	Ingress CIR	Ingress CBS	Exceed Action
Table is empty				
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>				

This page displays the existing aggregate policers.

2. Click **Add**. The [Add Aggregate Policar Page](#) is displayed.

**Figure 194: Add Aggregate Policar Page**

Aggregate Policar Name \*

Ingress Committed Information Rate (CIR) \* 3 KBits/sec. (3 - 57982058, Default: 3)

Ingress Committed Burst Size (CBS) \* 3000 Bytes (3000 - 19173960, Default: 3000)

Exceed Action Forward

3. Enter the parameters.
  - **Aggregate Policar Name**—Enter the name of the Aggregate Policar.

- **Ingress Committed Information Rate (CIR)**—Enter the maximum bandwidth allowed in bits per second. See description in the [Bandwidth Page](#).
  - **Ingress Committed Burst Size (CBS)**—Enter the maximum burst size (even if it goes beyond the CIR) in bytes. See description in the [Bandwidth Page](#).
  - **Exceed Action**—Select the action to be performed on incoming packets that exceed the CIR. Possible values are:
    - *Forward*—Packets exceeding the defined CIR value are forwarded.
    - *Drop*—Packets exceeding the defined CIR value are dropped.
    - *Out of Profile DSCP*—The DSCP values of packets exceeding the defined CIR value are remapped to a value based on the Out Of Profile DSCP Mapping Table.
4. Click **Apply**. The Running Configuration file is updated with the settings.

## CONFIGURING A POLICY

The [Policy Table Page](#) displays the list of advanced QoS polices defined in the system. The page also allows you to create and delete polices. Only those policies that are bound to an interface are active (see [Policy Binding Page](#)).

Each policy consists of:

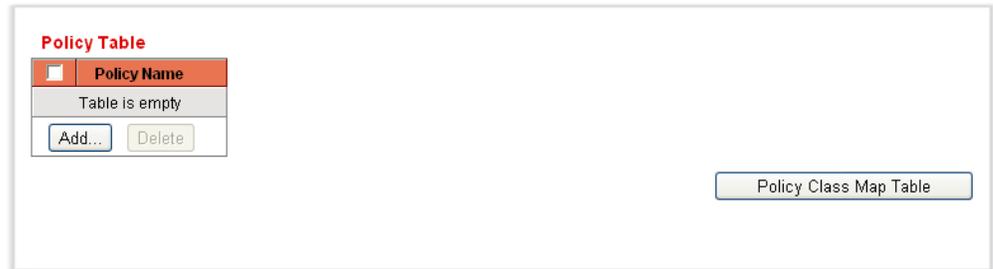
- ◆ One or more class maps of ACLs which define the traffic flows in the policy.
- ◆ One or more aggregates that applies the QoS to the traffic flows in the policy.

After a policy has been added, class maps can be added by using the [Policy Class Maps Page](#).

To add a QoS policy:

1. Click **Quality of Service > QoS Advanced Mode > Policy Table**. The [Policy Table Page](#) is displayed.

**Figure 195: Policy Table Page**



This page displays the list of defined policies.

2. Click **Add** to open the [Add Policy Table Page](#).

**Figure 196: Add Policy Table Page**



3. Enter the name of the new policy in the **New Policy Name** field.
4. Click **Apply**. The QoS policy profile is added, and the Running Configuration file is updated with the settings.

## CONFIGURING POLICY CLASS MAPS

One or more class maps can be added to a policy. A class map defines the type of packets that are considered to belong to the same traffic flow.

You cannot configure a policer to a class map when the switch is operating in Layer 3 mode. The switch supports policers only in Layer 2 mode.

To add a class map to a policy:

1. Click **Quality of Service > QoS Advanced Mode > Policy Class Maps**. The [Policy Class Maps Page](#) is displayed.

**Figure 197: Policy Class Maps Page**



2. Select a policy in the Filter, and click **Go**. All class maps in that policy are displayed.
3. To add a new class map, click **Add**. The [Add Policy Class Map Page](#) is displayed.

**Figure 198: Add Policy Class Map Page**

The screenshot shows the 'Add Policy Class Map Page' configuration interface. The form is titled 'Test2' and contains the following fields and options:

- Policy Name:** Test2
- Class Map Name:** A dropdown menu.
- Action Type:** Radio buttons for 'None', 'Trust CoS/802.1p, DSCP', and 'Set'. The 'Set' option is selected, with a 'DSCP' dropdown and a 'New Value' input field containing '0' and '(0-63)'.
- Police Type:** A dropdown menu with 'None' selected.
- Aggregate Policer:** A dropdown menu.
- Ingress Committed Information Rate (CIR):** An input field with 'kbits/sec. (3 - 10000000)'.
- Ingress Committed Burst Size (CBS):** An input field with 'Bytes (3000 - 19173960)'.
- Exceed Action:** A dropdown menu with 'None' selected.
- Apply:** A button in the bottom right corner.

4. Enter the parameters.
  - **Policy Name**—Displays the policy to which the class map is being added.
  - **Class Map Name**—Select an existing class map to be associated with the policy. Class maps are created in the [Class Mapping Page](#).
  - **Action Type**—Select the action regarding the ingress CoS/802.1p and/or DSCP value of all the matching packets.
    - **None**—Ignore the ingress CoS/802.1p and/or DSCP value. The matching packets are sent as best effort.
    - **Trust CoS/802.1p, DSCP**—If this option is selected, the switch will trust the CoS/802.1p and DSCP of the matching packet. If a packet is an IP packet, the switch will put the packet in the egress queue based on its DSCP value and the DSCP to Queue Table. Otherwise, the egress queue of the packet is based on the packet's CoS/802.1p value and the CoS/802.1p to Queue Table.
    - **Set**—If this option is selected, use the value entered in the **New Value** box to determine the egress queue of the matching packets as follows:

If the new value (0..7) is a CoS/802.1p priority, use the priority value and the CoS/802.1p to Queue Table to determine the egress queue of all the matching packets.

If the new value (0..63) is a DSCP, use the new DSCP and the DSCP to Queue Table to determine the egress queue of the matching IP packets.

Otherwise, use the new value (1..8) as the egress queue number for all the matching packets.

- **Police Type**—Available in Layer 2 Mode only. Select the policer type for the policy. The options are:
  - *None*—No policy is used.
  - *Single*—The policer for the policy is a single policer.
  - *Aggregate*—The policer for the policy is an aggregate policer.
- **Aggregate Policer**—Available in Layer 2 Mode only. If **Police Type** is *Aggregate*, select a previously-defined (in the [Aggregate Policer Page](#)) aggregate policer.

If **Police Type** is *Single*, enter the following QoS parameters:

- **Ingress Committed Information Rate (CIR)**—Enter the CIR in Kbps. See description in the [Bandwidth Page](#).
- **Ingress Committed Burst Size (CBS)**—Enter the CBS in bytes. See description in the [Bandwidth Page](#).
- **Exceed Action**—Select the action assigned to incoming packets exceeding the CIR. The options are:
  - *None*—No action.
  - *Drop*—Packets exceeding the defined CIR value are dropped.
  - *Out of Profile DSCP*—IP packets exceeding the defined CIR are forwarding with a new DSCP derived from the Out Of Profile DSCP Mapping Table.

5. Click **Apply**.

**POLICY BINDING** The [Policy Binding Page](#) shows which policy profile is bound and to which port. When a policy profile is bound to a specific port, it is active on that port. Only one policy profile can be configured on a single port, but a single policy can be bound to more than one port.

When a policy is bound to a port, it filters and applies QoS to ingress traffic that belongs to the flows defined in the policy. The policy does not apply to traffic egress to the same port.

To edit a policy, it must first be removed (unbound) from all those ports to which it is bound.

To define policy binding:

1. Click **Quality of Service > QoS Advanced Mode > Policy Binding**. The [Policy Binding Page](#) is displayed.



This section describes the Data Center Ethernet (DCE) feature.

A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems.

These features are used to configure the Data Center switch to monitor and control traffic.

This section contains the following topics:

- ◆ [Fiber Channel over Ethernet Initialization Protocol \(FIP\) Snooping](#)
- ◆ [Cut-Through](#)
- ◆ [Quantized Congestion Notification \(QCN\)](#)
- ◆ [Priority-based Flow Control \(PFC\)](#)
- ◆ [Configuring ETS](#)
- ◆ [Data Center Discovery and Capability Exchange Protocol \(DCBX\)](#)

---

## FIBER CHANNEL OVER ETHERNET INITIALIZATION PROTOCOL (FIP) SNOOPING

Fibre Channel over Ethernet (FCoE) is a protocol designed to move native Fibre Channel over 10 Gigabit Ethernet and above links. In order for FCoE, a mechanism is required to carry the base Fibre Channel port / device login mechanisms over Ethernet. These are the processes for a port to log in and obtain a routable Fibre Channel Address.

The FCoE Initialization Protocol (FIP) enables an Ethernet-attached FC node (Enode) to discover existing Fiber Channel Forwarders (FCFs) and supports the FC login procedure over 10+GE networks.

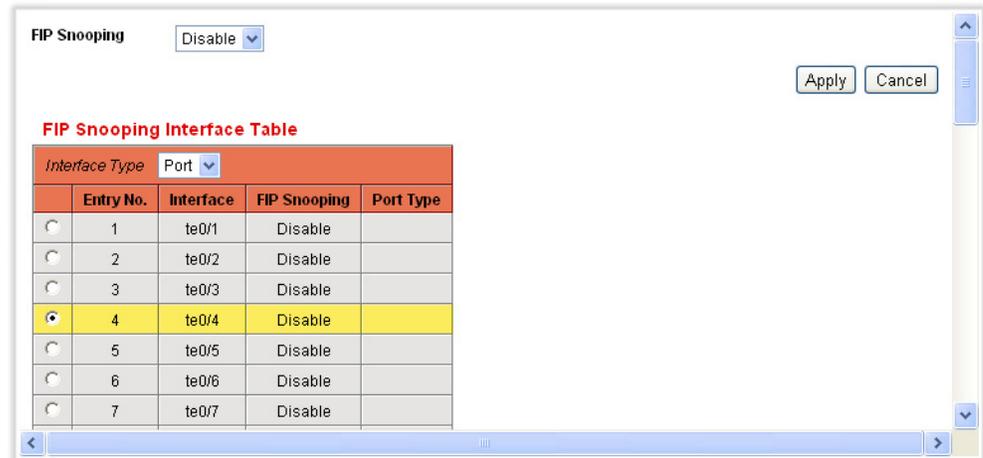
FIP provides an Ethernet MAC address used by FCoE to traverse the Ethernet network which contains the FCID required to be routed on the FC network. FIP also passes the query and query response from the FC name server. FIP uses a separate Ethertype from FCoE and its frames are standard Ethernet size (1518 Byte 802.1q frame) whereas FCoE frames are 2242 Byte Jumbo Frames

The switch performs FIP snooping, which is a frame inspection method that is used to monitor FIP frames and apply policies based on the information in those frames.

To configure FIP Snooping:

1. Click **DCE > FIP Snooping** in the tree view to display the [FIP Snooping Page](#).

**Figure 200: FIP Snooping Page**



2. Enable/disable FIP snooping globally.
3. To enable/disable FIP on a port/LAG, select the port/LAG, and click **Edit**. The [Edit FIP Snooping Interface Settings Page](#) is displayed.

**Figure 201: Edit FIP Snooping Interface Settings Page**



4. Enable or disable FIP snooping on the port/LAG in the **Administrative FIP Snooping** field. The following options are available:
  - *Disable*—The port/LAG does not support FIP.
  - *Non-FCoE*—Discard all FCoE and FIP traffic received on the port.
  - *FCF*—Place switch in this mode because router (or forwarder) is connected to it.
  - *Enode*—Place switch in this mode because a server is connected to port.
5. Click **Apply**. The Running Configuration file is updated with the settings.

**FIP MAC ADDRESS FILTERING** To create a list of MAC addresses for filtering purposes:

1. Click **DCE > FIP Snooping** in the tree view to display the [FIP Snooping Page](#).
2. To configure destination MAC address filtering, click **FIP Snooping FCF Address Filtering Setting**. The [FCF Mac Address Filtering Page](#) is displayed.

**Figure 202: FCF Mac Address Filtering Page**



3. (Optional) Enable **FCF Mac Address Filtering** and click **Apply**.
4. To add the permitted destination MAC addresses, Click **Add**. The [Add FCF MAC Address Filter Page](#) is displayed.

**Figure 203: Add FCF MAC Address Filter Page**



5. Enable or disable FCF MAC Address filtering. This determines how traffic from the source MAC addresses are handled:
  - Enable
    - Traffic from the MAC addresses in this list is discarded.
    - Tunnels whose destination addresses are not in this list are removed.
  - Disable - Removes rules to discard traffic with source addresses in the list.
6. Enter the **MAC Address**.

7. Click **Apply**. The Running Configuration file is updated with the settings.

**FIP TUNNELS** You can create static tunnels or enable the creation of dynamic tunnels.

The parameters for a tunnel are:

- ◆ Enode Port.
- ◆ Source address
- ◆ Destination address

A tunnel is added if a FC Fabric Login (FLOGI) request was accepted by the Fiber Channel Forwarder (FCF). The destination MAC address is the FCF address and the source MAC address is the address that was assigned to the virtual link.

A dynamic tunnel is removed in the following cases:

- ◆ A fabric logout request message was accepted by FCF.
- ◆ FIP Clear Virtual Links message were sent by FCF.
- ◆ FIP Keep Alive messages were not received for 270 seconds from the Enode.
- ◆ The FCF has stopped sending FIP Discovery Advertisements (for 3 times). The period time is one of the attributes in the discovery advertisement.

If there is no space in the TCAM, tunnels are not be created causing traffic to be discarded by the switch. The device issues rate-limited SYSLOG messages when it cannot create dynamic tunnels.

To configure tunneling on an interface for FIP snooping:

1. Click **DCE > FIP Snooping** in the tree view to display the [FIP Snooping Page](#).
2. Click **FIP Snooping Tunnel Setting**. The [FIP Snooping Tunnel Setting Table Page](#) is displayed.

**Figure 204: FIP Snooping Tunnel Setting Table Page**

3. Select port/LAG and tunnel type and click **Go**. The following is displayed for existing tunnels:
  - **Interface** —Port or LAG number.
  - **Source MAC Address**—MAC source of the (FC) enode.
  - **Destination MAC Address**—Destination MAC address of the forwarder.
  - **Type**—Tunnel type - static or dynamic.
  - **FCoE Source ID**—Source ID of the fiber channel.
4. To add a static tunnel, click **Add**. The [Add Static FIP Snooping Tunnel Page](#) is displayed.

**Figure 205: Add Static FIP Snooping Tunnel Page**

5. Enter the parameters:
  - **Interface**—Select a port/LAG.
  - **Source MAC Address**—Add the MAC source of the (FC) enode.
  - **Destination MAC Address**—Add the destination MAC address of the forwarder.
6. Click **Apply**. The Running Configuration file is updated with the settings.

---

## CUT-THROUGH

In cut-through switching the switch starts forwarding a frame before the whole frame has been received, normally as soon as the destination address is processed.

Cut-through reduces latency through the switch.

### LIMITATIONS AND INTERACTIONS WITH OTHER FEATURES

The disadvantage of Cut-through are:

- ◆ The FCS of the frame is not checked prior to transmitting the packet.
- ◆ Cut-through switching can only be used where the speed of the outgoing interface is less than or equal to the incoming interface speed.
- ◆ The packet size is unknown at the time of deciding whether to transmit the packet

The following limitations should be considered:

- ◆ PFC, QCN and Shaping cannot be enabled if there is at least one port that is configured for Cut-through.
- ◆ Cut-through cannot be enabled for a port if PFC or QCN or Shaping is enabled.
- ◆ Policing and Rate-Limiting for a port cannot be enabled if the port is configured for Cut-through.
- ◆ Cut-through for a port cannot be enabled if a policer or rate-limiter is enabled for that port.
- ◆ In case jumbo frame forwarding is disabled and Cut Through is enabled, Jumbo frames are forwarded, but the device marks the CRC as bad.

### CONFIGURING CUT-THROUGH

To configure cut-through:

1. Click **DCE > Cut-through** in the tree view to display the [Cut-through Page](#).

Figure 206: Cut-through Page

Cut-Through State: Disable

Cut-Through State After Reboot: Disable

Cut-Through 802.1Q priority:  0,  1,  2,  3,  4,  5,  6,  7

Cut-Through Packet Length: 1522

Cut-Through Packet Length After Reboot: 1522 Bytes (257 - 16383)

Apply Cancel

**Interface Setting Table**

	Entry No.	Interface	Cut-Through		Interface Speed(bits/sec)	Untagged Packets
			Administrative	Operational		
<input type="radio"/>	1	te0/1	Disable	Disable	1G	Disable
<input type="radio"/>	2	te0/2	Disable	Disable	10G	Disable
<input type="radio"/>	3	te0/3	Disable	Disable	10G	Disable
<input type="radio"/>	4	te0/4	Disable	Disable	10G	Disable
<input type="radio"/>	5	te0/5	Disable	Disable	10G	Disable

The Cut-through state (enabled/disabled) is displayed in **Cut-through State**.

- To change the Cut-through state, enter the parameters.
  - Cut-through State After Reboot**—Enable or disable the cut-through state after reboot. To actually change the Cut-through state, reboot the switch.
  - Cut-through Priority**—Set the QoS priorities for which cut-through is enabled.
  - Cut-through Packet Length**—Displays the assumed packet length. Since the ASIC does not know the packet length when it starts processing the packet, this is the length that is used as the packet length.
  - Cut-through Packet Length After Reboot**—Change the cut-through packet length. For this value to be changed, the system must be rebooted.
- Click **Apply**. The Running Configuration file is updated with the settings.

The Interface Setting Table displays the Cut-through parameters for the interfaces.

- To change Cut-through parameters for a port, select a port, and click **Edit**. The [Edit Interface Setting Page](#) is displayed.

Figure 207: Edit Interface Setting Page

Interface	te0/4
Cut-Through	Disable
Untagged Packets	Disable
Interface Speed	10G
Operational Cut-Through	Disable

5. Enter the parameters for the port:
  - **Interface**—Port number.
  - **Cut-through**—Enable or disable the cut-through on this port.
  - **Untagged packets**—Enable or disable forwarding in Cut-through mode untagged packets on this port. If enabled, untagged packets are stored and immediately forwarded. If the packets are tagged, this depends on the priority.
  - **Interface Speed**—Displays the speed of the port. Cut-through does not work on ports whose speed is less than 10G.
  - **Operational Cut-through**—Displays whether cut-through is actually enabled or disabled.
6. Click **Apply**. The Running Configuration file is updated with the settings.

---

## QUANTIZED CONGESTION NOTIFICATION (QCN)

Quantized Congestion Notification (QCN) addresses the problem of sustained congestion. This is done by having congestion points generate congestion notification messages. These messages can be used to take corrective action at the ingress of the switch.

**QUEUE CONFIGURATION** The system automatically creates a Congestion Point (CP) for a queue if at least one QCN priority is mapped to that queue. It creates a CP for all the ports that are QCN-enabled.

The QCN configuration of a queue is independent of the queue's buffers allocation:

- ◆ If the QCN priority is also a PFC priority, the egress queue is *infinite* (TD is disabled) and the set-point determines the optimal queue length in case of congestion.
- ◆ If the QCN priority is non-PFC priority, the egress queue is usually be able to take resources from a shared pool. Here again, the set-point

determines the optimal queue length in egress in case of congestion. If congestion occurs simultaneously in multiple non-PFC ports, then it is possible that the CN algorithm would not avoid packet discarding.

**CN TAG RECOGNITION** When QCN is globally enabled, the device recognizes EtherType 0x22E9 as a CN-tag. This means that the device is able to skip the CN-tag when searching the packet content. Because of this, IP ACLs can be applied on CN-tagged IP packets, and also on packets that are classified to QCN-disabled priorities.

VLAN untagged packets with CN tagged packets are not supported.

**LIMITATIONS AND  
INTERACTIONS WITH  
OTHER FEATURES**

Coexistence limitations:

- ◆ QCN can be globally enabled if:
  - The QoS mode is Basic and the basic trust mode is CoS.
  - The QoS mode is Advanced and the default action is Trust and advanced trust mode is CoS.
- ◆ If QCN is globally enabled then:
  - QoS cannot be disabled.
  - The Basic trust mode cannot be changed if Basic mode is enabled.
  - The Advanced trust mode cannot be changed if Advanced mode is enabled.
  - The default action cannot be changed if Advanced mode is enabled.
  - QoS can be set to Basic mode only if the Basic trust mode is CoS.
  - QoS can be set to Advanced mode only with the default action Trust and Advanced trust mode is CoS.

**CONFIGURING QCN** To configure QCN:

1. Click **DCE > QCN** in the tree view to display the [QCN Page](#).

Figure 208: QCN Page

Quantized Congestion Notification (QCN)

QCN Priority Enable

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7

QCN Messages (CNMs) Priority

---

**QCN Congestion Point**

Queue Size Set Point  Bytes (512 - 4294967295)

Feedback Weight  ((-8) - 7)

Minimum Sample Base  Bytes (10000 - 4294967295)

**Quantized Congestion Notification Table**

Entry No.	Interface	Quantized Congestion Notification
<input type="radio"/> 1	te0/1	Disable
<input type="radio"/> 2	te0/2	Disable
<input checked="" type="radio"/> 3	te0/3	Disable
<input type="radio"/> 4	te0/4	Disable

2. Enter the parameters.
  - **Quantized Congestion Notification**—Enable or disable QCN.
  - **QCN Priority Enable**—Check a priority to enable or disable QCN for it
  - **QCN Messages (CNMs) Priority**—Set the priority of for the Congestion Notification Messages. These messages can be received only if VLAN priority tagging is defined for the report.
  - **Queue Size Set Point**—Set the queue size set point in bytes. This is the reaction point or threshold of traffic that triggers generation of QCN messages.
  - **Feedback Weight**—Set the feedback weight. It is recommended that this value not be modified.
  - **Minimum Sample Base**—Set the minimum configure the minimum number of bytes to enqueue in a QCN egress queue between transmission of Congestion Notification Messages.
3. Click **Apply**. The Running Configuration file is updated with the settings.
4. Select a port, and click **Edit**. The [Edit Quantized Congestion Notification Page](#) is displayed.

**Figure 209: Edit Quantized Congestion Notification Page**

Interface	te0/3
Quantized Congestion Notification	Disable
<input type="button" value="Apply"/>	

5. Enable or disable QCN on the port:
6. Click **Apply**. The Running Configuration file is updated with the settings.

---

## PRIORITY-BASED FLOW CONTROL (PFC)

Priority-based flow control (PFC), IEEE standard 802.1Qbb, is a link-level flow control mechanism that operates on individual priorities, allowing you to selectively pause traffic according to its class.

Traditional IEEE 802.3 Ethernet defines an unreliable communication medium in that it does not guarantee that a packet, injected into the network, will arrive at its intended destination.

In a network path that normally consists of multiple hops between source and destination, lack of feedback between transmitters and receivers at each hop is one of the main causes of this unreliability.

Transmitters can send packets faster than receivers accept packets, and as the receivers run out of available buffer space to absorb incoming flows, they are forced to silently drop all traffic that exceeds their capacity. These processes work well at Layer 2, as long as upper-layer protocols handle drop-detection and retransmission logic.

For applications that cannot build reliability into upper layers, the addition of flow control functions at Layer 2 offers a solution. Flow control enables feedback from a receiver to its sender to communicate buffer availability.

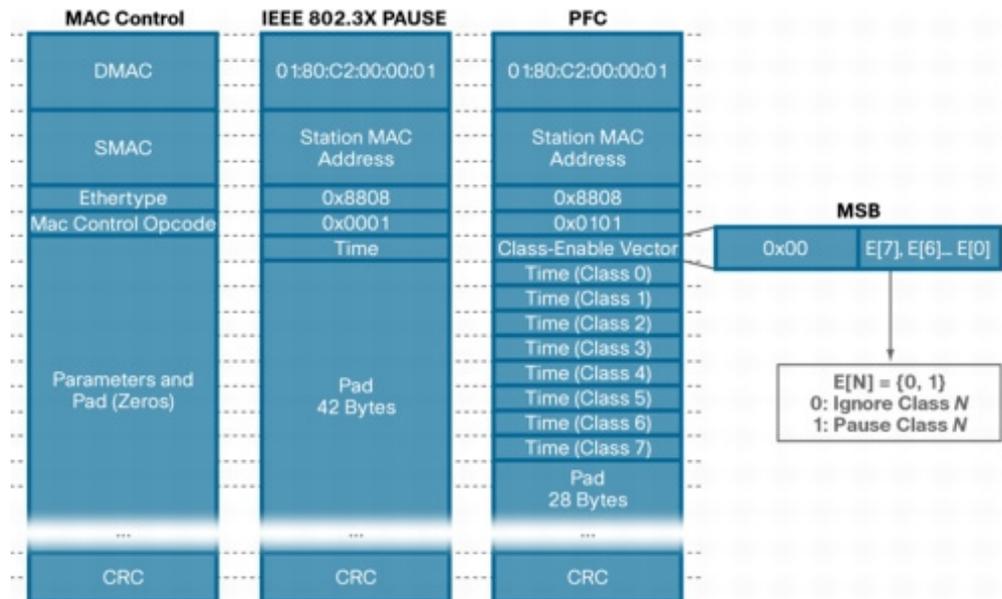
The first implementation of Flow Control in IEEE 802.3 Ethernet used the IEEE 802.3x PAUSE control frames. IEEE 802.3x PAUSE is defined in Annex 31B of the IEEE 802.3 specification. Simply put, a receiver can generate a MAC control frame and send a PAUSE request to a sender when it predicts the potential for buffer overflow. Upon receiving a PAUSE frame, the sender responds by stopping transmission of new packets until the receiver is ready to accept them again.

IEEE 802.3x PAUSE works as designed, but it suffers a basic disadvantage that limits its field of applicability: after a link is paused, a sender cannot generate any more packets. Because of this, the application of IEEE 802.3x PAUSE makes an Ethernet segment unsuitable for carrying multiple traffic flows that might require different quality of service (QoS). Thus, enabling IEEE 802.3x PAUSE for one application can affect the performance of other network applications.

IEEE 802.1Qbb PFC extends the basic IEEE 802.3x PAUSE semantics to multiple CoSs, enabling applications that require flow control to coexist on the same wire with applications that perform better without it. PFC uses the IEEE 802.1p CoS values in the IEEE 802.1Q VLAN tag to differentiate up to eight CoSs that can be subject to flow control independently.

The differences between IEEE 802.3x PAUSE and PFC frames are shown in Figure 210:

**Figure 210: Difference Between IEEE 802.3x PAUSE and PFC Frames**



**PRIORITY TO QUEUE MAPPING**

The system assumes that:

- ◆ Packets that are tagged with PFC-enabled priority are classified to the egress queue based on the Priority2Queue mapping table that is defined today in the QoS module.
- ◆ Packets that are tagged with PFC-disabled priority are not classified to an egress queue of PFC enabled priority.

The Priority2Queue mapping table that is defined in the QoS module is also used for the PFC feature.

**PFC PRIORITY OPERATIONAL STATE**

If the port speed is 1G or less, the **DCBX operational state** is disabled.

For 10G ports, if the **DCBX Operational State** is enabled for a port and the **DCBX Priority-Flow-Control Advertise** is enabled for the port, then the DCBX feature determines the operational state of PFC for the port. Otherwise, PFC is enabled for a port if the **Priority-Flow-Control** is enabled globally and on the port.

**Priority-Flow-Control Priority Oper** (global) is enabled for a priority if:

- ◆ **Priority-Flow-Control Priority** is globally enabled for that priority.
- ◆ That priority is mapped to a dedicated queue (I.e. no other priority is mapped to that queue).
- ◆ The priority is mapped to a queue that is equal to the priority number plus 1.

**BUFFERS ALLOCATION** For lossless traffic, a buffer is allocated to a frame before the frame is sent from the remote peer.

This is done in the following way:

- ◆ Allocating guaranteed buffers per port.
- ◆ Decrementing the number of available buffers for a port when buffers are allocated for a packet that ingresses the port.
- ◆ Incrementing the number of available buffers (for the ingress port) when buffers are released (at the egress port).
- ◆ Signaling PAUSE frame to remote peer when the number of available buffers has reach some threshold.

This allocation is called "allocation by ingress port". In many aspects it can be viewed as a queue at the ingress. The egress ports in this case are not TD queues. The main disadvantage of this allocation is Head of Line blocking (HOL).

For non HOL traffic, packets are not discarded at the ingress port due to lack of resources. The decision whether to discard the packet due to lack of resources is made at egress ports according to the congestion at the egress queues. The egress ports in this case are TD queues.

The allocation for non HOL traffic is called "allocation by egress port".

If **Priority-Flow-Control** (Global) is enabled and **Priority-Flow-Control Priority** (Global) is enabled for a priority then the buffer allocation for the associated Queue is per ingress port for all the ports in the device; otherwise the buffer allocation for the associated queue is per egress port.

**PFC AND QoS** This section describes the connection between PFC operation and QoS configuration.

### ADVANCED MODE

Advanced mode has two mode of default actions for packets that are not classified by the Policy map to a QoS action: No trust and trust.

In the Trust default action mode, traffic is classified according to packets fields. The trusted packet fields are determined by a new global configuration command named Advanced Trust mode. The available values of this mode are: **cos**, **dscp** or **cos-dscp**.

This default action mode applies to all the ports. There is no trust control per port in Advanced mode.

The Advanced Trust mode also specifies the packet fields that are trusted when a packet matches a trust command in a policy-map (For both default action modes).

The **trust cos-dscp** command in policy-map class configuration mode is replaced by the **trust** command.

The remapping requirement that is described below is also relevant in Advanced mode for PFC-disabled ports for both default action modes.

Set queue, set VPT and set DSCP actions are also supported. The user must take not to map lossless packets to the wrong queue and lossy traffic to PFC queues.

#### LIMITATION IN REGARD TO QoS

PFC can be globally enabled if:

- ◆ The QoS mode is Basic and the Basic Trust mode is CoS.
- ◆ The QoS mode is Advanced and the default action is trust and Advanced Trust mode is CoS.
- ◆ If PFC is globally enabled, the Basic Trust mode cannot be changed if Basic mode is enabled.
- ◆ Advanced trust mode and the default action cannot be changed if Advanced mode is enabled.
- ◆ QoS cannot be disabled.
- ◆ QoS can be set to Basic mode only when the Basic Trust mode is CoS.
- ◆ QoS can be set to Advanced mode only if the default action trust and Advanced Trust mode is CoS.
- ◆ In Basic mode, the user can enable PFC for a port only if the port state is trusted. The user cannot change the port state to untrust if PFC is enabled for that port.
- ◆ For PFC disabled (Admin) ports, the trust mode can be trusted or not.

#### REMAPPING

The ASIC does not support allocating buffers at ingress per <port, priority> but only per priority. The ASIC does support XON/XOFF for flow-control per <port, priority>. Hence, this requires directing to a new queue, traffic that ingresses a non-PFC port with a PFC-enabled priority tag.

Otherwise packets from a non-PFC port can fill all the buffers at ingress, causing loss of packets to PFC-enabled ports.

The following requirements are relevant for Basic mode and advanced mode:

Queue 1 cannot be PFC enabled.

If **Priority-Flow-Control** (Global) is enabled and **Priority-Flow-Control Priority** (Global) is enabled for a priority, traffic classified to that priority from ports with **Priority-Flow-Control Oper** (interface) disabled should be mapped to queue 1.

The remapping also performs remarking of VPT according to the assigned queue.

### Example:

#### VPT2 Queue

```
0 -> 0
1 -> 1
2 -> 2 PFC enabled
3 -> 3 PFC enabled
4 -> 4
5 -> 5
6 -> 6
7 -> 7
```

#### VPT2 Queue Remapped

```
0 -> 0
1 -> 1
2 -> 0 with remarking to VPT 0
3 -> 0 with remarking to VPT 0
4 -> 4
5 -> 5
6 -> 6
7 -> 7
```

**ISCSI WITH PFC** ISCSI traffic can be transmitted over PFC priorities and non-PFC priorities. For non-PFC priorities, QoS actions are required, while for PFC traffic QoS actions are not allowed.

For PFC sessions, the session rules (for counting) do not include QoS actions (Whether a session is a PFC session can be determined by the snooping application according to the VPT of the packet).

Permit rules (without QoS action) for the PFC priorities are added before the default QoS action rules in order to skip those rules for PFC traffic. This requires reserving two rules in the TCAM.

It is user's responsibility not to map the non-PFC ISCSI traffic to a PFC queue.

**VOICE VLAN** It is the user's responsibility not to map the Voice VLAN traffic to a PFC queue.

**PFC AND SHAPER COEXISTENCE** The following describe constraints between PFC and shaper.

- ◆ Port shaping cannot be enabled if PFC is enabled for the port.
- ◆ If PFC is enabled for an port then port shaping cannot be enabled.
- ◆ A PFC-enabled queue is a queue on a PFC-enabled port that PFC is enabled for the priority that is mapped to the queue.
- ◆ For PFC-enabled queues, shaping cannot be enabled.
- ◆ If shaping is enabled for a queue, that queue cannot be set to PFC-enabled.
- ◆ Shaping per queue can be enabled for a PFC port for PFC-disabled queues.

**PERFORMANCE** Define the associated Queue for Priority as follows:

Associated-Queue= priority2queue (Priority), where priority2queue function is the priority2queue mapping table.

If **Priority-Flow-Control Oper** (port) is enabled for a priority on a port, then the traffic that is classified to the associated queue should be lossless for links in length equal to and lower than X (Product Specific) with packet size of 2240 bytes (FCOE frames) and lower.

If **Priority-Flow-Control Oper** (interface) is enabled for a priority on an interface then traffic that is classified to the associated queue should be lossless for links in length equal and lower than Y with packet size of 9K bytes (FCOE frames) and lower.

If **Priority-Flow-Control Oper** (interface) is disabled for a priority for all the ports in the system, then HOL blocking should be prevented for traffic that is classified to the associated queue.

The link utilization should be 100% for any cable length with packets size of 64 – 2240 bytes in lossless and in non-HOL modes. Link utilization of 100% means that a congested egress port constantly transmits in full wire.

**CASCADE PORTS** PFC should be enabled on cascade ports for a priority if:

- ◆ PFC is globally enabled.
- ◆ PFC is enabled for that priority.

**PFC AND LAGS** PFC cannot be enabled on LAGs. It can be enabled on ports in LAGs.

**COEXISTENCE WITH LINK LEVEL FC (802.3X)** If **Priority-Flow-Control** (global) is disabled, Link level FC works in a usual way, including buffers allocation configurations.

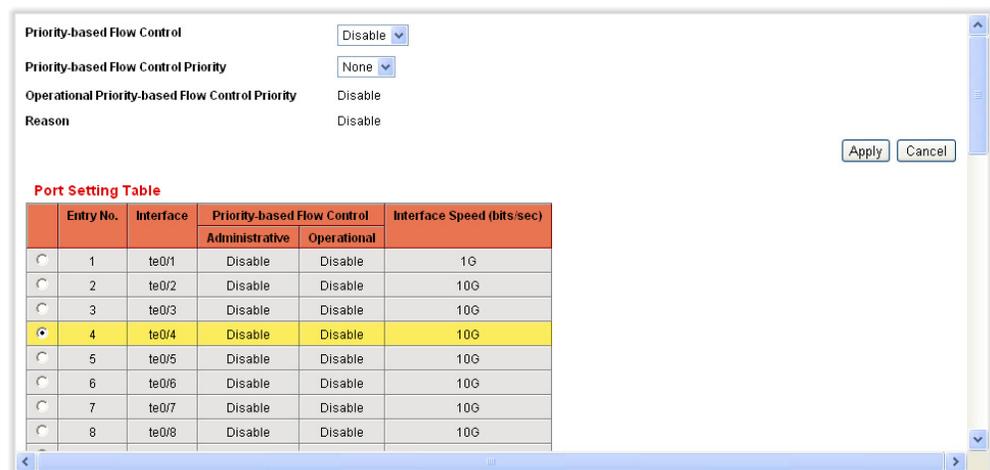
If for one of the ports link level FC is enabled, **Priority-Flow-Control** (global) cannot be enabled.

If **Priority-Flow-Control** (global) is enabled, Link level FC cannot be enabled.

**CONFIGURING PFC** To configure PFC on specific ports:

1. Click **DCE > PFC** in the tree view to display the [PFC Page](#).

**Figure 211: PFC Page**



2. Enter the parameters:
  - **Priority-based Flow Control**—Enable or disable PFC.
  - **Priority-based Flow Control Priority**—Enable/disable PFC per priority level.
  - **Operational Priority-based Flow Control Priority**—Displays whether PFC is actually enabled per priority, as opposed to how it was defined for that priority. See the *PFC Priority Operational State* section.
  - **Reason**—If flow control is disabled for any reason other than a user configuration, that reason is displayed here.
3. Click **Apply**. The Running Configuration file is updated with the settings.

4. To enable/disable PFC on a port, select it, and click **Edit**. The [Edit Priority-based Flow Control Page](#) is displayed.

**Figure 212: Edit Priority-based Flow Control Page**



Interface	te0/4
Priority-based Flow Control	Disable
<input type="button" value="Apply"/>	

5. Enable or disable PFC for the port:
6. Click **Apply**. The Running Configuration file is updated with the settings.

---

## CONFIGURING ETS

To support consolidation of Ethernet and Fibre-Channel (FCOE) in high-speed networks, such as data centers, link bandwidth between the applications must be shared.

IEEE 802.1az standard specifies the requirements for bandwidth sharing.

Enhanced Transmission Selection (ETS) is configured in the **Quality of Service > General > Queue** page.

To configure ETS:

1. Click **DCE > ETS** in the tree view to display the [ETS Page](#).

**Figure 213: ETS Page**

Quality of Service -> General -> Queue'." data-bbox="298 638 903 723"/>

ETS (Enhanced Transmission Selection) can be configured in the [Quality of Service -> General -> Queue](#)

2. Click **Quality of Service > General > Queue**. The [Queue Page](#) is displayed. This page is described in the [Configuring QoS Queues](#) section.

## DATA CENTER DISCOVERY AND CAPABILITY EXCHANGE PROTOCOL (DCBX)

DCBX is used by DCB devices to exchange configuration information with directly-connected peers. The protocol may also be used for detection of incorrect configurations and for configuration of the peer.

DCBX supports the following:

- ◆ **Discovery of DCB capability in a peer.** DCBX is used to discover the capabilities of peer devices. It is a means to know if the peer device supports a particular feature, such as Priority Groups (PG) or Priority-based Flow Control (PFC).
- ◆ **DCB enables detection of incorrect configuration.** DCBX can be used to detect misconfiguration of a feature between the peers on a link. Misconfiguration detection is feature-specific because some features may allow asymmetric configuration.
- ◆ **Peer configuration of DCB features.** DCBX can be used by a device to perform peer-to-peer configuration of DCB features in its link peer.

### CONFIGURING DCBX THROUGH THE GUI

To configure DCBX:

1. Click **System > DCBX** in the tree view to display the [DCBX Page](#).

Figure 214: DCBX Page

DCBX port settings							
Entry No.	Port	DCB Exchange Protocol	Advertise Priority Groups	Advertise Priority Flow-Control	Advertise Application Protocol	Application Protocol	
1	te0/1	Enable	Enable	Enable	Enable	Disable	
2	te0/2	Enable	Enable	Enable	Enable	Disable	
3	te0/3	Enable	Enable	Enable	Enable	Disable	
4	te0/4	Enable	Enable	Enable	Enable	Disable	
5	te0/5	Enable	Enable	Enable	Enable	Disable	
6	te0/6	Enable	Enable	Enable	Enable	Disable	
7	te0/7	Enable	Enable	Enable	Enable	Disable	
8	te0/8	Enable	Enable	Enable	Enable	Disable	
9	te0/9	Enable	Enable	Enable	Enable	Disable	
10	te0/10	Enable	Enable	Enable	Enable	Disable	
11	te0/11	Enable	Enable	Enable	Enable	Disable	
12	te0/12	Enable	Enable	Enable	Enable	Disable	

2. The page displays the following fields for all ports:

- **Port**—The port.
- **DCBX Exchange Protocol**—Displays whether the DCBX exchange protocol is enabled or disabled.
- **Advertise Priority Groups**—Displays whether advertising ETS configuration is enabled or disabled.
- **Advertise Priority Flow-Control**—Displays whether advertising Priority Flow Control (PFC) is enabled or disabled.

- **Advertise Application Protocol**—Displays whether advertising the protocol used (for example FCoE or FIP) is enabled or disabled.
  - **Application Protocol**—Displays whether mapping protocols to priorities is enabled or disabled.
3. To change these settings for a port, select it and click **Edit**. The [Edit Port Settings Page](#) is displayed.

**Figure 215: Edit Port Settings Page**

Port	te0/4
DCB Exchange Protocol	Enable
Advertise Priority Groups	Enable
Advertise Priority Flow-Control	Enable
Advertise Application Protocol	Enable
Application Protocol	Disable

Apply

4. Enter the parameters.
5. Click **Apply**. The Running Configuration file is updated with the settings.
6. To map applications to 802.1Q priorities, click **Application Priority Mapping**. The [Application to Priority Mapping Table Page](#) is displayed.

**Figure 216: Application to Priority Mapping Table Page**

**Application to Priority Mapping**  
Table

Application Protocol Type	Priority
Ether Type	TCP/UDP Port
Table is empty	

Add... Delete

DCBX Port Setting

7. To map an application to a priority, click **Add**. The [Add Application to Priority Mapping Page](#) is displayed.

**Figure 217: Add Application to Priority Mapping Page**

The screenshot shows a configuration form with the following fields and options:

- Application Protocol Type:** A dropdown menu with 'EtherType' selected.
- TCP/UDP Port:** A text input field with '(0-65535)' as a hint.
- Protocol:** A dropdown menu with 'FCoE' selected.
- EtherType:** A text input field with '(0x0 - 0xFFFF)' as a hint.
- Priority:** A list of radio buttons for values 0 through 7.
- Apply:** A button in the bottom right corner.

8. Enter the following fields:
  - **Application Protocol Type**—Enter the Ethernet Type, which determines if FIP or FCoE ethertype is used. Using the FIP Ethertype creates a tunnel.
  - **TCP/UDP Port**—.The TCP or UDP port used by the application.
  - **Protocol**—.The FCoE, FIP, or other protocol (as specified by the EtherType value).
  - **EtherType**—.Identifier for the application protocol.
  - **Priority**—.The 802.1p priority tag value to be assigned to the application, where 0 is the lowest and 7 is the highest priority.
9. Click **Apply**. The Running Configuration file is updated with the settings.



This chapter describes the Simple Network Management Protocol (SNMP) feature that provides a method for managing network devices.

It includes the following topics:

- ◆ [SNMP Versions and Workflow](#)
- ◆ [Model OID](#)
- ◆ [SNMP Engine ID](#)
- ◆ [Configuring SNMP Views](#)
- ◆ [Managing SNMP Users](#)
- ◆ [Creating SNMP Groups](#)
- ◆ [Defining SNMP Communities](#)
- ◆ [Defining Trap Settings](#)
- ◆ [Defining Notification Recipients](#)
- ◆ [Configuring SNMP Notification Filters](#)

---

## SNMP VERSIONS AND WORKFLOW

The switch functions as SNMP agent and supports SNMP v1, v2, and v3. It also reports system events to trap receivers using the traps defined in the MIB that it supports.

**SNMP v1 AND v2** To control access to the system, a list of community entries is defined. Each community entry consists of a *community string* and its access privilege. Only SNMP messages with the suitable community string and operation are responded to by the system.

SNMP agents maintain a list of variables that are used to manage the switch. The variables are defined in the *Management Information Base* (MIB). The MIB presents the variables controlled by the agent.



---

**NOTE:** SNMPv2 protocol has known security vulnerabilities, and it is recommended to use SNMPv3.

---

**SNMP v3** In addition to the functionality provided by SNMP v1 and v2, SNMP v3 applies access control and new trap mechanisms to SNMPv1 and SNMPv2 PDUs. SNMPv3 also defines a User Security Model (USM) that includes:

- ◆ **Authentication**—Provides data integrity and data origin authentication.
- ◆ **Privacy**—Protects against disclosure message content. *Cipher Block-Chaining (CBC)* is used for encryption. Either authentication alone is enabled on an SNMP message, or both authentication and privacy are enabled on an SNMP message. However, privacy cannot be enabled without authentication.
- ◆ **Timeliness**—Protects against message delay or playback attacks. The SNMP agent compares the incoming message time stamp to the message arrival time.
- ◆ **Key Management**—Defines key generation, key updates, and key use. The switch supports SNMP notification filters based on *Object IDs* (OID). OIDs are used by the system to manage device features.

**SNMP WORKFLOW** The following is the recommended series of actions for configuring SNMP:



---

**NOTE:** The switch comes with SNMP turned off by default. Before you can configure SNMP, you must turn on SNMP by using *Security-> TCP/UDP Services*.

---

#### **IF YOU DECIDE TO USE SNMP v1 OR v2:**

Define a community by using the [Add SNMP Community Page](#). The community can be associated with an access rights and view in Basic mode or with a group in Advanced mode. (See the [Communities Page](#) for information on Basic and Advanced modes.) There are two ways to define access rights to a community:

- ◆ Basic mode - The access rights of a community can configure with Read Only, Read Write, or SNMP Admin. In addition, you can restrict the access to the community to only certain MIB objects using a view. views are defined in the SNMP Views Page
- ◆ Advanced Mode - The access rights to a community is defined by a group. You can configure the group with a specific security model. The access rights in a group is defined by the Read, Write, and Notify access to the desired views Groups are defined in the SNMP Views Page.

If you decide to use SNMP v3:

1. Define the SNMP engine, one time, by using the [Engine ID Page](#).
2. If desired, define SNMP view(s) by using the [SNMP Views Page](#).
3. Define groups by using the [Groups Page](#).
4. Define users by using the [SNMP Users Page](#), where they can be associated with a group.

#### TRAPS AND NOTIFICATIONS MANAGEMENT FOR SNMP v1, v2, OR v3:

1. Enable or disable traps by using the [Trap Settings Page](#).
2. Optionally, define a notification filter(s) by using the [Notification Filter Page](#).
3. Define a notification recipient(s) by using the [SNMPv1,2 Notification Recipient Page](#) and/or [SNMPv3 Notification Recipient Page](#), respectively.

**SUPPORTED MIBS** The following standard MIBs are supported:

- ◆ CISCO-CDP-MIB.mib
- ◆ CISCO-SMI.mib
- ◆ CISCO-TC.mib
- ◆ CISCO-VTP-MIB.mib
- ◆ diffserv.mib
- ◆ draft-ietf-bridge-8021x.mib
- ◆ draft-ietf-bridge-rstpmib-04.mib
- ◆ draft-ietf-entmib-sensor-mib.mib
- ◆ draft-ietf-hubmib-etherif-mib-v3-00.mib
- ◆ draft-ietf-syslog-device-mib.mib
- ◆ ianaaddrfamnumbers.mib
- ◆ ianaifty.mib
- ◆ ianaprot.mib
- ◆ inet-address-mib.mib
- ◆ ip-forward-mib.mib
- ◆ ip-mib.mib
- ◆ lldp.mib
- ◆ p-bridge-mib.mib
- ◆ q-bridge-mib.mib
- ◆ RFC-1212.mib
- ◆ rfc1213.mib
- ◆ rfc1389.mib
- ◆ rfc1493.mib
- ◆ rfc1611.mib
- ◆ rfc1612.mib
- ◆ rfc1757.mib
- ◆ rfc1850.mib
- ◆ rfc1907.mib
- ◆ rfc2011.mib

- ◆ rfc2012.mib
- ◆ rfc2013.mib
- ◆ rfc2096.mib
- ◆ rfc2233.mib
- ◆ rfc2571.mib
- ◆ rfc2572.mib
- ◆ rfc2573.mib
- ◆ rfc2574.mib
- ◆ rfc2575.mib
- ◆ rfc2576.mib
- ◆ rfc2613.mib
- ◆ rfc2618.mib
- ◆ rfc2620.mib
- ◆ rfc2665.mib
- ◆ rfc2668.mib
- ◆ rfc2674.mib
- ◆ rfc2737.mib
- ◆ rfc2851.mib
- ◆ rfc2925.mib
- ◆ rfc3621.mib
- ◆ rfc4668.mib
- ◆ rfc4670.mib
- ◆ rmon2.mib
- ◆ SNMPv2-CONF.mib
- ◆ SNMPv2-SMI.mib
- ◆ SNMPv2-TC.mib
- ◆ trunk.mib
- ◆ udp-mib.mib

---

## MODEL OID

The switch MIB Object ID (OID) root is 1.3.6.1.4.1.259.10.1.14.

---

## SNMP ENGINE ID

The Engine ID is only used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set), and sends Trap messages to a manager. The agent's local information is encapsulated in fields in the message.

Each SNMP agent maintains local information that is used in SNMPv3 message exchanges (not relevant for SNMPv1 or SNMPv2). The default SNMP Engine ID is comprised of the enterprise number and the default MAC address. The SNMP engine ID must be unique for the administrative domain, so that no two devices in a network have the same engine ID.

The local information is stored in four MIB variables that are read-only (snmpEngineId, snmpEngineBoots, snmpEngineTime, and snmpEngineMaxMessageSize).



**NOTE:** When the engine ID is changed, all configured users and groups are erased.

To define the SNMP engine ID:

1. Click **SNMP > Engine ID**. The [Engine ID Page](#) is displayed.

**Figure 218: Engine ID Page**

Local Engine ID    None  Use default

2. Select the **Local Engine ID**.
  - **User defined**—Enter the local device engine ID. The field value is a hexadecimal string (**range: 10 - 64**). Each byte in the hexadecimal character strings is represented by two hexadecimal digits. Each byte can be separated by a period or a colon.
  - **None**—No Engine ID is used.
  - **Use default**—Select to use the device-generated engine ID. The default Engine ID is based on the switch MAC address, and is defined per standard as:
    - *First 4 octets*—First bit = 1, the rest is the IANA enterprise number.
    - *Fifth octet*—Set to 3 to indicate the MAC address that follows.
    - *Last 6 octets*—MAC address of the switch.
3. Click **Apply**. The Running Configuration file is updated with the settings.

## CONFIGURING SNMP VIEWS

A view is a user-defined label for a collection of MIB tree subtrees. Each subtree ID is defined by the *Object ID* (OID) of the root of the relevant subtrees. In extreme cases, this subtree can be a leaf, only. Well-known names can be used to specify the root of the desired subtree or an OID can be entered (see [Model OID](#)).

Each subtree is either included or excluded in the view being defined.

The [SNMP Views Page](#) enables creating and editing SNMP views. The default views (Default, DefaultSuper) cannot be changed.

Views can be attached to groups in the [Groups Page](#).

To define SNMP views:

1. Click **SNMP > Views**. The [SNMP Views Page](#) is displayed.

**Figure 219: SNMP Views Page**

The screenshot shows a 'View Table' with a dropdown menu for 'View Name' set to 'Default'. The table lists several views with their Object ID Subtree and Object ID Subtree View status. At the bottom right of the table are 'Add...' and 'Delete' buttons.

<input type="checkbox"/>	View Name	Object ID Subtree	Object ID Subtree View
<input type="checkbox"/>	Default	1	Included
<input type="checkbox"/>	Default	1.3.6.1.6.3.13	Excluded
<input type="checkbox"/>	Default	1.3.6.1.6.3.16	Excluded
<input type="checkbox"/>	Default	1.3.6.1.6.3.18	Excluded
<input type="checkbox"/>	Default	1.3.6.1.6.3.12.1.2	Excluded
<input type="checkbox"/>	Default	1.3.6.1.6.3.12.1.3	Excluded
<input type="checkbox"/>	Default	1.3.6.1.6.3.15.1.2	Excluded
<input type="checkbox"/>	Default	1.3.6.1.4.1.259.10.1.14.89.2.7.2	Excluded
<input type="checkbox"/>	DefaultSuper	1	Included

2. Select the user-defined views from the **ViewTable** list. The following views exist by default:
  - **Default**—Default SNMP view for read and read/write views.
  - **DefaultSuper**—Default SNMP view for administrator views.
  - Other views can be added.
  - **Object ID Subtree**—Displays the subtree to be included or excluded in the SNMP view.
  - **Object ID Subtree View**—Displays whether the defined subtree is included or excluded in the selected SNMP view.
3. Click **Add** to define new views. The [Add View Page](#) is displayed.

**Figure 220: Add View Page**

The screenshot shows the 'Add View Page' with the following fields and controls:

- View Name**: A text input field.
- Object ID Subtree**: A radio button labeled 'Select from list' is selected. Below it is a list box containing 'system', 'interfaces', 'ip', 'icmp', and 'tcp'. 'Up' and 'Down' buttons are next to the list box.
- User defined**: A radio button labeled 'User defined' is unselected. To its right is a text input field containing '1.3.6.1.2.1.1'.
- Include in view**: A checked checkbox.
- Apply**: A button at the bottom right.

4. Enter the parameters.
  - **View Name**—Enter a view name.
  - **Object ID Subtree**—Select the node in the MIB tree that is included or excluded in the selected SNMP view. The options to select the object are as follows:
    - *Select from list*—Enables you to navigate the MIB tree. Press the *Up* arrow to go to the level of the selected node's father and siblings; press the *Down* arrow to descend to the level of the selected node's descendents. Click nodes in the view to pass from one node to its brother. Use the scrollbar to bring siblings in view.
    - *User defined*—Enter an OID not offered in the *Select from List* option (if required). All descendents of this node are included or excluded in the view.
5. Select or deselect **Include in view**.
  - If *Select from list* is used, the **Object Identifier of the selected node** is included in or excluded from the view if the **Include in view** option is selected or not selected.
  - If *User defined* is used, the **entered Object Identifier** is included in or excluded from the view if the **Include in view** option is selected or not selected.
6. Click **Apply**. If you used *Select from list*, the object identifier of the selected node is included in or excluded from the view as determined by the **Include in view** option is selected.

If you used **Object ID**, the entered object identifier is included in or excluded from the view if the **Include in view** option is selected. This means that the node and its descendents are included or excluded from the view. The SNMP views are defined, and the Running Configuration file is updated with the settings.

---

## MANAGING SNMP USERS

An SNMP user is defined by the login credentials (username, passwords, and authentication method), and by the context and scope in which it operates by association with a group and an Engine ID.

After a user is authenticated, it takes on the attributes of its group, and can then see or not see the views associated with this group.

The [SNMP Users Page](#) enables the creation of SNMPv3 users. An SNMPv3 user is the combination of a user along with a method that is used to authenticate the user and a password. SNMP user login credentials are verified using the local database.

Groups enable network managers to assign access rights to specific features, or feature aspects, to an entire group of users instead of to a single user.

A user can only be a member of a single group.

To create an SNMPv3 user, the following must first exist:

- ◆ An engine ID must first be configured on the switch. This can be done in the [Engine ID Page](#).
- ◆ An SNMPv3 group must be available. An SNMPv3 group can be defined in the [Groups Page](#).

SNMP users are not saved to the configuration file for security reasons. If SNMP users are provisioned and you save the configuration, the SNMP users are not retained; you must manually re-enter them.

To display SNMP users and define new ones:

1. Click **SNMP > Users**. The [SNMP Users Page](#) is displayed.

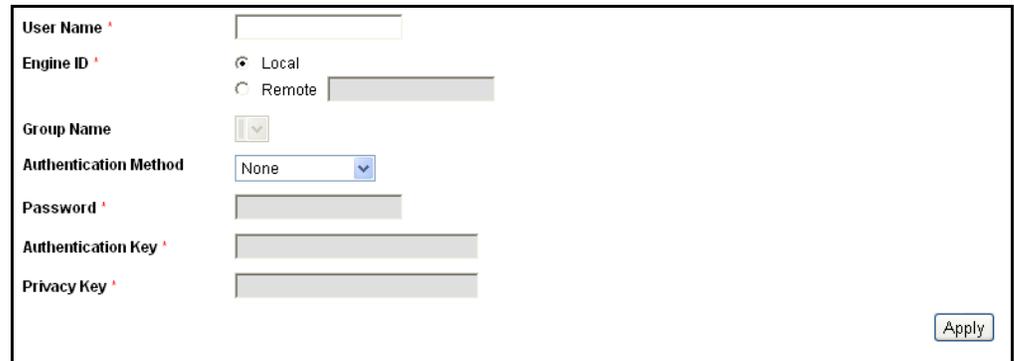
**Figure 221: SNMP Users Page**



This page displays existing users.

2. Click **Add**. The [SNMP Users Page](#) is displayed.

**Figure 222: Add User Page**



The screenshot shows the "Add User" configuration page. It includes the following fields and controls:

- User Name \***: A text input field.
- Engine ID \***: Radio buttons for "Local" (selected) and "Remote", followed by a text input field.
- Group Name**: A dropdown menu.
- Authentication Method**: A dropdown menu with "None" selected.
- Password \***: A text input field.
- Authentication Key \***: A text input field.
- Privacy Key \***: A text input field.
- Apply**: A button at the bottom right.

This page provides information for assigning SNMP access control privileges to SNMP users.

3. Enter the parameters.
  - **User Name**—Enter a name for the user.
  - **Engine ID**—Select either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 User Database. To receive both informs and request information, you must define both a local and remote user.
    - *Local*—User is connected to a local SNMP entity. The user can request information but does not receive inform messages.
    - *Remote*—User is connected to a remote SNMP entity. If the remote Engine ID is defined, remote devices receive inform messages, but cannot make requests for information. Enter the remote engine ID.
  - **Group Name**—Select the SNMP groups to which the SNMP user belongs. SNMP groups are defined in the [Add Group Page](#).
  - **Authentication Method**—Select the Authentication method. The options are:
    - *None*—No user authentication is used.
    - *MD5 Password*—Users must enter a password that is encrypted using the MD5 authentication method.
    - *SHA Password*—Users must enter a password that is encrypted by using the SHA (Secure Hash Algorithm) authentication method.
    - *MD5 Key*—Users are authenticated by using a valid MD5 key.
    - *SHA Key*—Users are authenticated by using a valid SHA key.
  - **Password**—If authentication is accomplished by either a MD5 or a SHA password, enter the local user password. Local user passwords are compared to the local database and can contain up to 32 ASCII characters.
  - **Authentication Key**—If the authentication method is either an MD5 or SHA key, enter the MD5 or SHA authentication key. If the MD5 key is selected, 16 bytes are required. If the SHA key is selected, 20 bytes are required.
  - **Privacy Key**—If the Authentication Method is either a MD5 or a SHA key, enter the MD5 or SHA privacy key. If the MD5 key is selected, 16 bytes are required. If the SHA key is selected, 20 bytes are required.
4. Click **Apply**. The Running Configuration file is updated with the settings.

## CREATING SNMP GROUPS

In SNMPv1 and SNMPv2, a community string is sent along with the SNMP frames. The community string acts as a password to gain access to a SNMP agent. However, neither the frames nor the community string are encrypted. So SNMPv1 and SNMPv2 are not secure. In SNMPv3, there are two security mechanisms, and both can be configured.

- ◆ Authentication—The switch checks that the SNMP user is an authorized system administrator. This is done for each and every frame.
- ◆ Privacy—SNMP frames can carry encrypted data.

Thus, in SNMPv3, there are three levels of security:

- ◆ No security
- ◆ Authentication
- ◆ Authentication and privacy (Note that two groups with the same name, one with authentication and one with privacy, must be added.)

In addition, SNMPv3 provides for a way to control what even authorized and authenticated users can see and perform, by associating each user with a group.

A group is a label for a logical entity (combination of attributes). A group is operational only when it is associated with an SNMP user or an SNMP community.

A group also has an attribute that tells if members should have read, write, and/or notify privileges for the view.

To create an SNMP group:

1. Click **SNMP > Groups**. The [Groups Page](#) is displayed.

**Figure 223: Groups Page**



Group Name	Security Model	Security Level	Views		
			Read	Write	Notify
Table is empty					
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>					

This page displays the existing SNMP groups.

2. Click **Add**. The [Add Group Page](#) is displayed.

Figure 224: Add Group Page

The screenshot shows a web-based configuration page for adding an SNMP group. It contains the following elements:

- Group Name:** A text input field.
- Security Model:** A dropdown menu currently set to "SNMPv1".
- Security Level:** A dropdown menu currently set to "No Authentication".
- Views:** Three checkboxes labeled "Read", "Write", and "Notify". Each checkbox is followed by a dropdown menu, all of which are currently set to "Default".
- Apply:** A button in the bottom right corner.

3. Enter the parameters.

- **Group Name**—Enter a new group name for which privileges are being defined. The field range is up to 30 ASCII characters.
- **Security Model**—Select the SNMP version attached to the group.
- **Security Level**—Define the security level attached to the group. Security levels apply to SNMPv3 only.
  - *No Authentication*—Neither the Authentication nor the Privacy security levels are assigned to the group.
  - *Authentication*—Authenticates SNMP messages, and ensures the SNMP message origin is authenticated but does not encrypt them, meaning that they can be intercepted and read.
  - *Privacy*—Encrypts SNMP messages.
- **Views**—Define the group access rights per group. The options are:
  - *Read*—Management access is read-only for the selected view. Otherwise, a user or a community associated with this group, is able to read all MIBs except those that control SNMP itself.
  - *Write*—Management access is write for the selected view. Otherwise, a user or a community associated with this group, is able to write all MIBs except those that control SNMP itself.
  - *Notify*—Sends only traps with contents that is included in the SNMP view selected for notification. Otherwise, there is no restriction on the contents of the traps. This can only be selected for SNMP v3.

4. Click **Apply**. The SNMP Group is defined, and the Running Configuration file is updated with the settings.

## DEFINING SNMP COMMUNITIES

Access rights in SNMPv1 and SNMPv2 are managed by defining communities in the [Communities Page](#). The community name is a type of shared password between the SNMP management station and the device. It is used to authenticate the SNMP management station.

Communities are only defined in SNMPv1 and v2 because SNMP v3 works with users instead of communities. The users belong to groups that have access rights assigned to them.

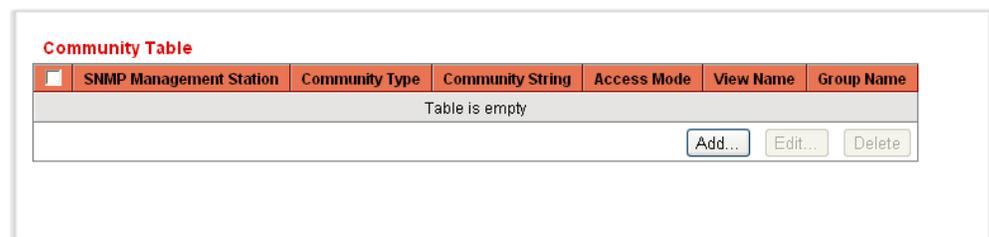
The [Communities Page](#) associates communities with access rights, either directly (Basic mode) or through groups (Advanced mode):

- ◆ Basic mode - The access rights of a community can configure with Read Only, Read Write, or SNMP Admin. In addition, you can restrict the access to the community to only certain MIB objects using a view. views are defined in the SNMP Views Page
- ◆ Advanced Mode - The access rights to a community is defined by a group. You can configure the group with a specific security model. The access rights in a group is defined by the Read, Write, and Notify access to the desired views Groups are defined in the SNMP Views Page.

To define SNMP communities:

1. Click **SNMP > Communities**. The [Communities Page](#) is displayed.

**Figure 225: Communities Page**



<input type="checkbox"/>	SNMP Management Station	Community Type	Community String	Access Mode	View Name	Group Name
Table is empty						
				<input type="button" value="Add..."/>	<input type="button" value="Edit..."/>	<input type="button" value="Delete"/>

This page displays the Basic and Advanced tables.

2. Click **Add**. The [Add SNMP Community Page](#) is displayed.

Figure 226: Add SNMP Community Page

This page enables network managers to define and configure new SNMP communities.

**3. SNMP Management Station**—Click **User defined** to enter the management station IP address that can access the SNMP community. Or click **All** to indicate that any IP device can access the SNMP community.

- **IP Version**—Select either IPv4 or IPv6.
- **IPv6 Address Type**—Select the supported IPv6 address type if IPv6 is used). The options are:
  - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - *Global*—The IPv6 address is a global Unicast IPv6 type that is visible and reachable from other networks.
- **Link Local Interface**—If the IPv6 address type is Link Local, select whether it is received through VLAN2 or ISATAP.
- **IP Address**—Enter the SNMP management station IPv4 address.
- **Community String**—Enter the community name (password) used to authenticate the management station to the device.
- **Basic**—Select this mode for a selected community. In this mode, there is no connection to any group. You can only choose the community access level (R/O, R/W, or Admin) and, optionally, further qualify it for a specific view. By default, it applies to the entire MIB. If this is selected, enter the following fields:
  - *Access Mode*—Select the access rights of the community. The options are:

Read Only—Management access is restricted to read-only. Changes cannot be made to the community.

Read Write—Management access is read-write. Changes can be made to the device configuration, but not to the community.

SNMP Admin—User has access to all device configuration options, as well as permissions to modify the community. Admin is equivalent to Read Write for all MIBs except for the SNMP MIBs. Admin is required for access to the SNMP MIBs.

- *View Name*—Select an SNMP view (a collection of MIB subtrees to which access is granted).
  - **Advanced**—Select this mode for a selected community.
  - *Group Name*—Select an SNMP group that determines the access rights.
4. Click **Apply**. The SNMP Community is defined, and the Running Configuration file is updated with the settings.

---

## DEFINING TRAP SETTINGS

The [Trap Settings Page](#) enables configuring whether SNMP notifications are sent from the switch, and for which cases. The recipients of the SNMP notifications can be configured in the [SNMPv1,2 Notification Recipient Page](#), or the [SNMPv3 Notification Recipient Page](#).

To define trap settings:

1. Click **SNMP > Trap Settings**. The [Trap Settings Page](#) is displayed.

**Figure 227: Trap Settings Page**



The screenshot shows a configuration interface with two rows of settings. The first row is labeled 'SNMP Notifications' and has a dropdown menu set to 'Enable'. The second row is labeled 'Authentication Notifications' and also has a dropdown menu set to 'Enable'. In the bottom right corner of the form, there are two buttons: 'Apply' and 'Cancel'.

2. Select **Enable** for **SNMP Notifications** to specify that the switch can send SNMP notifications.
3. Select **Enable** for **Authentication Notifications** to enable SNMP authentication failure notification.
4. Click **Apply**. The SNMP Trap settings are defined, and the Running Configuration file is updated with the settings.

## DEFINING NOTIFICATION RECIPIENTS

Trap messages are generated to report system events, as defined in RFC 1215. The system can generate traps defined in the MIB that it supports.

Trap receivers (aka Notification Recipients) are network nodes where the trap messages are sent by the switch. A list of trap receivers is defined as the targets of trap messages.

A trap receiver entry contains the IP address of the node and the SNMP credentials corresponding to the version that will be included in the trap message. When an event arises that requires a trap message to be sent, it is sent to every node listed in the trap receiver list.

The [SNMPv1,2 Notification Recipient Page](#) and the [SNMPv3 Notification Recipient Page](#) enable configuring the destination to which SNMP notifications are sent, and the types of SNMP notifications that are sent to each destination (traps or informs). The *Add/Edit* pop-ups enable configuring the attributes of the notifications.

An SNMP notification is a message sent from the switch to the SNMP management station indicating that a certain event has occurred, such as a link up/down.

It is also possible to filter certain notifications. This can be done by creating a filter in the [Notification Filter Page](#) and attaching it to an SNMP notification recipient. The notification filter enables filtering the type of SNMP notifications that are sent to the management station based on the OID of the notification that is about to be sent.

### DEFINING SNMPv1,2 NOTIFICATION RECIPIENTS

To define a recipient in SNMPv1,2:

1. Click **SNMP** > **Notification Recipient SNMPv1,2**. The [SNMPv1,2 Notification Recipient Page](#) is displayed.

**Figure 228: SNMPv1,2 Notification Recipient Page**

Notification Recipient Table									
<input type="checkbox"/>	Recipients IP	UDP Port	Community String	Notification Type	Notification Version	Filter Name	Timeout	Retries	
Table is empty									
							Add...	Edit...	Delete

This page displays recipients for SNMPv1,2.

2. Click **Add**. The [Add SNMP Notification Recipient Page](#) is displayed.

Figure 229: Add SNMP Notification Recipient Page

IP Version	<input type="radio"/> Version 6 <input checked="" type="radio"/> Version 4
IPv6 Address Type	<input type="radio"/> Link Local <input checked="" type="radio"/> Global
Link Local Interface	None
Recipient IP Address *	
UDP Port *	162 (1 - 65535, Default: 162)
Community String *	
Notification Type	Traps
Notification Version	SNMPv1
Notification Filter	Disabled
Filter Name	
Timeout *	15 sec. (1 - 300, Default: 15)
Retries *	3 (0 - 255, Default: 3)

Apply

3. Enter the parameters.

- **IP Version**—Select either IPv4 or IPv6.
- **IPv6 Address Type**—Select either *Link Local* or *Global*.
  - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **Link Local Interface**—If the IPv6 address type is Link Local, select whether it is received through VLAN2 or ISATAP.
- **Recipient IP Address**—Enter the IP address of where the traps are sent.
- **UDP Port**—Enter the UDP port used for notifications on the recipient device. Range 1-65535, default 162
- **Community String**—Enter the community string of the trap manager.
- **Notification Type**—Select whether to send traps or informs. If both are required, two recipients must be created.
- **Notification Version**—Select the trap SNMP version.
- Either SNMPv1 or SNMPv2 may be used as the version of traps, with only a single version enabled at a single time.

- **Notification Filter**—Select to enable filtering the type of SNMP notifications sent to the management station. The filters are created in the [Notification Filter Page](#).
  - **Filter Name**—Select the SNMP filter that defines the information contained in traps (defined in the [Notification Filter Page](#)).
  - **(Inform) Timeout**—Enter the number of seconds the device waits before re-sending informs. Timeout range: 1-300, default: 15.
  - **(Inform) Retries**—Enter the number of times that the device resends an inform request. Retries range:0-255, default: 3
4. Click **Apply**. The SNMP Notification Recipient settings are defined, and the Running Configuration file is updated with the settings.

## DEFINING SNMPv3 NOTIFICATION RECIPIENTS

To define a recipient in SNMPv3:

1. Click **SNMP > Notification Recipient SNMPv3**. The [SNMPv3 Notification Recipient Page](#) is displayed.

**Figure 230: SNMPv3 Notification Recipient Page**

Notification Recipient Table									
<input type="checkbox"/>	Recipients IP	UDP Port	User Name	Security Level	Notification Type	Filter Name	Timeout	Retries	
Table is empty									
							Add...	Edit...	Delete

This page displays recipients for SNMPv3.

2. Click **Add**. The [Add SNMP Notification Recipient Page](#) is displayed.

**Figure 231: Add SNMP Notification Recipient Page**

**IP Version**  Version 6  Version 4  
**IPv6 Address Type**  Link Local  Global  
**Link Local Interface**   
**Recipient IP Address \***   
**UDP Port \***  (1 - 65535, Default: 162)  
**User Name \***   
**Security Level**   
**Notification Type**   
**Notification Filter**   
**Filter Name**   
**Timeout \***  sec. (1 - 300, Default: 15)  
**Retries \***  (0 - 255, Default: 3)

3. Enter the parameters.
  - **IP Version**—Select either IPv4 or IPv6.
  - **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:
    - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
    - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
  - **Link Local Interface**—Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
  - **Recipient IP Address**—Enter the IP address of where the traps are sent.
  - **UDP Port**—Enter the UDP port used to for notifications on the recipient device. Range 1-65535, default 162
  - **User Name**—Enter the user to whom SNMP notifications are sent.
  - **Security Level**—Select how much authentication is applied to the packet. The options are:
    - *No Authentication*—Indicates the packet is neither authenticated nor encrypted.
    - *Authentication*—Indicates the packet is authenticated but not encrypted.
    - *Privacy*—Indicates the packet is both authenticated and encrypted.
  - **Notification Type**—Select whether to send traps or informs. If both are required, two recipients must be created.
  - **Notification Filter**—Select to enable filtering the type of SNMP notifications sent to the management station. The filters are created in the [Notification Filter Page](#).
  - **Filter Name**—Select the SNMP filter that defines the information contained in traps (defined in the [Notification Filter Page](#)).
  - **(Inform) Timeout**—Enter the amount of time (seconds) the device waits before re-sending informs/traps. Timeout: Range 1-300, default 15

- **(Inform) Retries**—Enter the number of times that the device resends an inform request. Retries: Range 0-255, default 3
4. Click **Apply**. The SNMP Notification Recipient settings are defined, and the Running Configuration file is updated with the settings.

## CONFIGURING SNMP NOTIFICATION FILTERS

The [Notification Filter Page](#) enables configuring SNMP notification filters and Object IDs (OIDs) that are checked. After creating a notification filter, it is possible to attach it to a notification recipient in the [SNMPv1,2 Notification Recipient Page](#), and [SNMPv3 Notification Recipient Page](#).

The notification filter enables filtering the type of SNMP notifications that are sent to the management station based on the OID of the notification to be sent.

To define a notification filter:

1. Click **SNMP > Notification Filter**. The [Notification Filter Page](#) is displayed.

**Figure 232: Notification Filter Page**



The [Notification Filter Page](#) displays notification information for each filter. You can filter notification entries by **Filter Name**.

2. Click **Add**. The [Add Notification Filter Page](#) is displayed.

**Figure 233: Add Notification Filter Page**



3. Enter the parameters.
  - **Filter Name**—Enter a name.
  - **Object ID Subtree**—Select the node in the MIB tree that is included or excluded in the selected SNMP view. The options are:
    - *Select from List*—Enables you to navigate the MIB tree. Click *Up* to go to the level of the selected node's father and siblings. Click *Down* to descend to the level of the selected node's descendents. Click the nodes in the view to pass from one node to its brother. Use the scrollbar to bring siblings into view.
    - *Object ID*—Enter an OID not offered in the *Select from List* option (if required). All descendents of this node are included or excluded in the view.
    - If *Select from list* is used, the object identifier of the selected node is included in or excluded from the view if the **Include in filter option** is selected.
    - If *Object ID* is used, the entered object identifier is included in or excluded from the view if the **Include in filter option** is selected.
  - **Include in filter**—If you used *Select from list*, the object identifier of the selected node is included in or excluded from the notification filter if the **Include in filter** option is selected. If you used **Object ID**, the entered object identifier is included in or excluded from the notification filter if the **Include in filter option** is selected. This means that the node and its descendents are included or excluded from the notification filter.
4. Click **Apply**. The SNMP views are defined, and the Running Configuration file is updated with the settings.

# 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 CLI Interface" on page 369](#)
- ◆ ["User Interface Commands" on page 375](#)
- ◆ ["System Management Commands" on page 391](#)
- ◆ ["Clock Commands" on page 411](#)
- ◆ ["Configuration and Image File Commands" on page 426](#)
- ◆ ["Auto-Update and Auto-Configuration" on page 435](#)
- ◆ ["Management ACL Commands" on page 439](#)
- ◆ ["Network Management Protocol \(SNMP\) Commands" on page 444](#)
- ◆ ["RSA and Certificate Commands" on page 462](#)
- ◆ ["Web Server Commands" on page 471](#)
- ◆ ["Telnet, Secure Shell \(SSH\), and Secure Login \(Slogin\) Commands" on page 476](#)
- ◆ ["Line Commands" on page 483](#)
- ◆ ["AAA Commands" on page 487](#)
- ◆ ["RADIUS Commands" on page 500](#)
- ◆ ["TACACS+ Commands" on page 507](#)
- ◆ ["Syslog Commands" on page 512](#)
- ◆ ["Remote Network Monitoring \(RMON\) Commands" on page 521](#)

- ◆ "802.1x Commands" on page 534
- ◆ "Ethernet Configuration Commands" on page 553
- ◆ "PHY Diagnostics Commands" on page 568
- ◆ "Port Channel Commands" on page 570
- ◆ "Address Table Commands" on page 573
- ◆ "Port Monitor Commands" on page 601
- ◆ "sFlow Commands" on page 605
- ◆ "Link Layer Discovery Protocol (LLDP) Commands" on page 609
- ◆ "Spanning-Tree Commands" on page 631
- ◆ "Virtual Local Area Network (VLAN) Commands" on page 661
- ◆ "Virtual Local Area Network (VLAN) NON-ISCLI Commands" on page 681
- ◆ "IGMP Snooping Commands" on page 686
- ◆ "IPv6 MLD Snooping Commands" on page 698
- ◆ "Link Aggregation Control Protocol (LACP) Commands" on page 709
- ◆ "GARP VLAN Registration Protocol (GVRP) Commands" on page 713
- ◆ "DHCP Snooping and ARP Inspection Commands" on page 720
- ◆ "IP Addressing Commands" on page 737
- ◆ "IPv6 Addressing Commands" on page 753
- ◆ "IP Routing Protocol-Independent Commands" on page 769
- ◆ "Tunnel Commands" on page 772
- ◆ "ACL Commands" on page 778
- ◆ "Quality of Service (QoS) Commands" on page 794
- ◆ "Data Center Ethernet Commands" on page 829

The CLI commands described in this document are organized according to feature groups in separate sections.

This section describes how to use the CLI. It contains the following topics:

- ◆ [CLI Command Modes](#)
- ◆ [Starting the CLI](#)
- ◆ [CLI Command Conventions](#)
- ◆ [Entering Commands](#)

---

## CLI COMMAND MODES

To configure devices, the CLI is divided into various command modes. Each command mode has its own set of specific commands. Entering a question mark "?" at the console prompt displays a list of commands available for that particular command mode.

A specific command, which varies from mode to mode, is used to navigate from one mode to another. The standard order to access the modes is as follows: *User EXEC mode*, *Privileged EXEC mode*, *Global Configuration mode*, and *Interface Configuration modes*.

When starting a session, the initial mode for non-privileged users is the User EXEC mode. Only a limited subset of commands is available in the User EXEC mode. This level is reserved for tasks that do not change the configuration.

Privileged users enter the Privileged EXEC mode directly using a password. This mode provides access to the device Configuration modes.

The modes are described below.

**USER EXEC MODE** After logging into the device, the user is automatically in *User EXEC* command mode unless the user is defined as a privileged user. In general, the *User EXEC* commands enable the user to perform basic tests, and display system information.

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

```
console>
```

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

---

## PRIVILEGED EXEC MODE

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

Privileged users enter directly into the *Privileged EXEC* mode.

Use **disable** to return to the *User EXEC* mode.

---

## GLOBAL CONFIGURATION MODE

*Global Configuration* mode commands apply to features that affect the system as a whole, rather than just a specific interface.

To enter the *Global Configuration* mode, enter **configure** in the Privileged EXEC mode, and press <Enter>.

The *Global Configuration* mode prompt is displayed.

```
console(config)#
```

Use **exit**, **end** or **ctrl/z** to return to the Privileged EXEC mode.

---

## INTERFACE CONFIGURATION MODES

Commands in the following modes perform specific interface operations:

- ◆ **Line Interface** — Contains commands to configure the management connections. These include commands such as line speed, timeout settings, etc. The *Global Configuration* mode command **line** is used to enter the *Line Configuration command* mode.
- ◆ **VLAN Database** — Contains commands to create a VLAN as a whole. The *Global Configuration* mode command **vlan database** is used to enter the *VLAN Database Interface Configuration* mode.

- ◆ **Management Access List** — Contains commands to define management access-lists. The *Global Configuration* mode command `management access-list` is used to enter the *Management Access List Configuration* mode.
- ◆ **Port Channel** — Contains commands to configure port-channels, for example, assigning ports to a VLAN or port-channel. The *Global Configuration* mode command `interface port-channel` is used to enter the *Port Channel Interface Configuration* mode.
- ◆ **SSH Public Key-Chain** — Contains commands to manually specify other device SSH public keys. The *Global Configuration* mode command `crypto key pubkey-chain ssh` is used to enter the *SSH Public Key-chain Configuration* mode.
- ◆ **Interface** — Contains commands that configure the interface. The *Global Configuration* mode command `interface` is used to enter the *Interface Configuration* mode.

---

## STARTING THE CLI

The switch can be managed over a direct connection to the switch console port, or via a Telnet connection. The switch is managed by entering command keywords and parameters at the prompt. Using the switch CLI commands is similar to entering commands on a UNIX system.

If access is via a Telnet connection, ensure the device has an IP address defined, corresponding management access is granted, and the workstation used to access the device is connected to the device prior to using CLI commands.

### ACCESSING THE CLI FROM THE CONSOLE LINE

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

### ACCESSING THE CLI FROM TELNET

1. Enter **telnet** and the IP address of the device. A User Name prompt is displayed.
2. Enter the User Name and Password. You are in the Privileged Exec mode.
3. Configure the device and enter the necessary commands to complete the required tasks.

4. When finished, exit the session with the quit or exit command.

When another user is required to log onto the system, the **login** command is entered in the Privileged EXEC command mode,. This effectively logs off the current user and logs on the new user.

---

## CLI COMMAND CONVENTIONS

The following table describes the command syntax conventions.

**Table 6: CLI Conventions**

Conventions	Description
[ ]	In a command line, square brackets indicates an optional entry.
{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated by the   character. One option must be selected. For example: <b>flowcontrol {auto on off}</b> means that for the <b>flowcontrol</b> command either <b>auto</b> , <b>on</b> or <b>off</b> must be selected.
<i>Italic font</i>	Indicates a parameter.
<Enter>	Any individual key on the keyboard. For example click <Enter>.
Ctrl+F4	Any combination keys pressed simultaneously on the keyboard.
Screen Display	Indicates system messages and prompts appearing on the console.
all	When a parameter is required to define a range of ports or parameters and <b>all</b> is an option, the default for the command is <b>all</b> when no parameters are defined. For example, the command <b>interface range port-channel</b> has the option of either entering a range of channels, or selecting <b>all</b> . When the command is entered without a parameter, it automatically defaults to <b>all</b> .

---

## ENTERING COMMANDS

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "**show interfaces status gi1/0/5**" **show**, **interfaces** and **status** are keywords, **gi** is an argument that specifies the interface type, and **1/0/5** is an argument that specifies the port.

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 smith
```

Help information can be displayed in the following ways:

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

The following describes features that assist in using the CLI:

---

## TERMINAL COMMAND BUFFER

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a First In First Out (FIFO) basis. These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets. The keys that can be used to access the history buffer are described in [Table 7](#).

By default, the history buffer system is enabled, but it can be disabled at any time. For information about the command syntax to enable or disable the history buffer, see the **history** command.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 256. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command syntax for configuring the command history buffer, see the **history size** command.

To display the history buffer, see **show history** command.

## NEGATING THE EFFECT OF COMMANDS

For many configuration commands, the prefix keyword "no" can be entered to cancel the effect of a command or reset the configuration to the default value. This guide describes the negation effect for all applicable commands.

## COMMAND COMPLETION

If the command entered is incomplete, invalid, or has missing or invalid parameters, an appropriate error message is displayed.

To complete an incomplete command, press the <Tab> button. If the characters already entered are not enough for the system to identify a single matching command, press "?" to display the available commands matching the characters already entered.

Incorrect or incomplete commands are automatically re-entered next to the cursor. If a parameter must be added, the parameter can be added to the basic command already displayed next to the cursor. The following

example indicates that the command interface requires a missing parameter.

```
(config)#interface
%missing mandatory parameter
(config)#interface
```

## KEYBOARD SHORTCUTS

The CLI has a range of keyboard shortcuts to assist in entering the CLI commands.

The following table describes these shortcuts:

**Table 7: Keyboard Keys**

Keyboard Key	Description
Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow key	Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any mode.
Backspace key	Moves the cursor back one space.
Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.

**enable** The **enable** EXEC mode command enters the Privileged EXEC mode.

#### SYNTAX

**enable** [*privilege-level*]

#### PARAMETERS

**privilege-level**—Specifies the privilege level at which to enter the system.  
(Range: 1–15)

#### DEFAULT CONFIGURATION

The default privilege level is 15.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example enters the Privileged EXEC mode.

```
Console> enable
enter password:
Console#
```

**disable** The **disable** Privileged EXEC mode command leaves the Privileged EXEC mode and returns to the User EXEC mode.

#### SYNTAX

**disable** [*privilege-level*]

#### PARAMETERS

**privilege-level**—Specifies the privilege level at which to enter the system.  
(Range: 1–15)

#### DEFAULT CONFIGURATION

The default privilege level is 1.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example returns to the User EXEC mode.

```
Console# disable
Console>
```

**login** The **login** EXEC mode command changes a user's login.

#### SYNTAX

**login**

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example enters Privileged EXEC mode and logs in with username 'admin'.

```
Console> login
User Name:admin
Password:*****
Console#
```

**configure** The **configure** Privileged EXEC mode command enters the Global Configuration mode.

#### SYNTAX

**configure** [*terminal*]

#### PARAMETERS

**terminal**—Enter the Global Configuration mode with or without the keyword terminal.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example enters Global Configuration mode.

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

**exit (Configuration)** The **exit** command exits any configuration mode to the next highest mode in the CLI mode hierarchy.

#### SYNTAX

**exit**

#### COMMAND MODE

All commands in configuration modes.

#### EXAMPLES

The following examples change the configuration mode from Interface Configuration mode to Privileged EXEC mode.

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

```
Router(config-if)# exit
Router(config)# exit
Router#
```

**exit (EXEC)** The **exit** EXEC mode command closes an active terminal session by logging off the device.

#### SYNTAX

**exit**

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following examples close an active terminal session.

```
Console> exit
```

```
Router> exit
```

**end** The **end** command ends the current configuration session and returns to the Privileged EXEC mode.

#### SYNTAX

**end**

**COMMAND MODE**

All configuration modes

**EXAMPLE**

The following examples end the Global Configuration mode session and return to the Privileged EXEC mode.

```
Console(config)# end
Console#
```

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

**help** The **help** command displays a brief description of the Help system.

**SYNTAX**

**help**

**COMMAND MODE**

All command modes

**EXAMPLE**

The following example describes the Help system.

```
Console# help
Help may be requested at any point in a command by entering a question mark
'?' . If nothing matches the currently entered incomplete command, the help
list is empty. This indicates that there is no command matching the input as
it currently appears. If the request is within a command, press the
Backspace key and erase the entered characters to a point where the request
results in a match.
Help is provided when:
1. There is a valid command and a help request is made for entering a
parameter or argument (e.g. 'show ?'). All possible parameters or arguments
for the entered command are then displayed.
2. An abbreviated argument is entered and a help request is made for arguments
matching the input (e.g. 'show pr?').
```

**history** The **history** Line Configuration mode command enables the command history function. Use the **no** form of this command to disable the command history function.

**SYNTAX**

**history**

**no history**

**DEFAULT CONFIGURATION**

The history command is enabled.

**COMMAND MODE**

Line Configuration mode

**USER GUIDELINES**

This command enables the command history function for a specified line. Use the **terminal history** EXEC mode command to enable or disable the command history function for the current terminal session.

**EXAMPLE**

The following example enables the command history function for Telnet.

```
Console(config)# line telnet
Console(config-line)# history
```

**history size** The **history size** Line Configuration mode command changes the command history buffer size for a particular line. Use the **no** form of this command to reset the command history buffer size to the default value.

**SYNTAX**

**history size** *number-of-commands*

**no history size**

**PARAMETERS**

**number-of-commands**—Specifies the number of commands the system records in its history buffer. (Range: 0–256)

**DEFAULT CONFIGURATION**

The default command history buffer size is 10 commands.

**COMMAND MODE**

Line Configuration mode

**USER GUIDELINES**

This command configures the command history buffer size for a particular line. Use the **terminal history size** EXEC mode command to configure the command history buffer size for the current terminal session.

The allocated command history buffer is per terminal user, and is taken from a shared buffer. If there is not enough space available in the shared buffer, the command history buffer size ( ) cannot be increased above the default size.

**EXAMPLE**

The following example changes the command history buffer size to 100 entries for a particular line

```
Console(config)# line telnet
Console(config-line)# history size 100
```

**terminal history** The **terminal history** EXEC mode command enables the command history function for the current terminal session. Use the **no** form of this command to disable the command history function.

**SYNTAX**

**terminal history**

**terminal no history**

**DEFAULT CONFIGURATION**

The default configuration for all terminal sessions is defined by the **history** Line Configuration mode command.

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

The command enables the command history for the current session. The default is determined by the **history** Line Configuration mode command.

**EXAMPLE**

The following example disables the command history function for the current terminal session.

```
Console> terminal no history
```

**terminal history size** The **terminal history size** EXEC mode command changes the command history buffer size for the current terminal session. Use the **no** form of this command to reset the command history buffer size to the default value.

**SYNTAX**

**terminal history size** *number-of-commands*

**terminal no history size**

**PARAMETERS**

**number-of-commands**—Specifies the number of commands the system maintains in its history buffer. (Range: 10–256)

**DEFAULT CONFIGURATION**

The default configuration for all terminal sessions is defined by the **history size** Line Configuration mode command.

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

The **terminal history size** EXEC command changes the command history buffer size for the current terminal session. Use the **history** Line Configuration mode command to change the default command history buffer size.

The maximum number of commands in all buffers is 256.

**EXAMPLE**

The following example sets the command history buffer size to 20 commands for the current terminal session.

```
Console> terminal history size 20
```

**terminal datadump** The **terminal datadump** EXEC mode command enables dumping all the output of a show command without prompting. Use the **no** form of this command to disable dumping.

**SYNTAX**

**terminal datadump**

**terminal no datadump**

**DEFAULT CONFIGURATION**

Dumping is disabled.

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

By default, a **More** prompt is displayed when the output contains more lines than can be displayed on the screen. Pressing the **Enter** key displays the next line; pressing the **Spacebar** displays the next screen of output. The **terminal datadump** command enables dumping all output immediately after entering the show command.

This command is relevant only for the current session.

**EXAMPLE**

The following example dumps all output immediately after entering a show command.

```
Console> terminal datadump
```

**debug-mode** The **debug-mode** Privileged EXEC mode command mode switches to debug mode.

**SYNTAX**

**debug-mode**

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example enters Debug mode.

```
Console# debug-mode
```

**show history** The **show history** EXEC mode command lists commands entered in the current session.

**SYNTAX**

**show history**

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

The buffer includes executed and unexecuted commands.

Commands are listed from the first to the most recent command.

The buffer remains unchanged when entering into and returning from configuration modes.

**EXAMPLE**

The following example displays all the commands entered while in the current Privileged EXEC mode.

```
Console# show version
SW version 3.131 (date 23-Jul-2005 time 17:34:19)
HW version 1.0.0
```

```

Console# show clock
15:29:03 Jun 17 2005
Console# show history
show version
show clock
show history
3 commands were logged (buffer size is 10)

```

**show privilege** The **show privilege** EXEC mode command displays the current privilege level.

#### SYNTAX

**show privilege**

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the current privilege level for the Privileged EXEC mode.

```

Console# show privilege
Current privilege level is 15

```

**do** The **do** command executes an EXEC-level command from Global Configuration mode or any configuration submode.

#### SYNTAX

**do** *command*

#### PARAMETERS

**command**—Specifies the EXEC-level command to execute.

#### COMMAND MODE

All configuration modes

#### EXAMPLE

The following example executes the **show vlan** Privileged EXEC mode command from Global Configuration mode.

#### EXAMPLE

```

Console (Config)# do show vlan

```

Vlan	Name	Ports	Type	Authorization
1	1	te1-39, Po1, Po2, Po3, Po4, Po5, Po6, Po7, Po8	other	Required
2	2	tel	dynamicGvrp	Required

```

10 v0010 tel permanent Not Required
11 V0011 tel,te13 permanent Required
20 20 tel permanent Required
30 30 tel,te13 permanent Required
31 31 tel permanent Required
91 91 tel,te40 permanent Required
4093 guest-vlan tel,te13 permanent Guest
console(config)#s

```

**banner exec** Use the **banner exec** command to specify and enable a message to be displayed when an EXEC process is created (The user has successfully logged in), use the banner exec command in Global Configuration mode. Use the **no** form of this command to delete the existing EXEC banner.

#### SYNTAX

**banner exec** *d* *message-text* *d*

**no banner exec**

#### PARAMETERS

- ◆ **d**—Delimiting character of your choice—a pound sign (**#**), for example. You cannot use the delimiting character in the banner message.
- ◆ **message-text**—The message must start in a new line. You can enter multi-line messages. You can include tokens in the form of **\$(token)** in the message text. Tokens are replaced with the corresponding configuration variable. Tokens are described in the User Guidelines. The message can contain up to 2000 characters (after every 510 characters, you must press <Enter> to continue).

#### DEFAULT CONFIGURATION

Disabled (no EXEC banner is displayed).

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to a device, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the device, the EXEC banner is displayed.

Use tokens in the form of **\$(token)** in the message text to customize the banner. The tokens are described in the table below:

Token	Information displayed in the banner
\$(hostname)	Displays the host name for the device.
\$(domain)	Displays the domain name for the device.

\$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
\$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
\$(contact)	Displays the system contact string.
\$(location)	Displays the system location string.
\$(mac-address)	Displays the base MAC address of the device.

Use the `no exec-banner` line configuration command to disable the EXEC banner on a particular line or lines.

#### EXAMPLE

The following example sets an EXEC banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the **\$(token)** syntax is replaced by the corresponding configuration variable.

```
Device(config)# banner exec %
Enter TEXT message. End with the character '%'.
$(bold)Session activated.$(bold) Enter commands at the prompt.
%
When a user logs on to the system, the following output is displayed:
Session activated. Enter commands at the prompt.
```

**banner login** Use the **banner login** command in Global Configuration mode to specify and enable a message to be displayed before the username and password login prompts. Use the **no** form of this command to delete the existing Login banner.

#### SYNTAX

```
banner login d message-text d
no banner login
```

#### PARAMETERS

- ◆ **Delimiting character of your choice**—A pound sign (#), for example. You cannot use the delimiting character in the banner message.
- ◆ **message-text**—Message text. The message must start on a new line. You can enter multi-line messages. You can include tokens in the form of **\$(token)** in the message text. Tokens are replaced with the corresponding configuration variable. Tokens are described in the User Guidelines. The message can contain up to 2000 characters (after every 510 characters, you must press <Enter> to continue).

#### DEFAULT CONFIGURATION

Disabled (no Login banner is displayed).

#### COMMAND MODE

Global Configuration mode

**USER GUIDELINES**

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to a device, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the device, the EXEC banner is displayed.

Use tokens in the form of **\$(token)** in the message text to customize the banner. The tokens are described in the table below:

Token	Information displayed in the banner
\$(hostname)	Displays the host name for the device.
\$(domain)	Displays the domain name for the device.
\$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
\$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
\$(contact)	Displays the system contact string.
\$(location)	Displays the system location string.
\$(mac-address)	Displays the base MAC address of the device.

Use the **no login-banner** line configuration command to disable the Login banner on a particular line or lines.

**EXAMPLE**

The following example sets a Login banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the **\$(token)** syntax is replaced by the corresponding configuration variable.

```
Device(config)# banner login %
Enter TEXT message. End with the character '%'.
You have entered $(hostname).$(domain)
%
When the login banner is executed, the user will see the following banner:
You have entered host123.ourdomain.com
```

**banner motd** Use the **banner motd** command in Global Configuration mode to specify and enable a message-of-the-day banner. Use the **no** form of this command to delete the existing MOTD banner.

**SYNTAX**

```
banner motd d message-text d
no banner motd
```

**PARAMETERS**

- ◆ **d**—Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.

- ◆ **message-text**—The message must start on a new line. You can enter multi-line messages. You can include tokens in the form of **\$(token)** in the message text. Tokens are replaced with the corresponding configuration variable. Tokens are described in the User Guidelines. The message can contain up to 2000 characters (after every 510 characters, you must press <Enter> to continue).

#### DEFAULT CONFIGURATION

Disabled (no MOTD banner is displayed).

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to a device, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the device, the EXEC banner is displayed.

Use tokens in the form of **\$(token)** in the message text to customize the banner. The tokens are described in the table below:

Token	Information displayed in the banner
\$(hostname)	Displays the host name for the device.
\$(domain)	Displays the domain name for the device.
\$(bold)	Indicates that the next text is a bold text. Using this token again to indicates the end of the bold text.
\$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
\$(contact)	Displays the system contact string.
\$(location)	Displays the system location string.
\$(mac-address)	Displays the base MAC address of the device.

Use the **no motd-banner** line configuration command to disable the MOTD banner on a particular line or lines.

#### EXAMPLE

The following example sets an MOTD banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the **\$(token)** syntax is replaced by the corresponding configuration variable.

```
Device(config)# banner motd %
Enter TEXT message. End with the character '%'.
$(bold)Upgrade$(bold) to all devices begins at March 12
%
When the login banner is executed, the user will see the following banner:
Upgrade to all devices begins at March 12
```

**exec-banner** Use the **exec-banner** command in Line Configuration mode to enable the display of exec banners. Use the **no** form of this command to disable the display of exec banners.

#### SYNTAX

```
exec-banner
no exec-banner
```

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT CONFIGURATION

Disabled

#### COMMAND MODE

Line Configuration mode

#### EXAMPLE

```
console# configure
console(config)# line console
console(config-line)# exec-banner
console(config-line)# exit
console(config)# line telnet
console(config-line)# exec-banner
console(config-line)# exit
console(config)# line ssh
console(config-line)# exec-banner
```

**login-banner** Use the **login-banner** command in Line Configuration mode to enable the display of login banners. Use the **no** form of this command to disable the display of login banners.

#### SYNTAX

```
login-banner
no login-banner
```

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT CONFIGURATION

Enabled

#### COMMAND MODE

Line Configuration mode

**EXAMPLE**

```

console# configure
console(config)# line console
console(config-line)# login-banner
console(config-line)# exit
console(config)# line telnet
console(config-line)# login-banner
console(config-line)# exit
console(config)# line ssh
console(config-line)# login-banner

```

**motd-banner** Use the **motd-banner** command in Line Configuration mode to enable the display of message-of-the-day banners. Use the **no** form of this command to disable the display of MOTD banners.

**SYNTAX**

**motd-banner**  
**no motd-banner**

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

Enabled

**COMMAND MODE**

Line Configuration mode

**EXAMPLE**

```

console# configure
console(config)# line console
console(config-line)# motd-banner
console(config-line)# exit
console(config)# line telnet
console(config-line)# motd-banner
console(config-line)# exit
console(config)# line ssh
console(config-line)# motd-banner

```

**show banner** Use the **show banner** command in EXEC mode to display the configuration of banners.

**SYNTAX**

**show banner motd**  
**show banner login**  
**show banner exec**

**PARAMETERS**

This command has no arguments or keywords.

**COMMAND MODE**

EXEC mode

**EXAMPLES**

```
Device> show banner motd
Banner: MOTD
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
10000 giga ports switch

console#
console# show banner login
-----
Banner: Login
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled

console#
console# show banner exec
```

```
Banner: EXEC
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
dsadsa

console#
```

**ping** Use the **ping** command to send ICMP echo request packets to another node on the network.

#### SYNTAX

```
ping [ip] {ipv4-address | hostname} [size packet_size] [count  
packet_count] [timeout time_out]
```

```
ping ipv6 {ipv6-address | hostname} [size packet_size] [count  
packet_count] [timeout time_out]
```

#### PARAMETERS

- ◆ **ip**—Use IPv4 to check the network connectivity.
- ◆ **ipv6**—Use IPv6 to check the network connectivity.
- ◆ **ipv4-address**—IPv4 address to ping.
- ◆ **ipv6-address**—Unicast or multicast IPv6 address to ping. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.
- ◆ **hostname**—Hostname to ping (160 characters. Maximum label size: 63.)
- ◆ **packet\_size**—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64-1518, IPv6: 68-1518)
- ◆ **packet\_count**—Number of packets to send, from 1 to 65535 packets. The default is 4 packets. If 0 is entered, it pings until stopped (0–65535).
- ◆ **time-out**—Timeout in milliseconds to wait for each reply, from 50 to 65535 milliseconds. The default is 2000 milliseconds (50–65535).

#### COMMAND MODE

EXEC mode

#### USER GUIDELINES

Press **Esc** to stop pinging. Following are sample results of the ping command:

- ◆ **Destination does not respond**—If the host does not respond, a “no answer from host” appears within 10 seconds.

- ◆ **Destination unreachable**—The gateway for this destination indicates that the destination is unreachable.
- ◆ **Network or host unreachable**—The switch found no corresponding entry in the route table.

The format of an **IPv6Z** address is: `<ipv6-link-local-address>%<interface-name>`

- ◆ **interface-name** = `vlan<integer>` | `ch<integer>` | `isatap<integer>` | `<physical-port-name>` | `0`
- ◆ **integer** = `<decimal-number>` | `<integer><decimal-number>`
- ◆ **decimal-number** = `0` | `1` | `2` | `3` | `4` | `5` | `6` | `7` | `8` | `9`
- ◆ **physical-port-name** = Designated port number, for example `te1`

When using the ping **ipv6** command to check network connectivity of a directly attached host using its link local address, the egress interface may be specified in the **IPv6Z** format. If the egress interface is not specified, the default interface is selected. Specifying `interface zone=0` is equivalent to not defining an egress interface.

When using the ping **ipv6** command with MC address, the information displayed is taken from all received echo responses.

## EXAMPLES

```

Console> ping ip 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:

64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11

Console> ping ip yahoo.com
Pinging yahoo.com [66.218.71.198] with 64 bytes of data:

64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11

Console> ping ip oob/176.16.1.1
Pinging oob/176.16.1.1 with 64 bytes of data:

64 bytes from oob/176.16.1.1: icmp_seq=0. time=5 ms
64 bytes from oob/176.16.1.1: icmp_seq=1. time=5 ms
64 bytes from oob/176.16.1.1: icmp_seq=2. time=5 ms
64 bytes from oob/176.16.1.1: icmp_seq=3. time=5 ms

```

```

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 5/5/5

console> ping ipv6 3003::11
Pinging 3003::11 with 64 bytes of data:

64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::11: icmp_seq=2. time=50 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
64 bytes from 3003::11: icmp_seq=4. time=0 ms

----3003::11 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/12/50

console> ping ipv6 FF02::1
Pinging FF02::1 with 64 bytes of data:

64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::33: icmp_seq=1. time=70 ms
64 bytes from 3003::11: icmp_seq=2. time=0 ms
64 bytes from 3003::55: icmp_seq=1. time=1050 ms
64 bytes from 3003::33: icmp_seq=2. time=70 ms
64 bytes from 3003::55: icmp_seq=2. time=1050 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
64 bytes from 3003::33: icmp_seq=3. time=70 ms
64 bytes from 3003::11: icmp_seq=4. time=0 ms
64 bytes from 3003::55: icmp_seq=3. time=1050 ms
64 bytes from 3003::33: icmp_seq=4. time=70 ms
64 bytes from 3003::55: icmp_sq=4. time=1050 ms

---- FF02::1 PING Statistics----
4 packets transmitted, 12 packets received

```

**traceroute** To discover (?) the routes that packets will take when traveling to their destination, use the **traceroute** EXEC command.

#### SYNTAX

```
traceroute ip {ipv4-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address] [tos tos]
```

```
traceroute ipv6 {ipv6-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address] [tos tos]
```

#### PARAMETERS

- ◆ **ip**—Use IPv4 to discover the route.
- ◆ **ipv6**—Use IPv6 to discover the route.
- ◆ **ipv4-address**—IPv4 address of the destination host. (Range: Valid IP address)
- ◆ **ipv6-address**—IPv6 address of the destination host.

- ◆ **hostname**—Hostname of the destination host. (Range: 1–160 characters. Maximum label size: 63.)
- ◆ **packet\_size**—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64-1518, IPv6: 68-1518)
- ◆ **tll max-ttl**—The largest TTL value that can be used. The default is 30. The **traceroute** command terminates when the destination is reached or when this value is reached. (Range: 1–255)
- ◆ **count packet\_count**—The number of probes to be sent at each TTL level. The default count is 3. (Range: 1–10)
- ◆ **timeout time\_out**—The number of seconds to wait for a response to a probe packet. The default is 3 seconds. (Range: 1–60)
- ◆ **source ip-address**—One of the interface addresses of the device to use as a source address for the probes. The device will normally pick what it feels is the best source address to use. (Range: Valid IP address)
- ◆ **tos tos**—The Type-Of-Service byte in the IP Header of the packet.(Range: 0–255)

#### COMMAND MODE

EXEC mode

#### USER GUIDELINES

The traceroute command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The traceroute command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The traceroute command sends several probes at each TTL level and displays the round-trip time for each.

The traceroute command sends out one probe at a time. Each outgoing packet can result in one or two error messages. A "time exceeded" error message indicates that an intermediate router has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the traceroute command prints an asterisk (\*).

The traceroute command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with Esc.

The traceroute command is not relevant to IPv6 link local addresses.

**EXAMPLE**

```

Router> traceroute ip umaxpl.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxpl.physics.lsa.umich.edu (141.211.101.64)
 0  i2-gateway.stanford.edu (192.68.191.83)  0 msec 0 msec 0 msec
 1  STAN.POS.calren2.NET (171.64.1.213)  0 msec 0 msec 0 msec
 2  SUNV--STAN.POS.calren2.net (198.32.249.73)  1 msec 1 msec 1 msec
 3  Abilene--QSV.POS.calren2.net (198.32.249.162)  1 msec 1 msec 1 msec
 4  kscyang-snyang.abilene.ucaid.edu (198.32.8.103)  33 msec 35 msec 35 msec
 5  iplsng-kscyang.abilene.ucaid.edu (198.32.8.80)  47 msec 45 msec 45 msec
 6  so-0-2-0x1.aa1.mich.net (192.122.183.9)  56 msec 53 msec 54 msec
 7  atm1-0x24.michnet8.mich.net (198.108.23.82)  56 msec 56 msec 57 msec
 8  * * *
 9  A-ARB3-LSA-NG.c-SEB.umnet.umich.edu (141.211.5.22)  58 msec 58 msec 58
    msec
10  umaxpl.physics.lsa.umich.edu (141.211.101.64)  62 msec 63 msec 63 msec
Trace completed

```

The following table describes the significant fields shown in the display:

Field	Description
1	Indicates the sequence number of the router in the path to the host.
i2-gateway.stanford.edu	Host name of this router.
192.68.191.83	IP address of this router.
1 msec 1 msec 1 msec	Round-trip time for each of the probes that are sent.

The following are characters that can appear in the traceroute command output:

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
F	Fragmentation required and DF is set.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
R	Fragment reassembly time exceeded
S	Source route failed.
U	Port unreachable.

**telnet** The **telnet** EXEC mode command enables logging on to a host that supports Telnet.

#### SYNTAX

```
telnet {ip-address | hostname} [port] [keyword ...]
```

#### PARAMETERS

- ◆ **ip-address**—Specifies the destination host IP address.
- ◆ **hostname**—Specifies the destination host name. (Length: 1-160 characters. Maximum label length: 63 characters.)
- ◆ **port**—Specifies the decimal TCP port number or one of the keywords listed in the Ports table in the User Guidelines.
- ◆ **keyword**—Specifies the one or more keywords listed in the Keywords table in the User Guidelines.

#### DEFAULT CONFIGURATION

The default port is the Telnet port (23) on the host.

By default, Telnet is enabled.

#### COMMAND MODE

EXEC mode

#### USER GUIDELINES

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To enter a Telnet sequence, press the escape sequence keys (Ctrl-shift-6) followed by a Telnet command character.

#### Special Telnet Sequences

Telnet Sequence	Purpose
Ctrl-shift-6-b	Break
Ctrl-shift-6-c	Interrupt Process (IP)
Ctrl-shift-6-h	Erase Character (EC)
Ctrl-shift-6-o	Abort Output (AO)
Ctrl-shift-6-t	Are You There? (AYT)
Ctrl-shift-6-u	Erase Line (EL)

At any time during an active Telnet session, available Telnet commands can be listed by pressing the Ctrl-shift-6-? keys at the system prompt.

A sample of this list follows. Note that the Ctrl-shift-6 sequence appears as ^^ on the screen.

```

Console> `Ctrl-shift-6` ?
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
Ctrl-shift-6 x suspends the session (return to system command prompt)

```

Several concurrent Telnet sessions can be opened, enabling switching between the sessions. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence keys (Ctrl-shift-6) and x to return to the system command prompt. Then open a new connection with the telnet EXEC mode command.

This command lists concurrent Telnet connections to remote hosts that were opened by the current Telnet session to the local device. It does not list Telnet connections to remote hosts that were opened by other Telnet sessions.

### Keywords Table

Options	Description
<b>/echo</b>	Enables local echo.
<b>/quiet</b>	Prevents onscreen display of all messages from the software.
<b>/source-interface</b>	Specifies the source interface.
<b>/stream</b>	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
<b>Ctrl-shift-6 x</b>	Returns to the System Command Prompt.

### Ports Table

Keyword	Description	Port Number
BGP	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79

**Ports Table**

<b>Keyword</b>	<b>Description</b>	<b>Port Number</b>
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

**EXAMPLE**

The following example displays logging in to IP address 176.213.10.50 via Telnet.

```
Console> telnet 176.213.10.50
Esc U sends telnet EL
```

**resume** The **resume** EXEC mode command enables switching to another open Telnet session.

**SYNTAX**

**resume** [*connection*]

**PARAMETERS**

**connection**—Specifies the connection number. (Range: 1-4 connections.)

**DEFAULT CONFIGURATION**

The default connection number is that of the most recent connection.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following command switches to open Telnet session number 1.

```
Console> resume 1
```

**hostname** The **hostname** Global Configuration mode command specifies or modifies the device host name. Use the **no** form of the command to remove the existing host name.

**SYNTAX**

**hostname** *name*

**no hostname**

**PARAMETERS**

**Name**—specifies The Device Host Name. (Length: 1-160 Characters. Maximum label length: 63 characters.)

**DEFAULT CONFIGURATION**

No host name is defined.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example specifies the device host name as 'enterprise'.

```
Console(config)# hostname enterprise
enterprise(config)#
```

**reload** The **reload** Privileged EXEC mode command reloads the operating system.

**SYNTAX**

**reload**

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example reloads the operating system.

```

Console# reload
This command will reset the whole system and disconnect your current session.
Do you want to continue? (y/n) [n]

```

**service cpu-  
utilization**The **service cpu-utilization** Global Configuration mode command enables measuring CPU utilization. Use the **no** form of this command to restore the default configuration.**SYNTAX****service cpu-utilization****no service cpu-utilization****DEFAULT CONFIGURATION**

Measuring CPU utilization is disabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**Use the **show cpu utilization** Privileged EXEC command to view information on CPU utilization.**EXAMPLE**

The following example enables measuring CPU utilization.

```

Console(config)# service cpu-utilization

```

**show cpu utilization**The **show cpu utilization** Privileged EXEC mode command displays information about CPU utilization.**SYNTAX****show cpu utilization****COMMAND MODE**

Privileged EXEC mode

**USER GUIDELINES**

Use the **service cpu-utilization** Global Configuration mode command to enable measuring CPU utilization.

**EXAMPLE**

The following example displays CPU utilization information.

```

Console# show cpu utilization
CPU utilization service is on.
CPU utilization
-----
five seconds: 5%; one minute: 3%; five minutes: 3%

```

**clear cpu counters** The **clear cpu counters** EXEC mode command clears traffic counters to and from the CPU.

**SYNTAX**

**clear cpu counters**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example clears the CPU traffic counters.

```

Console# clear cpu counters

```

**service cpu-counters** The **service cpu-counters** Global Configuration mode command enables traffic counting to and from the CPU. To disable counting, use the **no** form of this command.

**SYNTAX**

**service cpu-counters**

**no service cpu-counters**

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Use the **show cpu counters** command to display the CPU traffic counters.

**EXAMPLE**

The following example enables counting CPU traffic.

```
Console(config)# service cpu-counters
```

**show cpu counters** The **show cpu counters** EXEC mode command displays traffic counter information to and from the CPU.

**SYNTAX**

**show cpu counters**

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

Use the **service cpu-counters** command to enable traffic counting to and from the CPU.

**EXAMPLE**

The following example displays the CPU traffic counters.

```
Console# show cpu counters
```

```
CPU counters are active.
```

```
In Octets: 987891
In Unicast Packets: 3589
In Multicast Packets: 29
In Broadcast Packets: 8
```

```
Out Octets: 972181
Out Unicast Packets: 3322
Out Multicast Packets: 22
Out Broadcast Packets: 8
```

**show users** The **show users** EXEC mode command displays information about the active users.

**SYNTAX**

**show users**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays information about the active users.

---

```

Console# show users

Username      Protocol      Location
-----      -
Bob           -            172.16.0.1
John          Serial       172.16.0.8
Robert        SSH          172.16.1.7
Betty         HTTP         172.16.1.6
Sam           Telnet       172.16.1.6

```

**show sessions** The **show sessions** EXEC mode command displays open Telnet sessions.

**SYNTAX**

**show sessions**

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

The command displays Telnet sessions to remote hosts opened by the current Telnet session to the local device. It does not display Telnet sessions to remote hosts opened by other Telnet sessions to the local device.

**EXAMPLE**

The following example displays open Telnet sessions.

---

```

Console# show sessions

Connection  Host          Address      Port      Byte
-----
1           Remote router 172.16.1.1  23        89
2           172.16.1.2    172.16.1.2  23        8

```

The following table describes significant fields shown above.

Field	Description
Connection	The connection number.
Host	The remote host to which the device is connected through a Telnet session.
Address	The remote host IP address.
Port	The Telnet TCP port number.
Byte	The number of unread bytes for the user to see on the connection.

**show system** The **show system** EXEC mode command displays system information.

#### SYNTAX

**show system**

#### PARAMETERS

There are no parameters for this command.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the system information.

```

console# show system
System Description:                Standalone Managed L3 10G Switch with
    48 SFP+ slots
System Up Time (days,hour:min:sec): 00,02:21:59
System Contact:
System Name:
System Location:
System MAC Address:                00:08:f2:66:66:66
System Object ID:                  1.3.6.1.4.1.259.10.1.14

Main Power Supply Status:          OK
Fan 1 Status:                      OK

-----
Unit          Temperature (Celsius)      Status
-----
1             37                      OK
-----

```

**show version** The **show version** EXEC mode command displays system version information.

#### SYNTAX

**show version**

#### PARAMETERS

There are no parameters for this command.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays system version information.

```

console > show version
SW version  2.0.0.24 ( date 10-Jan-2011 time 11:57:59 )
Boot version 0.0.2.1 ( date 09-Jan-2011 time 11:47:11 )

```

```
HW version    00.00.01
```

**system resources routing** The **system resources routing** Global Configuration mode command configures the routing table maximum size. Use the **no** form of this command to return to the default size.

#### SYNTAX

**system resources routing** *routes hosts interfaces*

**no system resources routing**

#### PARAMETERS

- ◆ **routes**—Specifies the maximum number of remote networks in the routing table.
- ◆ **hosts**—Specifies the maximum number of directly attached hosts.
- ◆ **interfaces**—Specifies the maximum number of IP interfaces.

#### DEFAULT CONFIGURATION

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The settings are effective after reboot.

#### EXAMPLE

The following example configures the routing table maximum size.

```
Console# system resources routing 20 23 5
```

**show system resources routings** The **show system resources routings** EXEC mode command displays system routing resources information.

#### SYNTAX

**show system resources routings**

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the system routing resources information.

```
Console> show system resources routings
```

Parameters	Current value	After reboot Value
-----	-----	-----
Hosts:	100	100
Routes:	32	32
IP Interfaces:	32	32

**show system tcam utilization** The **show system tcam utilization** EXEC mode command displays the Ternary Content Addressable Memory (TCAM) utilization.

#### SYNTAX

**show system tcam utilization**

#### PARAMETERS

There are no parameters for this command.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays TCAM utilization information.

```
Console> show system tcam utilization
```

```
TCAM utilization: 58%
```

**show system defaults** Use the **show system defaults** command to display system defaults.

#### SYNTAX

**show system defaults** [*section*]

#### PARAMETERS

**section**—Show information for specific session only. Available values are: management, 802.1x, port, fdb, port-mirroring, spanning-tree, vlan, voice-vlan, ip-addressing, network-security and qos-acl.

#### COMMAND MODE

EXEC mode

#### EXAMPLES

```
console# show system defaults
System Mode: Router
```

```
# Management defaults
Telnet: Enabled (Maximum 4 sessions, shared with SSH)
SSH: Disabled (Maximum 4 sessions, shared with Telnet)
```

```

HTTP: Enabled, port 80 (Maximum 27 sessions)
HTTPS: Disabled
SNMP: Enabled.
    User: first
SNMP version: V3
SNMP Local Engine ID: 0000000001
SNMP Notifications: Enabled
SNMP Authentication Notifications: Enabled
Console: Enabled.
Cryptographic keys are generated
HTTPS certificate is generated
Management ACL: No ACL is defined
AAA Telnet authentication login: Local user data base
AAA HTTP authentication login: Local data base
AAA HTTPS authentication login: Local data base
Radius accounting: Disabled
Radius: No server is defined
Tacacs: No server is defined
Syslog: No server is defined
Logging: Enabled
Logging to console: Informational messages
Logging to internal buffer: Informational messages
Logging to file: Error messages
Logging to remote server: Informational messages
Maximum no. of syslog messages: 200
SNTP: supported
SNTP Port No.: 123
SNTP Interface: Enabled
IP Domain Naming System: Enabled
DHCP Auto Configuration: Enabled
DHCP Option 67: Enabled
DHCP Option 82: Enabled

# IPv6 defaults
MLD Version: version 2

# 802.1x defaults
802.1X is disabled
Mode: Multiple session
Guest VLAN: Not defined
Port Authentication Auto Recovery: Disabled

# Interface defaults in present unit
48 10G fiberOptics
Duplex: Full
Flow control: Off
LAGs: No LAG is defined
Storm control: Disabled
Storm control mode: unknown unicast, broadcast, multicast
Port security: Disabled
Port security Auto Recovery: Disabled
LLDP: Enabled
LLDPDU Handeling: Filtering
Jumbo frames: Disabled
Port-Channel Load Balancing: Layer 2,3 & 4

# Bridging defaults
Maximum 32K entries
Aging time: 5 minutes

# Multicast defaults
Multicast filtering: Disabled
IGMP snooping: Disabled
IGMP Querier: Disabled
Unregistered Multicast Addresses: disabled

```

```

MLD snooping: Disabled

# Port monitoring defaults
Port monitor is not defined
Maximum source port: 8
Maximum destination ports for mirroring: 1

# Spanning tree defaults
Spanning tree is Enabled
Spanning tree mode is Rstp
Spanning tree interface: Enabled
Port fast: Disabled
BPDU handling: Flooding
BPDU Guard: Disabled
BPDU Guard Auto Recovery: Disabled
Loopback Guard: Disabled
Loopback Guard Auto Recovery: Disabled

# Vlan defaults
Maximum Vlans: 4094
Default VLAN: Enabled
Default VLAN id: 1
GVRP: Disabled
Port mode: Access
PVID: 1
VLAN membership: 1

# Network security defaults
DHCP snooping: Disabled
ARP inspection: Disabled
ARP inspection Validation: Disabled

# IP addressing defaults
No IP interface is defined

# QoS and ACLs defaults
QoS mode is basic
QoS Basic Trust Mode: CoS
QoS Advanced Trust Mode: CoS-DSCP
ACL Auto Recovery: Disabled
Queue default mapping:
cos  qid:
0    3
1    1
2    2
3    4
4    5
5    6
6    7
7    8

```

**show tech-support** Use the **show tech-support** command to display system and configuration information you can provide to the Technical Assistance Center when reporting a problem.

#### SYNTAX

```
show tech-support [config] [memory]
```

**PARAMETERS**

**Memory**—Displays memory and processor state data.

**Config**—Displays switch configuration within the CLI commands supported on the device.

**DEFAULT CONFIGURATION**

By default, this command displays the output for technical-support-related show commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data.

**COMMAND TYPES**

Switch command.

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**


---

**CAUTION:** Avoid running multiple **show tech-support** commands on a switch or multiple switches on the network segment. Doing so may cause starvation of some time sensitive protocols, like STP.

---

The show tech-support command may timeout if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a set logout timeout value of **0** to disable automatic disconnection of idle sessions or enter a longer timeout value.

The show tech-support command output is continuous, it does not display one screen at a time. To interrupt the output, press Esc.

If you specify the **config** keyword, the show tech-support command displays a list of the commands supported on the device.

If user specifies the **memory** keyword, the show tech-support command displays the output:

**flash info** (dir if existed, or flash mapping)

**show bootvar**

**buffers info** (like print os buff)

**memory info** (like print os mem)

**proc info** (like print os tasks)

versions of software components

**show cpu utilization**

**show system id** The **show system id** EXEC mode command displays the system identity information.

#### SYNTAX

**show system id**

#### PARAMETERS

There are no parameters for this command.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the system identity information.

```
Console> show system id
Serial number : AC5210000024
```

**clock set** The **clock set** Privileged EXEC mode command manually sets the system clock.

#### SYNTAX

```
clock set hh:mm:ss {[day month] | [month day]} year
```

#### Parameters

- ◆ **hh:mm:ss**—Specifies the current time in hours (military format), minutes, and seconds. (Range: hh: 0-23, mm: 0-59, ss: 0-59)
- ◆ **day**—Specifies the current day of the month. (Range: 1-31)
- ◆ **month**—Specifies the current month using the first three letters of the month name. (Range: Jan-Dec)
- ◆ **year**—Specifies the current year. (Range: 2000-2037)

#### COMMAND MODE

Privileged EXEC mode

#### USER GUIDELINES

The user should enter the local clock time and date.

#### EXAMPLE

The following example sets the system time to 13:32:00 on March 7th, 2005.

```
Console# clock set 13:32:00 7 Mar 2005
```

**clock source** The **clock source** Global Configuration mode command configures an external time source for the system clock. Use the **no** form of this command to disable the external time source.

#### SYNTAX

```
clock source {sntp}  
no clock source
```

#### PARAMETERS

**sntp**—Specifies that an SNTP server is the external clock source.

**DEFAULT CONFIGURATION**

There is no external clock source.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example configures an SNTP server as an external time source for the system clock.

```
Console(config)# clock source sntp
```

**clock timezone** Use the **clock timezone** Global Configuration command to set the time zone for display purposes. Use the **no** form of this command to set the time to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), which is the same.

**SYNTAX**

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

**no clock timezone**

**PARAMETERS**

- ◆ **zone**—The acronym of the time zone. (Range: Up to 4 characters)
- ◆ **hours-offset**—Hours difference from UTC. (Range: (-12)-(+13))
- ◆ **minutes-offset**—Minutes difference from UTC. (Range: 0-59)

**DEFAULT CONFIGURATION**

Offset is **0**.

Acronym is empty.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

**EXAMPLE**

```
console(config)# clock timezone abc +2 minutes 32
```

**clock summer-time** Use one of the formats of the **clock summer-time** Global Configuration command to configure the system to automatically switch to summer time (daylight saving time). Use the **no** form of this command to configure the software not to automatically switch to summer time.

#### SYNTAX

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

```
clock summer-time zone date date month year hh:mm date month
year hh:mm [offset]
```

```
clock summer-time zone date month date year hh:mm month date
year hh:mm [offset]
```

```
no clock summer-time
```

#### PARAMETERS

- ◆ **zone**—The acronym of the time zone to be displayed when summer time is in effect. (Range: Up to 4 characters)
- ◆ **recurring**—Indicates that summer time should start and end on the corresponding specified days every year.
- ◆ **date**—Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
- ◆ **usa**—The summer time rules are the United States rules.
- ◆ **eu**—The summer time rules are the European Union rules.
- ◆ **week**—Week of the month. Can be 1-4, first, last.
- ◆ **day**—Day of the week (first three letters by name, such as Sun). (characters)
- ◆ **date**—Date of the month. (Range: 1-31)
- ◆ **month**—Month (first three letters by name, such as Feb). (characters)
- ◆ **year**—year (no abbreviation). (Range: 2000-2097)
- ◆ **hh:mm**—Time (military format) in hours and minutes. (Range: hh:mmhh: 0-23, mm: 0-59)
- ◆ **offset**—Number of minutes to add during summer time (default is 60). (Range: 1440)

#### DEFAULT CONFIGURATION

Summer time is disabled.

#### COMMAND MODE

Global Configuration mode

**USER GUIDELINES**

In both the date and recurring forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

USA rule for daylight saving time:

- ◆ From 2007:
  - Start: Second Sunday in March
  - End: First Sunday in November
  - Time: 2 am local time
- ◆ Before 2007:
  - Start: First Sunday in April
  - End: Last Sunday in October
  - Time: 2 am local time

**EXAMPLE**

```
console(config)# clock summer-time abc date apr 1 2010 09:00 aug 2 2010 09:00

EU rule for daylight saving time:
Start: Last Sunday in March
End: Last Sunday in October
Time: 1.00 am (01:00) Greenwich Mean Time (GMT)
```

**sntp authentication-key** The **sntp authentication-key** Global Configuration mode command defines an authentication key for Simple Network Time Protocol (SNTP). Use the **no** form of this command to remove the authentication key for SNTP.

**SYNTAX**

```
sntp authentication-key key-number md5 key-value
no sntp authentication-key key-number
```

**PARAMETERS**

- ◆ **key-number**—Specifies the key number. (Range: 1–4294967295)
- ◆ **key-value**—Specifies the key value. (Length: 1–8 characters)

**DEFAULT CONFIGURATION**

No authentication key is defined.

**COMMAND MODE**

Global Configuration mode

**EXAMPLES**

The following example defines the authentication key for SNTP.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
```

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

**sntp authenticate** The **sntp authenticate** Global Configuration mode command enables authentication for received Simple Network Time Protocol (SNTP) traffic from servers. Use the **no** form of this command to disable the feature.

**SYNTAX****sntp authenticate****no sntp authenticate****DEFAULT CONFIGURATION**

Authentication is disabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The command is relevant for both unicast and broadcast.

**EXAMPLES**

The following example enables authentication for received SNTP traffic.

```
Console(config)# sntp authenticate
```

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

**sntp trusted-key** The **sntp trusted-key** Global Configuration mode command authenticates the system identity with which Simple Network Time Protocol (SNTP) synchronizes. Use the **no** form of this command to disable system identity authentication.

#### SYNTAX

```
sntp trusted-key key-number
no sntp trusted-key key-number
```

#### PARAMETERS

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

#### DEFAULT CONFIGURATION

No keys are trusted.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The command is relevant for both received unicast and broadcast.

#### EXAMPLES

The following example authenticates key 8.

```
Console(config)# sntp trusted-key 8
```

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

**sntp client poll timer** The **sntp client poll timer** Global Configuration mode command sets the polling time for the Simple Network Time Protocol (SNTP) client. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
sntp client poll timer seconds
no sntp client poll timer
```

#### PARAMETERS

**seconds**—Specifies the polling interval in seconds. (Range: 60–86400)

#### DEFAULT CONFIGURATION

The default polling interval is 1024 seconds.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example sets the polling time for the SNTP client to 120 seconds.

```
Console(config)# sntp client poll timer 120
```

**sntp broadcast client enable**

The **sntp broadcast client enable** Global Configuration mode command enables Simple Network Time Protocol (SNTP) broadcast clients. Use the **no** form of this command to disable SNTP broadcast clients.

**SYNTAX**

**sntp broadcast client enable**  
**no sntp broadcast client enable**

**DEFAULT CONFIGURATION**

The SNTP broadcast client is disabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Use the **sntp client enable** Interface Configuration mode command to enable the SNTP client on a specific interface.

**EXAMPLE**

The following example enables the SNTP broadcast clients.

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

**sntp anycast client enable**

The **sntp anycast client enable** Global Configuration mode command enables the SNTP anycast client. Use the **no** form of this command to disable the SNTP anycast client.

**SYNTAX**

**sntp anycast client enable**  
**no sntp anycast client enable**

**DEFAULT CONFIGURATION**

The SNTP anycast client is disabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The polling time is configured with the **sntp client poll timer** Global Configuration mode command.

Use the **sntp client enable** Interface Configuration mode command to enable the SNTP client on a specific interface.

**EXAMPLE**

The following example enables SNTP anycast clients.

```
Console(config)# sntp anycast client enable
```

**sntp client enable** The **sntp client enable** Global Configuration mode command enables the Simple Network Time Protocol (SNTP) broadcast and anycast client on an interface. Use the **no** form of this command to disable the SNTP client.

**SYNTAX**

**sntp client enable** *{interface-id}*

**no sntp client enable** *{interface-id}*

**PARAMETERS**

**interface-id**—Specifies an interface ID, which can be one of the following types: Ethernet port, Port-channel or VLAN.

**DEFAULT CONFIGURATION**

The SNTP client is disabled on an interface.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The **sntp broadcast client enable** Global Configuration mode command globally enables broadcast clients.

The **sntp anycast client enable** Global Configuration mode command globally enables anycast clients.

**EXAMPLE**

The following example enables the SNTP broadcast and anycast client on tengigabitethernet port te3

```
Console(config)# sntp client enable tengigabitethernet 0/3
```

**sntp client enable (Interface)** To enable the Simple Network Time Protocol (SNTP) broadcast and anycast client on an interface, use the **sntp client enable** Interface Configuration command. Use the **no** form of this command to disable the SNTP client.

The **sntp client enable** Interface Configuration (Ethernet, Port-channel, VLAN) mode command enables the Simple Network Time Protocol (SNTP) broadcast and anycast client on an interface. Use the **no** form of this command to disable the SNTP client.

#### SYNTAX

**sntp client enable**  
**no sntp client enable**

#### DEFAULT CONFIGURATION

The SNTP client is disabled on an interface.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-channel, VLAN) mode

#### USER GUIDELINES

The **sntp broadcast client enable** Global Configuration mode command globally enables broadcast clients.

The **sntp anycast client enable** Global Configuration mode command globally enables anycast clients.

#### EXAMPLE

The following example enables the SNTP broadcast and anycast client on an interface.

```
Console(config-if)# sntp client enable
```

**sntp unicast client enable** The **sntp unicast client enable** Global Configuration mode command enables the device to use Simple Network Time Protocol (SNTP) predefined unicast clients. Use the **no** form of this command to disable the SNTP unicast clients.

#### SYNTAX

**sntp unicast client enable**  
**no sntp unicast client enable**

#### DEFAULT CONFIGURATION

The SNTP unicast client is disabled.

#### COMMAND MODE

Global Configuration mode

**USER GUIDELINES**

Use the **sntp server** Global Configuration mode command to define SNTP servers.

**EXAMPLE**

The following example enables the device to use Simple Network Time Protocol (SNTP) unicast clients.

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

**sntp unicast client poll**

The **sntp unicast client poll** Global Configuration mode command enables polling for the Simple Network Time Protocol (SNTP) predefined unicast clients. Use the **no** form of this command to disable the polling for the SNTP client.

**SYNTAX**

```
sntp unicast client poll
no sntp unicast client poll
```

**DEFAULT CONFIGURATION**

Polling is disabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Polling time is configured with the **sntp client poll timer** Global Configuration mode command.

**EXAMPLE**

The following example enables polling for SNTP predefined unicast clients.

```
Console(config)# sntp unicast client poll
```

**sntp server**

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

**SYNTAX**

```
sntp server {ipv4-address | ipv6-address | ipv6z-address |
             hostname} [poll] [key keyid]
```

```
no sntp server {ipv4-address | ipv6-address | ipv6z-address |
hostname}
```

#### PARAMETERS

- ◆ **ipv4-address**—Specifies the server IPv4 address.
- ◆ **ipv6-address**—Specifies the server IPv6 address. A Link Local address (IPv6Z address) can be defined.
- ◆ **pv6z-address**—Specifies the IPv6Z address to ping. The IPv6Z address format is: *ipv6-link-local-address*%*{interface-name}*. The subparameters are:
  - ◆ **ipv6-link-local-address**—Specifies the IPv6 Link Local address.
    - **interface-name**—Specifies the outgoing interface name. The interface name has the format: *vlan {integer}* | *ch {integer}* | *isatap {integer}* | *{physical-port-name}*. The subparameter integer has the format: *{decimal-digit}* | *{integer}{decimal-digit}*. (Range for the decimal-digit: 0–9)
- ◆ **hostname**—Specifies the server hostname. Only translation to IPv4 addresses is supported. (Length: 1–158 characters. Maximum label length: 63 characters)
- ◆ **poll**—Enables polling.
- ◆ **key keyid**—Specifies the Authentication key to use when sending packets to this peer. (Range:1–4294967295)

#### DEFAULT CONFIGURATION

No servers are defined.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Up to 8 SNTP servers can be defined.

The **sntp unicast client enable** Global Configuration mode command enables predefined unicast clients.

The **sntp unicast client poll** Global Configuration mode command globally enables polling.

Polling time is configured with the **sntp client poll timer** Global Configuration mode command.

The format of an IPv6Z address is: *<ipv6-link-local-address>%<interface-name>*.

**interface-name** = *vlan<integer>* | *ch<integer>* | *isatap<integer>* | *<physical-port-name>* | *0*

**integer** = *<decimal-number>* | *<integer><decimal-number>*

**decimal-number** = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

**physical-port-name** = Designated port number, for example:te16.

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

#### EXAMPLE

The following example configures the device to accept SNTP traffic from the server on 192.1.1.1.

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

**sntp port** The **sntp port** Global Configuration mode command specifies a Simple Network Time Protocol (SNTP) User Datagram Protocol (UDP) port. Use the **no** form of this command to use the SNTP server default port.

#### SYNTAX

**sntp port** *port-number*

**no sntp port**

#### PARAMETERS

**port-number**—Specifies the UDP port number used by an SNTP server. (Range 1–65535)

#### DEFAULT CONFIGURATION

The default port number is 123.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example specifies that port 321 of the SNTP server is the UDP port.

```
Console(config)# sntp port 321
```

**show clock** The **show clock** EXEC mode command displays the time and date from the system clock.

### SYNTAX

```
show clock [detail]
```

### PARAMETERS

**detail**—Displays the TimeZone and SummerTime configuration.

### COMMAND MODE

EXEC mode

### EXAMPLE

The following example displays the system time and date.

```

Console> show clock
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Console> show clock detail
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Time zone:
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.

DHCP timezone: Disabled

```

```

Device> show clock detail
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Timezone (DHCP):
Acronym is PST
Offset is UTC-8

Timezone (static):
Acronym is PST
Offset is UTC-8

Summertime (Static):
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.

DHCP timezone: Enabled

```

**show sntp configuration** The **show sntp configuration** Privileged EXEC mode command displays the Simple Network Time Protocol (SNTP) configuration on the device.

#### SYNTAX

**show sntp configuration**

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example displays the device's current SNTP configuration.

```

console# show sntp configuration
SNTP port : 123 .
Polling interval: 1024 seconds.
No MD5 authentication keys.
Authentication is not required for synchronization.
No trusted keys.

Unicast Clients: Enabled
Unicast Clients Polling: Enabled

-----
          Server                Polling   Encryption Key
-----
          1.1.1.121             Disabled   Disabled

Broadcast Clients: disabled
Anycast Clients: disabled
No Broadcast Interfaces.
console#

```

**show sntp status** The **show sntp status** Privileged EXEC mode command displays the Simple Network Time Protocol (SNTP) servers status.

#### SYNTAX

**show sntp status**

#### COMMAND MODE

Privileged EXEC mode

**EXAMPLE**

The following example displays the SNTP servers status.

```

Console# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:

Server          Status      Last response                               Offset      Delay
                [mSec]     [mSec]
-----
176.1.1.8       Up          19:58:22.289 PDT Feb 19 2005              7.33       117.79
176.1.8.179     Unknown    12:17:17.987 PDT Feb 19 2005              8.98       189.19

Anycast server:

Server          Interface   Status   Last response                               Offset      Delay
                [mSec]     [mSec]
-----
176.1.11.8      VLAN 118   Up       9:53:21.789 PDT Feb 19 2005              7.19       119.89
                2005

Broadcast:

Server          Interface   Last response
-----
176.9.1.1       VLAN 119   19:17:59.792 PDT Feb 19 2002

```

**EXAMPLE**

```

Device# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:

Server          Status      Last response                               OffsetDelay
                [mSec] [mSec]
-----
176.1.1.8       Up19:58:22.289 PDT Feb 19 2002 7.33117.79
176.1.8.179Unknown12:17:17.987 PDT Feb 19 2002 8.98189.19

Broadcast:

Server          InterfaceLast response
-----
176.9.1.1 VLAN 11919:17:59.792 PDT Feb 19 2002

```

# CONFIGURATION AND IMAGE FILE COMMANDS

**copy** The **copy** Privileged EXEC mode command copies files from a source to a destination.

## SYNTAX

```
copy source-url destination-url [snmp]
```

## PARAMETERS

- ◆ **source-url**—Specifies the source file location URL or source file reserved keyword to be copied. (Length: 1–160 characters)
- ◆ **destination-url**—Specifies the destination file URL or destination file reserved keyword. (Length: 1–160 characters)
- ◆ **snmp**—Specifies that the destination/source file is in SNMP format. Used only when copying from/to startup-config.

The following table displays URL options.

Keyword	Source or Destination
<b>flash://</b>	Source or destination URL for flash memory. This is the default URL. If a URL is specified without a prefix.
<b>running-config</b>	Currently running configuration file.
<b>startup-config</b>	Startup configuration file.
<b>image</b>	Image file. If specified as the source file, it is the active image file. If specified as the destination file, it is the non-active image file.
<b>boot</b>	Boot file.
<b>tftp://</b>	Source or destination URL for a TFTP network server. The syntax for this alias is <i>tftp://host/[directory]/filename</i> . The host can be either an IP address or a host name.
<b>xmodem:</b>	Source for the file from a serial connection that uses the Xmodem protocol.
<b>null:</b>	Null destination for copies or files. A remote file can be copied to null to determine its size.
<b>backup-config</b>	Backup configuration file.
<b>unit://member/ backup-config</b>	Backup configuration file.
<b>WORD&lt;1-128&gt;</b>	Specify URL prefixes.

## COMMAND MODE

Privileged EXEC mode

**USER GUIDELINES**

The location of a file system dictates the format of the source or destination URL.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

If the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. The format of an IPv6Z address is: `{ipv6-link-local-address}%{interface-name}`. The subparameters are:

- ◆ **ipv6-link-local-address**—Specifies the IPv6 Link Local address.
- ◆ **interface-name**—Specifies the outgoing interface name. The interface name has the format: `vlan{integer} | ch{integer} | isatap{integer} | {physical-port-name}`. The subparameter *integer* has the format: `{decimal-digit} | {integer}{decimal-digit}`. *decimal-digit* has the range 0–9

If the egress interface is not specified, the default interface is selected. Specifying **interface zone=0** is equal to not defining an egress interface.

**Understanding Invalid Combinations of Source and Destination**

Some invalid combinations of source and destination exist. Specifically, if one of the following conditions exists:

- ◆ The source file and destination file are the same file.
- ◆ **xmodem:** is the destination file. The source file can be copied to **image**, **boot** and **null:** only.
- ◆ **tftp://** is the source file and destination file on the same copy.
- ◆ **\*.prv** files cannot be copied.

The following table describes the copy characters:

Character	Description
!	For network transfers, indicates that the copy process is taking place. Each exclamation point indicates successful transfer of ten packets (512 bytes each).
.	For network transfers, indicates that the copy process timed out. Generally, several periods in a row means that the copy process may fail.s

**Copying an Image File from a Server to Flash Memory**

Use the **copy source-url image** command to copy an image file from a server to flash memory.

**Copying a Boot File from a Server to Flash Memory**

Use the **copy source-url boot** command to copy a boot file from a server to flash memory.

### **Copying a Configuration File from a Server to the Running Configuration File**

Use the **copy source-url running-config** command to load a configuration file from a network server to the running device configuration file. The commands in the loaded configuration file are added to those in the running configuration file as if the commands were typed in the command-line interface (CLI). The resulting configuration file is a combination of the previous running configuration and the loaded configuration files, with the loaded configuration file taking precedence.

### **Copying a Configuration File from a Server to the Startup Configuration**

Use the **copy source-url startup-config** command to copy a configuration file from a network server to the device startup configuration file. The startup configuration file is replaced by the copied configuration file.

### **Storing the Running or Startup Configuration on a Server**

Use the **copy running-config destination-url** command to copy the current configuration file to a network server using TFTP, .

Use the **copy startup-config destination-url** command to copy the startup configuration file to a network server.

### **Saving The Running Configuration To The Startup Configuration**

Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration file.

### **Backing Up the Running Configuration or Startup Configuration to a Backup Configuration file**

Use the **copy running-config file** command to back up the running configuration to a backup configuration file.

Use the **copy startup-config file** command to back up the startup configuration to a backup configuration file.

### **Backing Up the Running Configuration or Startup Configuration to the Backup Configuration**

Use the **copy running-config backup-config** command to back up the running configuration to the backup configuration file.

Use the **copy startup-config backup-config** command to back up the startup configuration to the backup configuration file.

**EXAMPLES**

The following example copies system image file1 from the TFTP server 172.16.101.101 to a non-active image file.

```

Console# copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!! [OK]
Copy took 0:01:11 [hh:mm:ss]

```

**Copying an Image from a Server to Flash Memory**

The following example copies a system image named file1 from the TFTP server with an IP address of 172.16.101.101 to a non-active image file.

```

Router# copy tftp://172.16.101.101/file1 image
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!! [OK]
Copy took 0:01:11 [hh:mm:ss]

```

**delete** The **delete** Privileged EXEC mode command deletes a file from a flash memory device.

**SYNTAX**

**delete** *url*

**PARAMETERS**

**url**—Specifies the location URL or reserved keyword of the file to be deleted. (Length: 1–160 characters)

The following table displays keywords and URL prefixes:

Keyword	Source or Destination
<b>flash://</b>	URL of the flash memory. This is the default URL if a URL is specified without a prefix.
<b>startup-config</b>	Startup configuration file.
<b>WORD</b>	Specify URL prefixes.

**COMMAND MODE**

Privileged EXEC mode

**USER GUIDELINES**

**\*.sys, \*.prv, image-1** and **image-2** files cannot be deleted.

**EXAMPLE**

The following example deletes the file called 'test' from the flash memory.

```
Console# delete flash:test
Delete flash:test? [confirm]
```

**dir** The **dir** Privileged EXEC mode command displays the list of files on a flash file system.

**SYNTAX**

**dir**

**dir** [*directory-path*]

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the list of files on a flash file system

```
Total size of flash: 33292288 bytes
Free size of flash: 20708893 bytes

console# dir
Directory of flash:

File Name          Permission  Size Data Size      Modified
-----
Flash
-----
tmp                rw          524288    104      01-Jan-2010 05:35:04
image-1            rw          10485760 10485760 01-Jan-2010 06:10:23
image-2            rw          10485760 10485760 01-Jan-2010 05:43:54
dhcpsn.prv         --          262144    --        01-Jan-2010 05:25:07
sshkeys.prv        --          262144    --        04-Jan-2010 06:05:00
syslog1.sys        r-          524288    --        01-Jan-2010 05:57:00
syslog2.sys        r-          524288    --        01-Jan-2010 05:57:00
directry.prv       --          262144    --        01-Jan-2010 05:25:07
startup-config    rw          786432    1081     01-Jan-2010 10:05:34

Total size of flash: 66322432 bytes
Free size of flash: 42205184 bytes

console#
```

**more** The **more** Privileged EXEC mode command displays a file.

**SYNTAX**

**more** *url*

**PARAMETERS**

**url**—Specifies the location URL or reserved keyword of the source file to be displayed. (Length: 1–160 characters).

The following table displays options for the URL parameter:

Keyword	Source or Destination
<b>flash://</b>	Source or destination URL for flash memory. If a URL is specified without a prefix, this is the default URL.
<b>running-config</b>	Current running configuration file.
<b>startup-config</b>	Startup configuration file.

**COMMAND MODE**

Privileged EXEC mode

**USER GUIDELINES**

Files are displayed in ASCII format, except for the images, which are displayed in a hexadecimal format.

\*.prv files cannot be displayed.

**EXAMPLE**

The following example displays the running configuration file contents.

```

console# more running-config
no spanning-tree
interface range te1-48
speed 1000
exit
no lldp run
line console
exec-timeout 0
exit

```

**rename** The **rename** Privileged EXEC mode command renames a file.

**SYNTAX**

```
rename url new-url
```

**PARAMETERS**

- ◆ **url**—Specifies the file location URL. (Length: 1–160 characters)
- ◆ **new-url**—Specifies the file's new URL. (Length: 1–160 characters)

The following table displays options for the URL parameter:

Keyword	Source or Destination
<b>flash://</b>	URL for flash memory. If a URL is specified without a prefix, this is the default URL.
<b>WORD</b>	Specify URL prefixes.

#### COMMAND MODE

Privileged EXEC mode

#### USER GUIDELINES

\*.**sys** and \*.**prv** files cannot be renamed.

#### EXAMPLE

The following example renames the configuration file.

```
Console# rename configuration.bak m-config.bak
```

**boot system** The **boot system** Privileged EXEC mode command specifies the active system image file that is loaded by the device at startup.

#### SYNTAX

```
boot system { image-1 | image-2 }
```

#### PARAMETERS

- ◆ **image-1**—Specifies that image-1 is loaded as the system image during the next device startup.
- ◆ **image-2**—Specifies that image-2 is loaded as the system image during the next device startup.

#### DEFAULT CONFIGURATION

This command has no default configuration.

#### COMMAND MODE

Privileged EXEC mode

#### USER GUIDELINES

Use the **show bootvar** command to determine which image is the active image.

**EXAMPLE**

The following example specifies that **image-1** is the active system image file loaded by the device at startup.

```
Console# boot system image-1
```

**show running-config** The **show running-config** Privileged EXEC mode command displays the current running configuration file contents.

**SYNTAX**

**show running-config**

**PARAMETERS**

This command has no arguments or keywords.

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the running configuration file contents.

```
Console# show running-config
no spanning-tree
interface range te1-48
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
console#
```

**show startup-config** The **show startup-config** Privileged EXEC mode command displays the startup configuration file contents.

**SYNTAX**

**show startup-config**

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the startup configuration file contents.

```

Console# show startup-config
no spanning-tree
interface range te1-48
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
console#

```

**show bootvar** The **show bootvar** EXEC mode command displays the active system image file that is loaded by the device at startup.

**SYNTAX**

**show bootvar**

**PARAMETERS**

There are no parameters for this command.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the active system image file that is loaded by the device at startup.

```

Console# show bootvar

Image      filename      Version      Date                Status
-----      -
1          image-1       1.1.04       23-Jul-2010  17:34:19      Active
2          image-2       1.1.0.5      22-Jan-2010  19:22:32      Not active*

"": Designates that the image was selected for the next boot.

```

# AUTO-UPDATE AND AUTO-CONFIGURATION

**boot host auto-config** Use the **boot host auto-config** Global Configuration mode command to enable the support of auto configuration via DHCP. Use the **no** form of this command to disable DHCP auto configuration.

## SYNTAX

**boot host auto-config**

**no boot host auto-config**

## PARAMETERS

This command has no arguments or key words.

## COMMAND MODE

Global Configuration mode

## DEFAULT CONFIGURATION

Enabled by default.

**show boot** Use the **show boot** Privilege EXEC mode command to show the status of the IP DHCP Auto Config process.

## SYNTAX

**show boot**

## PARAMETERS

This command has no keywords or arguments.

## COMMAND MODE

Privilege EXEC mode

## EXAMPLES

```
console# show boot
Auto Config
-----
Config Download via DHCP: enable
Next Boot Config Download via DHCP: force

Auto Config State: Finished
TFTP Server IP address: 1.2.20.2
Configuration filename: /config/configfile1.cfg

Auto Update
```

```

-----
Image Download via DHCP: enabled

```

```

console# show boot
Auto Config
-----
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Opening <hostname>-config file

```

```

          Auto Update
          -----
Image Download via DHCP: enabled

```

```

console# show boot
Auto Config
-----
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Downloading configuration file

```

```

Auto Update
-----
Image Download via DHCP: enabled

```

```

console# show boot
Auto Config
-----
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Searching hostname in indirect configuration file

```

```

Auto Update
-----
Image Download via DHCP: enabled

```

```

console# show boot
Auto Config
-----
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Quit - failed all steps of finding existing configuration
file

```

```

Auto Update
-----
Image Download via DHCP: enabled

```

```

console# show boot
Auto Config
-----
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default

```

```

Auto Update
-----
Image Download via DHCP: enabled
Auto Update State: Downloaded indirect image file

```

```

console# show boot
Auto Config
-----
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default

Auto Update
-----
Image Download via DHCP: enabled
Auto Update State: Downloading image file

```

```

console# show boot
Auto Config
-----
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Finished
TFTP Server IP address: 1.2.20.2
Configuration filename: /config/configfile1.cfg

```

```

Auto Update
-----
Image Download via DHCP: enabled
Auto Update State: Downloading image file

```

**ip dhcp tftp-server ip addr** Use the **ip dhcp tftp-server ip addr** Global Configuration mode command to set the TFTP server's IP address, used by a switch when it has not been received from the DHCP server. Use the **no** form of this command to remove the address.

#### SYNTAX

```

ip dhcp tftp-server ip addr ip-addr
no ip dhcp tftp-server ip-addr

```

#### PARAMETERS

**ip-addr IP**—Address of TFTP server

#### DEFAULT CONFIGURATION

No IP address

#### COMMAND MODE

Global Configuration mode

**ip dhcp tftp-server file** Use the **ip dhcp tftp-server file** Global Configuration mode command to set the full file name on the TFTP server by a switch when it has not been received from the DHCP server. Use the **no** form of this command to remove the name.

#### SYNTAX

```
ip dhcp tftp-server file file-path
no ip dhcp tftp-server file
```

#### PARAMETERS

**file-path**—full file name on TFTP server

#### DEFAULT CONFIGURATION

No file name

#### COMMAND MODE

Global Configuration mode

**show ip dhcp tftp-server** Use the **show ip dhcp tftp-server** EXEC mode command to display information about the TFTP server.

#### SYNTAX

```
show ip dhcp tftp-server
```

#### COMMAND MODE

EXEC

#### EXAMPLE

```
console# show ip dhcp tftp server
tftp server address
active                    1.1.1.1 from sname
manual                    2.2.2.2
file path on tftp server
activeconf/conf-file from option 67
```

**management access-list** The **management access-list** Global Configuration mode command configures a management access list and enters the Management Access-List Configuration command mode. Use the **no** form of this command to delete an access list.

#### SYNTAX

**management access-list** *name*  
**no management access-list** *name*

#### PARAMETERS

**name**—Specifies the access list name. (Length: 1–32 characters)

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Use this command to configure a management access list. This command enters the Management Access-List Configuration mode, where the denied or permitted access conditions are defined with the **deny** and **permit** commands.

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

When re-entering the access-list context, the new rules are entered at the end of the access list.

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

The active management list cannot be updated or removed.

For IPv6 management traffic that is tunneled in IPv4 packets, the management ACL is applied first on the external IPv4 header (rules with service field are ignored), and then again on the inner IPv6 header.

#### EXAMPLE

The following example creates a management access list called **m1ist**, configures management tengigabitethernet interfaces 0/1 and 0/9, and makes the new access list the active list.

```
Console(config)# management access-list m1ist
Console(config-macl)# permit te1
Console(config-macl)# permit te9
```

```

Console(config-macl)# exit
Console(config)# management access-class mlist

```

The following example creates a management access list called 'mlist', configures all interfaces to be management interfaces except tengigabitethernet interfaces 0/1 and 0/9, and makes the new access list the active list.

```

Console(config)# management access-list mlist
Console(config-macl)# deny tengigabitethernet 0/1
Console(config-macl)# deny tengigabitethernet 0/9
Console(config-macl)# permit
Console(config-macl)# exit
Console(config)# management access-class mlist

```

**permit (Management)** The **permit Management** Access-List Configuration mode command sets conditions for the management access list.

#### SYNTAX

```
permit [interface-id] [service service]
```

```
permit ip-source {ipv4-address | ipv6-address/ipv6-prefix-length}
[mask {mask | prefix-length}] [interface-id] [service service]
```

#### PARAMETERS

- ◆ **interface-id**:—Specify an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- ◆ **service service** — Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- ◆ **ipv4-address**— Specifies the source IPv4 address.
- ◆ **ipv6-address/ipv6-prefix-length**— Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- ◆ **mask mask** — Specifies the source IPv4 address network mask. This parameter is relevant only to IPv4 addresses.
- ◆ **mask prefix-length** — Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). This parameter is relevant only to IPv4 addresses. (Range: 0–32)

#### COMMAND MODE

Management Access-List Configuration mode

**USER GUIDELINES**

Rules with ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

**EXAMPLE**

The following example permits all ports in the access list called **mlist**

```
Console(config)# management access-list mlist
Console(config-macl)# permit
```

**deny (Management)** The **deny** Management Access-List Configuration mode command sets conditions for the management access list.

**SYNTAX**

**deny** [*interface-id*] [*service service*]

**deny ip-source** {*ipv4-address* | *ipv6-address/ipv6-prefix-length*}  
[*mask {mask | prefix-length}*] [*interface-id*] [*service service*]

**PARAMETERS**

- ◆ **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- ◆ **service service**—Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- ◆ **ipv4-address**—Specifies the source IPv4 address.
- ◆ **ipv6-address/ipv6-prefix-length**—Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- ◆ **mask mask**—Specifies the source IPv4 address network mask. The parameter is relevant only to IPv4 addresses.
- ◆ **mask prefix-length**—Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). The parameter is relevant only to IPv4 addresses. (Range: 0–32)

**COMMAND MODE**

Management Access-List Configuration mode

**USER GUIDELINES**

Rules with ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

**EXAMPLE**

The following example denies all ports in the access list called **mlist**.

```
Console(config)# management access-list mlist
Console(config-macl)# deny
```

**management access-class**

The **management access-class** Global Configuration mode command restricts management connections by defining the active management access list. To disable management connection restrictions, use the **no** form of this command.

**SYNTAX**

```
management access-class {console-only | name}
no management access-class
```

**PARAMETERS**

- ◆ **console-only**—Specifies that the device can be managed only from the console.
- ◆ **name**—Specifies the access list name to be used. (Length: 1–32 characters)

**DEFAULT CONFIGURATION**

The default configuration is no management connection restrictions.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example defines an access list called **mlist** as the active management access list.

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

**show management access-list**

The **show management access-list** Privileged EXEC mode command displays management access lists.

**SYNTAX**

```
show management access-list [name]
```

**PARAMETERS**

**name**—Specifies the name of a management access list to be displayed. (Length: 1–32 characters)

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**The following example displays the **mlist** management access list.

```

Console# show management access-list mlist
console-only
-----
deny
! (Note: all other access implicitly denied)
mlist
-----
permit tel
permit te9
! (Note: all other access implicitly denied)
console#

```

**show management access-class** The **show management access-class** Privileged EXEC mode command displays information about the active management access list.

**SYNTAX****show management access-class****COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the active management access list information.

```

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

```

# NETWORK MANAGEMENT PROTOCOL (SNMP) COMMANDS

**snmp-server** Use the **snmp-server server** Global Configuration mode command to enable the device to be configured by SNMP. Use the **no** form of this command to disable this function.

## SYNTAX

```
snmp-server server  
no snmp-server server
```

## PARAMETERS

This command has no arguments or keywords.

## DEFAULT

Enabled

## COMMAND MODE

Global Configuration mode

## EXAMPLE

```
console(config)# snmp-server server
```

**snmp-server community** Use the **snmp-server community** Global Configuration mode command to set up the community access string to permit access to the Simple Network Management Protocol command. Use the **no** form of this command to remove the specified community string.

## SYNTAX

```
snmp-server community string [view view-name] [ro | rw | su]  
                          {ipv4-address | ipv6-address} [mask | prefix-length] [type router |  
                          oob]  
no snmp-server community string [ipv4-address | ipv6-address]
```

## PARAMETERS

- ◆ **string**—Community string that acts like a password and permits access to the SNMP protocol. (Range: 1–20 characters)
- ◆ **ro**—Specifies read-only access (default)
- ◆ **rw**—Specifies read-write access

- ◆ **su**—Specifies SNMP administrator access
- ◆ **view view-name**—Specifies the name of a view to be configured using the command **snmp-server view** (no specific order of the command configurations is imposed on the user). The view defines the objects available to the community. It is not relevant for **su**, which has access to the whole MIB. If unspecified, all the objects, except the community-table and SNMPv3 user and access tables, are available. (Range: 1–30 characters)
- ◆ **ipv4-address**—Management station IPv4 address. The default is all IP addresses.
- ◆ **ipv6-address**—Management station IPv4 address. The default is all IP addresses.
- ◆ **mask**—Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet's source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- ◆ **prefix-length**—Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.
- ◆ **group-name**—Specifies the name of a group that should be configured using the command **snmp-server group** with v1 or v2 parameter (no specific order of the two command configurations is imposed on the user). The group defines the objects available to the community. (Range: 1–30 characters)
- ◆ **type router**—Specifies that SNMP requests for duplicate tables configure the router tables. This is the default.
- ◆ **type oob**—Specifies that SNMP requests for duplicate tables configure the oob tables.

**DEFAULT**

No community is defined

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

You can't specify view-name for su, which has access to the whole MIB.

You can use the view-name to restrict the access rights of a community string.

The logical key of the command is the pair (community, ip-address). If ip-address is omitted then the key is (community, All-Ips).

By specifying the view-name parameter, the software:

- ◆ Generates an internal security-name.
- ◆ Maps the internal security-name for SNMPv1 and SNMPv2 security models to an internal group-name.
- ◆ Maps the internal group-name for SNMPv1 and SNMPv2 security models to view-name (read-view and notify-view always, and for rw for write-view also),

You can use the group-name to restrict the access rights of a community string. By specifying the group-name parameter the software:

- ◆ Generates an internal security-name.
- ◆ Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

The **snmp-server community-group** command and **snmp-server user** command for v1 and v2 are equivalent. You should use the **snmp-server community-group** command when you want to configure the ipv4-address| ipv6-address management addresses.

The Type keyword is used for a different purpose. Therefore, when defining an SNMP community, the administrator must indicate which tables are being configured. If Type is router, it means that the device's tables are being configured.

#### EXAMPLE

```
snmp-server community
=====
console(config)# snmp-server community abcd su 1.1.1.121 mask 255.0.0.0
console(config)# snmp-server community-group tom abcd 1.1.1.122 prefix 8
```

**snmp-server view** The **snmp-server view** Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server view entry. Use the **no** form of this command to remove an SNMP server view entry.

#### SYNTAX

```
snmp-server view view-name oid-tree {included | excluded}
no snmp-server view view-name [oid-tree]
```

#### PARAMETERS

- ◆ **view-name**—Specifies the label for the view record that is being created or updated. The name is used to reference the record. (Length: 1–30 characters)
- ◆ **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System.

Replace a single sub-identifier with the asterisk (\*) wildcard to specify a subtree family; for example 1.3.\*.4.

- ◆ **included**—Specifies that the view type is included.
- ◆ **excluded**—Specifies that the view type is excluded.

#### DEFAULT CONFIGURATION

Default and DefaultSuper are the default view names.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

This command can be entered multiple times for the same view record.

The command logical key is the pair (view-name, oid-tree).

The number of views is limited to 64.

Default and DefaultSuper views are reserved for internal software use and cannot be deleted or modified.

#### EXAMPLE

The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group.

```
Console(config)# snmp-server view user-view system included
Console(config)# snmp-server view user-view system.7 excluded
Console(config)# snmp-server view user-view ifEntry.*.1 included
```

**snmp-server group** The **snmp-server group** Global Configuration mode command configures a new Simple Network Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. Use the **no** form of this command, remove a specified SNMP group.

#### SYNTAX

```
snmp-server group groupname {v1 | v2 | v3 {noauth | auth | priv}
[notify notifyview]} [read readview] [write writeview]
```

```
no snmp-server group groupname {v1 | v2 | v3 [noauth | auth |
priv]} [context name]
```

#### PARAMETERS

- ◆ **groupname**—Specifies the group name. (Length: 1–30 characters)
- ◆ **v1**—Specifies the SNMP Version 1 security model.
- ◆ **v2**—Specifies the SNMP Version 2 security model.

- ◆ **v3**—Specifies the SNMP Version 3 security model.
- ◆ **noauth**—Specifies no packet authentication. Applicable only to the SNMP Version 3 security model.
- ◆ **auth**—Specifies packet authentication without encryption. Applicable only to the SNMP Version 3 security model.
- ◆ **priv**—Specifies packet authentication with encryption. Applicable only to the SNMP Version 3 security model.
- ◆ **notify notifyview**—Specifies the view name that enables specifying an inform or a trap. Applicable only to the SNMP Version 3 security model. (Length: 1–30 characters)
- ◆ **read readview**—Specifies the view name that enables viewing only the agent contents. (Length: 1–30 characters)
- ◆ **write writeview**—Specifies the view name that enables entering data and configuring the agent contents. (Length: 1–30 characters)

#### DEFAULT CONFIGURATION

No group entry exists.

If **notifyview** is not specified, nothing is defined for the notify view.

If **readview** is not specified, all objects except for the community-table and SNMPv3 user and access tables are available.

If **writeview** is not specified, nothing is defined for the write view.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The command logical key is (**groupname, snmp-version, security-level**). For snmp-version v1/v2 the security-level is always **noauth**.

The **Router** context is translated to "" context in the MIB.

#### EXAMPLE

The following example attaches a group called user-group to SNMPv3 and assigns to the group the privacy security level and read access rights to a view called user-view.

```
Console(config)# snmp-server group user-group v3 priv read user-view
```

**snmp-server user** Use the **snmp-server user** Global Configuration mode command to configure a new SNMP Version 3 user. Use the **no** form of the command to remove a user.

#### SYNTAX

```
snmp-server user username groupname {v1 | v2c | [remote host]
v3 [encrypted] [auth {md5 | sha} auth-password]}
no snmp-server user username [remote host]
```

#### PARAMETERS

- ◆ **username**—The name of the user on the host that connects to the agent. (Range: Up to 20 characters)
- ◆ **groupname**—The name of the group to which the user belongs. The group should be configured using the command **snmp-server group** with v3 parameters (no specific order of the 2 command configurations is imposed on the user). (Range: Up to 30 characters)
- ◆ **remote host**—IP address of the remote SNMP host.
- ◆ **v1**—Specifies that v1 is to be used.
- ◆ **v2c**—Specifies that v2c is to be used.
- ◆ **v3**—Specifies that v3 is to be used.
- ◆ **encrypted**—Specifies whether the password appears in encrypted format.
- ◆ **auth**—Specifies which authentication level is to be used.
- ◆ **md5**—Specifies the HMAC-MD5-96 authentication level.
- ◆ **Sha**—Specifies the HMAC-SHA-96 authentication level.
- ◆ **auth-password**—Specifies the authentication password.

**Parameters Range** engineid-string 5 - 32 characters.

auth-passwordUp to 32 characters.

#### DEFAULT

No group entry exists.

#### COMMAND MODE

Global configuration

#### USER GUIDELINES

If **auth md5** or **auth sha** is specified, both authentication and privacy are enabled for the user.

When you enter a **show running-config** command, you do not see a line for this user. To see if this user has been added to the configuration, type the **show snmp user** command.

An SNMP EngineID should be defined in order to add users to the device.

Changing or removing the value of **snmpEngineID** deletes the SNMPv3 users' database.

The logical key of the command is Username.

Configuring a remote host is required in order to send informs to that host. A configured remote host is also able to manage the device (besides getting the informs)

To configure a remote user, specify the IP address for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID remote** command. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command fails.

#### EXAMPLE

```

snmp-server user
=====
console(config)# snmp-server user tom acbd v1
console(config)# snmp-server user tom acbd v2c
console(config)# snmp-server engineid local default
The engine-id must be unique within your administrative domain.
Do you wish to continue? [Y/N]
y
The SNMPv3 database will be erased. Do you wish to continue? [Y/N]
y
console(config)# snmp-server user tom acbd v3

```

**snmp-server filter** The **snmp-server filter** Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server filter entry. Use the **no** form of this command to remove the specified SNMP server filter entry.

#### SYNTAX

```

snmp-server filter filter-name oid-tree {included | excluded}
no snmp-server filter filter-name [oid-tree]

```

#### PARAMETERS

- ◆ **filter-name**—Specifies the label for the filter record that is being updated or created. The name is used to reference the record. (Length: 1–30 characters)

- ◆ **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System. Replace a single sub-identifier with the asterisk (\*) wildcard to specify a subtree family; for example, 1.3.\*.4.
- ◆ **included**—Specifies that the filter type is included.
- ◆ **excluded**—Specifies that the filter type is excluded.

#### DEFAULT CONFIGURATION

No view entry exists.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

This command can be entered multiple times for the same filter record. If an object identifier is included in two or more lines, later lines take precedence. The command's logical key is the pair (filter-name, oid-tree).

#### EXAMPLE

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group.

```
Console(config)# snmp-server filter filter-name system included
Console(config)# snmp-server filter filter-name system.7 excluded
Console(config)# snmp-server filter filter-name ifEntry.*.1 included
```

**snmp-server host** Use the **snmp-server host** Global Configuration mode command to specify the recipient of a Simple Network Management Protocol notification operation. Use the **no** form of this command to remove the specified host.

#### SYNTAX

```
snmp-server host { ipv4-address | ipv6-address | hostname } [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [filter filtername] [timeout seconds] [retries retries]
```

```
no snmp-server host { ipv4-address | ipv6-address | hostname } [traps | informs] [version {1 | 2c | 3}]
```

#### PARAMETERS

- ◆ **pv4-address**—IPv4 address of the host (the targeted recipient).
- ◆ **ipv6-address**—Pv6 address of the host (the targeted recipient). When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.

- ◆ **hostname**—Hostname of the host. (Range: 1–158 characters. Maximum label size: 63)
- ◆ **trap**—Sends SNMP traps to this host (default).
- ◆ **informs**—Sends SNMP informs to this host. Not applicable to SNMPv1.
- ◆ **1**—SNMPv1 traps are used.
- ◆ **2c**—SNMPv2 traps are used
- ◆ **3**—SNMPv2 traps are used
- ◆ **community-string**—Password-like community string sent with the notification operation. (Range: 1–20 characters)
- ◆ **noauth**—Specifies no authentication of a packet.
- ◆ **auth**—Specifies authentication of a packet without encrypting it.
- ◆ **priv**—Specifies authentication of a packet with encryption.
- ◆ **udp-port port**—UDP port of the host to use. The default is 162. (Range: 1–65535)
- ◆ **filter filename**—A string that is the name of the filter that defines the filter for this host. If unspecified, nothing is filtered. The filter should be defined using the command **snmp-server filter** (no specific order of the command configurations is imposed on the user). (Range: Up to 30 characters)
- ◆ **timeout seconds**—Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. The parameter is relevant only for informs. (Range: 1–300)
- ◆ **retries retries**—Maximum number of times to resend an inform request, when a response is not received for a generated message. The default is 3. The parameter is relevant only for informs. (Range: 0–255)

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The logical key of the command is the pair (ip-address/hostname, traps/informs, version).

When configuring snmp v1 or v2 notifications recipient the software would automatically generate a notification view for that recipient for all the MIB. (.For SNMPv3 the software doesn't automatically create a user nor a notify view. Use the commands **snmp-server user**, **snmp-server group** and **snmp-server view** in Global Configuration mode to create a user, a group or a notify group respectively.

The format of an IPv6Z address is: *<ipv6-link-local-address>%<interface-name>*

**interface-name** = *vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name> | 0*

**integer** = *<decimal-number> | <integer><decimal-number>*

**decimal-number** = *0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9*

**physical-port-name** = Designated port number, for example 0/16

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

#### EXAMPLE

The following defines a host at the IP address displayed.

```
console(config)# snmp-server host 1.1.1.121 abc
```

### snmp-server engineID local

The **snmp-server engineID local** Global Configuration mode command specifies the Simple Network Management Protocol (SNMP) engineID on the local device. Use the **no** form of this command to remove the configured engine ID.

#### SYNTAX

**snmp-server engineID local** *{engineid-string | default}*

**no snmp-server engineID local**

#### PARAMETERS

- ◆ **engineid-string**—Specifies a concatenated hexadecimal character string identifying the engine ID. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. If an odd number of hexadecimal digits are entered, the system automatically prefixes the digit 0 to the string. (Length: 5–32 characters, 9–64 hexadecimal digits)
- ◆ **default**—Specifies that the engine ID is created automatically based on the device MAC address.

#### DEFAULT CONFIGURATION

The engine ID is not configured.

If SNMPv3 is enabled using this command, and the default is specified, the default engine ID is defined per standard as:

- ◆ First 4 octets: First bit = 1, the rest is IANA Enterprise number = 674.
- ◆ Fifth octet: Set to 3 to indicate the MAC address that follows.

- ◆ Last 6 octets: The device MAC address.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

To use SNMPv3, specify an engine ID for the device. Any ID can be specified or use a default string, which is generated using the device MAC address.

As the EngineID should be unique within an administrative domain, the following guidelines are recommended:

- ◆ For standalone devices, use the default keyword to configure the Engine ID.
- ◆ For stackable systems, configure an EngineID, and verify that it is unique within the administrative domain.

Changing or removing the value of **snmpEngineID** deletes the SNMPv3 users database.

The SNMP EngineID cannot be all 0x0 or all 0xF or 0x00000001

#### EXAMPLE

The following example enables SNMPv3 on the device and sets the device local engine ID to the default value.

```
Console(config)# snmp-server engineID local default
```

**snmp-server enable traps** Use the **snmp-server enable traps** Global Configuration mode command to enable the device to send SNMP traps. Use the **no** form of the command to disable SNMP traps.

#### SYNTAX

**snmp-server enable traps**

**no snmp-server enable traps**

#### DEFAULT CONFIGURATION

SNMP traps are enabled.

#### COMMAND MODE

Global Configuration mode

**EXAMPLE**

The following example enables SNMP traps.

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

**snmp-server trap authentication**

Use the **snmp-server trap authentication** Global Configuration mode command to enable the device to send SNMP traps when authentication fails. Use the **no** form of this command to disable SNMP failed authentication traps.

**SYNTAX**

**snmp-server trap authentication**

**no snmp-server trap authentication**

**DEFAULT CONFIGURATION**

SNMP failed authentication traps are enabled.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example enables SNMP failed authentication traps.

```
Console(config)# snmp-server trap authentication
```

**snmp-server contact**

Use the **snmp-server contact** Global Configuration mode command to configure the system contact (sysContact) string. Use the **no** form of the command to remove the system contact information.

**SYNTAX**

**snmp-server contact** *text*

**no snmp-server contact**

**PARAMETERS**

**text**—Specifies the string describing system contact information. (Length: 1–160 characters)

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example configures the system contact point called Technical\_Support.

```
Console(config)# snmp-server contact Technical_Support
```

**snmp-server location** Use the **snmp-server location** Global Configuration mode command to configure the system location string. Use the **no** form of this command to remove the location string.

**SYNTAX**

**snmp-server location** *text*

**no snmp-server location**

**PARAMETERS**

**text**—Specifies a string describing system location information. (Length: 1–160 characters)

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example defines the device location as New\_York.

```
Console(config)# snmp-server location New_York
```

**snmp-server set** Use the **snmp-server set** Global Configuration mode command to define the SNMP MIB value.

**SYNTAX**

**snmp-server set** *variable-name name value [name2 value2 ...]*

**PARAMETERS**

- ◆ **variable-name**—Specifies the SNMP MIB variable name, which must be a valid string.
- ◆ **name value**—Specifies a list of name and value pairs. Each name and value must be a valid string. In the case of scalar MIBs, there is only a single name-value pair. In the case of an entry in a table, there is at least one name-value pair, followed by one or more fields.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Although the CLI can set any required configuration, there might be a situation where an SNMP user sets a MIB variable that does not have an equivalent command. To generate configuration files that support those situations, use the **snmp-server set** command.

**EXAMPLE**

The following example configures the scalar MIB sysName with the value TechSupp.

```
Console(config)# snmp-server set sysName sysname TechSupp
```

**show snmp** Use the **show snmp** Privileged EXEC mode command to display the SNMP status.

**SYNTAX**

**show snmp**

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the SNMP communications status.

```
Console# show snmp
```

SNMP is enabled

Community-String	Community-Access	View name	IP Address	type
public	read only	user-view	All	Router
private	read write	Default	172.16.1.1/10	Router
private	su	DefaultSuper	172.16.1.1	Router

Community-string	Group name	IP address	type
public	user-group	All	Router

Traps are enabled.

Authentication trap is enabled.

Version 1,2 notifications

Target Address	Type	Community	Version	UDP Port	Filter name	T0 Sec	Retries
192.122.173.42	Trap	public	2	162		15	3
192.122.173.42	Inform	public	2	162		15	3

Version 3 notifications

```

Target Address      Type      Username      Security      UDP      Filter      TO      Retries
-----
192.122.173.42     Inform    Bob           Priv          162     -----
                                         Level      Port      name      Sec
-----
System Contact: Robert
System Location: Marketing
    
```

The following table describes the significant fields shown in the display.

Field	Description
<b>Community-string</b>	The community access string permitting access to the SNMP protocol.
<b>Community-access</b>	The access type—read-only, read-write, super access.
<b>IP Address</b>	The management station IP Address.
<b>Trap-Rec-Address</b>	The targeted recipient.
<b>Trap-Rec-Community</b>	The statistics sent with the notification operation.
<b>Version</b>	The SNMP version (1 or 2) for the sent trap.

**show snmp engineID** Use the **show snmp engineID** Privileged EXEC mode command to display the local Simple Network Management Protocol (SNMP) engine ID.

**SYNTAX**

**show snmp engineID**

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the SNMP engine ID.

```

Console # show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
#Editor: If snmp-server engineID remote command is supported add the
following line
IP address                               Remote SNMP engineID
-----
172.16.1.108009009020C0B099C075879
    
```

**show snmp views** Use the **show snmp views** Privileged EXEC mode command to display the configured SNMP views.

**SYNTAX**

**show snmp views** [*viewname*]

**PARAMETERS**

**viewname**—Specifies the view name. (Length: 1–30 characters)

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the configured SNMP views.

```

Console# show snmp views

Name                OID Tree                Type
-----
Default             iso                     Included
Default             snmpNotificationMIB    Excluded

```

**show snmp groups** Use the **show snmp groups** Privileged EXEC mode command to display the configured SNMP groups.

**SYNTAX**

**show snmp groups** [*groupname*]

**PARAMETERS**

**groupname**—Specifies the group name. (Length: 1–30 characters)

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the configured SNMP groups.

```

Console# show snmp groups

Name                Security                Views
                   Model    Level    Read    Write    Notify
-----
user-group          V3      priv    Default  "      "
managers-group     V3      priv    Default  Default  "

```

The following table describes significant fields shown above.

Field	Description
<b>Name</b>	Group name.
<b>Security Model</b>	SNMP model in use (v1, v2 or v3).
<b>Security Level</b>	Packet authentication with encryption. Applicable to SNMP v3 security only.

Field	Description	
<b>Views</b>	Read	View name enabling viewing the agent contents. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.
	Write	View name enabling data entry and managing the agent contents.
	Notify	View name enabling specifying an inform or a trap.

**show snmp filters** Use the **show snmp filters** Privileged EXEC mode command to display the configured SNMP filters.

#### SYNTAX

**show snmp filters** [*filtername*]

#### PARAMETERS

**filtername**—Specifies the filter name. (Length: 1–30 characters)

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example displays the configured SNMP filters.

```

Console# show snmp filters

Name          OID Tree          Type
-----
user-filter   1.3.6.1.2.1.1     Included
user-filter   1.3.6.1.2.1.1.7   Excluded
user-filter   1.3.6.1.2.1.2.2.1.*.1 Included

```

**show snmp users** Use the **show snmp users** Privileged EXEC mode command to display the configured SNMP users.

#### SYNTAX

**show snmp users** [*username*]

#### PARAMETERS

**username**—Specifies the user name. (Length: 1–30 characters)

#### COMMAND MODE

Privileged EXEC mode

**EXAMPLE**

The following example displays the configured SNMP users.

```
Console# show snmp users
```

Name	Group name	Auth Method	Remote
John	user-group	md5	
John	user-group	md5	08009009020C0B099C075879

**crypto key generate dsa** The **crypto key generate dsa** Global Configuration mode command generates DSA key pairs.

#### SYNTAX

**crypto key generate dsa**

#### DEFAULT CONFIGURATION

DSA key pairs do not exist.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

DSA keys are generated in pairs - one public DSA key and one private DSA key.

If the device already has DSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is not saved in the router configuration. However, the keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

#### EXAMPLE

The following example generates DSA key pairs.

```
Console(config)# crypto key generate dsa
```

**crypto key generate rsa** The **crypto key generate rsa** Global Configuration mode command generates RSA key pairs.

#### SYNTAX

**crypto key generate rsa**

#### DEFAULT CONFIGURATION

RSA key pairs do not exist.

#### COMMAND MODE

Global Configuration mode

**USER GUIDELINES**

RSA keys are generated in pairs - one public RSA key and one private RSA key.

If the device already has RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is not saved in the router configuration; however, the keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

**EXAMPLE**

The following example generates RSA key pairs.

```
Console(config)# crypto key generate rsa
```

**show crypto key mypubkey** The **show crypto key mypubkey** Privileged EXEC mode command displays the device SSH public keys.

**SYNTAX**

```
show crypto key mypubkey [rsa | dsa]
```

**PARAMETERS**

- ◆ **rsa**—Displays the RSA key.
- ◆ **dsa**—Displays the DSA key.

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the SSH public RSA keys on the device.

```
Console# show crypto key mypubkey rsa
RSA key data:
005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 87685768
Fingerprint(Hex): 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
Fingerprint(Bubble Babble): yteriuwt jgkljhgk yewiury hdskjfryt gfhkjgk
```

**crypto certificate generate** The **crypto certificate generate** Global Configuration mode command generates a self-signed certificate for HTTPS.

#### SYNTAX

```
crypto certificate number generate [key-generate [length]]
    [passphrase string] [cn common-name] [ou organization-unit] [or
    organization] [loc location] [st state] [cu country] [duration days]
```

#### PARAMETERS

- ◆ **number**—Specifies the certificate number. (Range: 1–2)
- ◆ **key-generate**—Regenerates SSL RSA key.
- ◆ **length**—Specifies the SSL's RSA key length. (Range: 512–2048)
- ◆ **passphrase string**—Specifies the passphrase used for exporting the certificate in PKCS12 file format. (Length: 8–96 characters)
- ◆ **cn common-name**—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters)
- ◆ **ou organization-unit**—Specifies the organization-unit or department name. (Length: 1–64 characters)
- ◆ **or organization**—Specifies the organization name. (Length: 1–64 characters)
- ◆ **loc location**—Specifies the location or city name. (Length: 1–64 characters)
- ◆ **st state**—Specifies the state or province name. (Length: 1–64 characters)
- ◆ **cu country**—Specifies the country name. (Length: 2 characters)
- ◆ **duration days**—Specifies the number of days a certification is valid. (Range: 30–3650)

#### DEFAULT CONFIGURATION

The default certificate number is 1.

The default SSL's RSA key length is 1024.

If **passphrase string** is not specified, the certificate is not exportable.

If **cn common-name** is not specified, it defaults to the device's lowest static IPv6 address (when the certificate is generated), or to the device's lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

If **duration days** is not specified, it defaults to 365 days.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

This command is not saved in the router configuration. However, the certificate and keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

When exporting a RSA key pair to a PKCS#12 file, the RSA key pair is as secure as the passphrase. Keep the passphrase secure.

If the RSA key does not exist, you must use the parameter **key-generate**.

**EXAMPLE**

The following example generates a self-signed certificate for HTTPS.

```
Console# crypto certificate generate key-generate
```

**crypto certificate request** The **crypto certificate request** Privileged EXEC mode command generates and displays a certificate request for HTTPS.

**SYNTAX**

```
crypto certificate number request common-name [ou organization-unit] [or organization] [loc location] [st state] [cu country]
```

**PARAMETERS**

- ◆ **number**—Specifies the certificate number. (Range: 1–2)
- ◆ **common-name**—Specifies the device’s fully qualified URL or IP address. (Length: 1–64 characters)
- ◆ **ou organization-unit**—Specifies the organization-unit or department name. (Length: 1–64 characters)
- ◆ **or organization**—Specifies the organization name. (Length: 1–64 characters)
- ◆ **loc location**—Specifies the location or city name. (Length: 1–64 characters)
- ◆ **st state**—Specifies the state or province name. (Length: 1–64 characters)
- ◆ **cu country**—Specifies the country name. (Length: 2 characters)

**COMMAND MODE**

Privileged EXEC mode

**USER GUIDELINES**

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, first generate a self-signed certificate using the **crypto certificate generate** Global Configuration mode command to generate the keys. The certificate fields must be re-entered.

After receiving the certificate from the Certification Authority, use the **crypto certificate import** Global Configuration mode command to import the certificate into the device. This certificate replaces the self-signed certificate.

**EXAMPLE**

The following example displays the certificate request for HTTPS.

```

Console# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIWTCASoCAQAwYjELMAKGA1UEBhMCUFAXCzAJBgNVBAGTAkNDM0swCQYDVQQHEwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxOzAJBgNVBAMTAmxkMRAwDgKoZ0IhvcNAQkBFgFsmIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQHdML0831i0fh/F0MV/Kib6Ssz5p+3nUUenbfHp/igVPmFM+1nbqTDeKb2ymCu6KaKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QV1+8Ubx3GyCm/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkHMRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBAUAA4GBAGb8UgIx7rB05m+2m5ZZPhIw18ARSPXwhVdJexFjbnmvcaqjPG8pIiRV6LkxryGF2bVU3jKEipcZa
g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----

CN= router.gm.com
O= General Motors
C= US

```

**crypto certificate import** The **crypto certificate import** Global Configuration mode command imports a certificate signed by a Certification Authority for HTTPS.

**SYNTAX**

**crypto certificate *number* import**

**PARAMETERS**

**number**—Specifies the certificate number. (Range: 1–2)

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

To end the session, use a blank line.

The imported certificate must be based on a certificate request created by the **crypto certificate request** privileged EXEC command.

If the public key found in the certificate does not match the device's SSL RSA key, the command fails.

This command is not saved in the router configuration. However, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).

#### EXAMPLE

The following example imports a certificate signed by Certification Authority for HTTPS.

```

Console(config)# crypto certificate 1 import
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZxJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1Gaqchfmqge0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCA4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBByEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASKwgdkKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTlWU29mdHdhcmU1MjBSb290JTlWQ2VydGlmaWVYLENOPXNlcnZl
-----END CERTIFICATE-----

Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788

```

**crypto certificate export pkcs12** The **crypto certificate export pkcs12** Privileged EXEC mode command exports the certificate and the RSA keys within a PKCS12 file.

#### SYNTAX

**crypto certificate *number* export pkcs12**

#### PARAMETERS

**number**—Specifies the certificate number. (Range: 1–2)

#### COMMAND MODE

Privileged EXEC mode

#### USER GUIDELINES

The **crypto certificate export pkcs12** command creates a PKCS 12 file that contains the certificate and an RSA key pair.

The passphrase for the export is determined when the key is generated.

The certificate and key pair are exported in a standard PEM-format PKCS12 file. This format can be converted to and from the binary PFX file used by Windows and Linux by using the **openssl** command-line tool. See an open source OpenSSL user manual (man pkcs12) for more information.

**EXAMPLE**

The following example exports the certificate and the RSA keys within a PKCS12 file.

```

Console# crypto certificate 1 export pkcs12
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
subject=/C=us/ST= /L= /CN= /O= /OU=
issuer= /C=us/ST= /L= /CN= /O= /OU=
-----BEGIN CERTIFICATE-----
MIIBfDCCASYCAQAwDQYJKoZIhvcNAQEEBQAwSTELMAkGA1UEBhMCdXMxCjAIBgNV
BAGTASAxCjAIBGNVBAcTASAxCjAIBGNVBAMTASAxCjAIBGNVBAoTASAxCjAIBGNV
BAsTASAwHhcNMDQwMjA3MTU1NDQ0WncNMDUwMjA2MTU1NDQ0WjBJMQswCQYDVQQG
EwJ1czEKMAgGA1UECBMBIDEKMAgGA1UEBxMBIDEKMAgGA1UEAxMBIDEKMAgGA1UE
ChMBIDEKMAgGA1UECxMBIDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCZXP/tk3e/
jrulfZw8q8T2oS5ymrEIES/sRJE8uahTBJqKulVHqRYJR3VYa/03HSJ741w5MzPI
iuWZzrbbuXAxAgMBAAEwDQYJKoZIhvcNAQEEBQADQQBQ+GTLeN1p1kARxI4C1fTU
efig3ffZ/tjW5q1t1r5F6zNv/GuXWw7rGzmRyoMXDcYp1TaA4gAIFQCpFGqiSbAx
-----END CERTIFICATE-----
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
Key Attributes: <No Attributes>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 085DCBF3A41D2669
dac0m9jqEp1DM50sIDb8Jq1jxw/1P0kqSxuMhc25OdbE/1fPBg9VSvV1ARaYt16W
bX67UyJ8t7HHF3AowjcWzElQ5GJgSQ0VemsqsRQzjpcTb090rx+cNwVfIvjoedgQ
Mt15+fKIAcqsfeGEGJNXQ4jEzsXakwfQLFfgt4703IpkUn0AxrQzutJDOcC28Uxp
ramVTVS1SkJIvaPuXJxdZ279tDMwZffILBfKJGACT5V5/4WEqDkrF+uuF9/oxm2
5SVL8TvUmXB/3hX4UoaXtxAhuyOdhh1kyyZSpw9BPPR/8bc/wUYERh7+7JXLKHpD
ueeu3znfIX4dDeti8B3xYvvE8kGZjxFN1cC3zc3JsD0IVu1LkyiAa93P4LPEvAwG
Fw1LqmGiiqw9JM/tzc6kYkZXY1FzCrSVf2exP+/tEvM=
-----END RSA PRIVATE KEY-----

```

**crypto certificate import pkcs12** The **crypto certificate import pkcs12** Privileged EXEC mode command imports the certificate and the RSA keys within a PKCS12 file.

**SYNTAX**

**crypto certificate *number* import pkcs12 *passphrase***

**PARAMETERS**

- ◆ **number**—Specifies the certificate number. (Range: 1–2)
- ◆ **passphrase**—Specifies the passphrase used to encrypt the PKCS12 file for export. (Length: 8–96 characters)

**COMMAND MODE**

Privileged EXEC mode

**USER GUIDELINES**

Use the passphrase that was exported by the **crypto certificate export pkcs12** command.

This passphrase is saved for later exports.

**EXAMPLE**

The following example imports the certificate and the RSA keys within a PKCS12 file.

```

Console# crypto certificate 1 import pkcs12 passphrase
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
subject=/C=us/ST= /L= /CN= /O= /OU=
issuer= /C=us/ST= /L= /CN= /O= /OU=
-----BEGIN CERTIFICATE-----
MIIBfDCCASYCAQAwDQYJKoZIhvcNAQEEBQAwSTELMAkGA1UEBhMCdXMxCjAIBgNV
BAGTASAxCjAIBGNVBAcTASAxCjAIBGNVBAMTASAxCjAIBGNVBAoTASAxCjAIBGNV
BAStASAwHhcNMDQwMjA3MTU1NDQ4WhcNMDUwMjA2MTU1NDQ4WjBjMQswCQYDVQQG
EwJ1czEKMAgGA1UECBMIDEKMAgGA1UEBxMBIDEKMAgGA1UEAxMBIDEKMAgGA1UE
ChMBIDEKMAgGA1UECxMBIDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQCZXP/tk3e/
jrulfZw8q8T2oS5ymrEIES/sRJE8uahTBJqKulVHqRYJR3VYa/03HSJ741w5MzPI
iuWZzrbbuXAxAgMBAAEwDQYJKoZIhvcNAQEEBQADQQBQ+GTLeN1p1kARxI4C1fTU
efig3ffz/tjW5q1t1r5F6zNv/GuXWw7rGzmRyoMXDcYp1TaA4gAIFQCpFGqiSbAx
-----END CERTIFICATE-----
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
Key Attributes: <No Attributes>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 085DCBF3A41D2669
dac0m9jqEp1DM50sIDb8Jq1jxw/1P0kqSxuMhc250dBE/1fPBg9VSvV1ARaYt16W
bX67UyJ8t7HHF3AowjcWzElQ5GJgSQ0VemsqsRQzjpcTb090rx+cNwVfIvjoedgQ
Mt15+fKIAcqsEfEgEGJNXQ4jEzsXakwfQLFfgt4703IpkUn0AxrQzutJDOcC28Uxp
raMVTVSlSkJIvaPuXJxdZ279tDMwZffILBfKJGACT5V5/4WEqDkrF+uuF9/oxm2
5SVL8TvUmXB/3hX4UoaXtxAhuyOdhh1kyyzSpw9BPPR/8bc/wUYERh7+7JXLKHpD
ueeu3znfIX4dDeti8B3Yvve8kGZjxFN1cC3zc3JsD0IVu1LkyiAa93P4LPEvAwG
Fw1LqmGiiqw9JM/tzc6kYkZxylFzCrSVf2exP+/tEvM=
-----END RSA PRIVATE KEY-----

```

**show crypto certificate mycertificate** The **show crypto certificate mycertificate** Privileged EXEC mode command displays the device SSL certificates.

**SYNTAX**

**show crypto certificate mycertificate** [*number*]

**PARAMETERS**

**number**—Specifies the certificate number. (Range: 1–2)

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays SSL certificate # 1 present on the device.

```

Console# show crypto certificate mycertificate 1
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZxJ0awZpZXIwX DANBgkqhkiG9w0BAQEFAANLADBIAEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47

```

```
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwdKggc+ggcyGgclsZGFwOi8v  
L0VByb3h5JTlwU29mdHdhcmU1MjBSb290JTlwQ2VydGlmaWVyLENOPXNlcnZl  
-----END CERTIFICATE-----
```

```
Issued by: www.verisign.com  
Valid from: 8/9/2003 to 8/9/2004  
Subject: CN= router.gm.com, O= General Motors, C= US  
Finger print: DC789788 DC88A988 127897BC BB789788
```

---

**ip http server** The **ip http server** Global Configuration mode command enables configuring and monitoring the device from a web browser. Use the **no** form of this command to disable this function.

#### SYNTAX

**ip http server**  
**no ip http server**

#### DEFAULT CONFIGURATION

HTTP server is enabled.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example enables configuring the device from a web browser.

```
Console(config)# ip http server
```

**ip http port** The **ip http port** Global Configuration mode command specifies the TCP port used by the web browser interface. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**ip http port** *port-number*  
**no ip http port**

#### PARAMETERS

**port-number****Port number**—For use by the HTTP server. (Range: 0–65534)

#### DEFAULT CONFIGURATION

The default port number is 80.

#### COMMAND MODE

Global Configuration mode

**EXAMPLE**

The following example configures the http port number as 100.

```
Console(config)# ip http port 100
```

**ip http timeout-policy**

Use the **ip http timeout-policy** Global Configuration mode command to set the interval for the system to wait for user input in http sessions before automatic logoff. Use the **no** form of this command to return to the default value.

**SYNTAX**

**ip http timeout-policy** *idle seconds*

**no ip http timeout-policy**

**PARAMETERS**

**seconds**—Specifies the maximum number of seconds that a connection is kept open if no data is received or response data cannot be sent out. (Range: 0–86400)

**DEFAULT**

600 seconds

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

This command also configures the timeout-policy for HTTPS.

To specify no timeout, enter the **ip http timeout-policy 0** command.

**EXAMPLE**

The following example configures the http port number as 100.

```
Console(config)# ip http timeout-policy 0
```

**ip http secure-server** Use the **ip http secure-server** Global Configuration mode command to enable the device to be configured securely from a browser, and to also enable the device to be monitored or have its configuration modified securely from a browser,. Use the **no** form of this command to disable this function.

#### SYNTAX

```
ip http secure-server
no ip http secure-server
```

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT

Disabled

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Use the **crypto certificate generate** command to generate an HTTPS certificate.

#### EXAMPLE

```
console(config)# ip http secure-server
```

**ip http secure-port** To specify the TCP port to be used by the secure web browser interface, use the **ip http secure-port** Global Configuration mode command. To use the default port, use the **no** form of this command.

#### SYNTAX

```
ip http secure-port port-number
no ip http secure-port
```

#### PARAMETERS

**port-number**—Port number for use by the HTTPS server (Range: 0–65534)

#### DEFAULT

The default port number is 443.

#### COMMAND MODE

Global Configuration mode

**EXAMPLE**

```
console(config)# ip http secure-port 1234
```

**ip https certificate** The **ip https certificate** Global Configuration mode command configures the active certificate for HTTPS. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**ip https certificate** *number*

**no ip https certificate**

**PARAMETERS**

**number**—Specifies the certificate number. (Range: 1–2)

**DEFAULT CONFIGURATION**

The default certificate number is 1.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Use the **crypto certificate generate** command to generate a HTTPS certificate.

**EXAMPLE**

The following example configures the active certificate for HTTPS.

```
Console(config)# ip https certificate 2
```

**show ip http** The **show ip http** EXEC mode command displays the HTTP server configuration.

**SYNTAX**

**show ip http**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the HTTP server configuration.

```

Console# show ip http
HTTP server enabled
Port: 80
Interactive timeout: 10 minutes

```

**show ip https** The **show ip https** Privileged EXEC mode command displays the HTTPS server configuration.

**SYNTAX**

**show ip https**

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the HTTPS server configuration.

```

Console# show ip https
HTTPS server enabled
Port: 443
Interactive timeout: Follows the HTTP interactive timeout (10 minutes)

Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788

Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, O= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA

```

# TELNET, SECURE SHELL (SSH), AND SECURE LOGIN (SLOGIN) COMMANDS

**ip telnet server** The **ip telnet server** Global Configuration mode command enables the device to be configured from a Telnet server. Use the **no** form of this command to disable the device configuration from a Telnet server.

## SYNTAX

**ip telnet server**  
**no ip telnet server**

## DEFAULT CONFIGURATION

Device configuration from a Telnet server is enabled.

## COMMAND MODE

Global Configuration mode

## USER GUIDELINES

To control the device configuration by SSH, use the **ip ssh server** Global Configuration mode command.

## EXAMPLE

The following example enables the device to be configured from a Telnet server.

```
Console(config)# ip telnet server
```

**ip ssh port** The **ip ssh port** Global Configuration mode command specifies the port used by the SSH server. Use the **no** form of this command to restore the default configuration.

## SYNTAX

**ip ssh port** *port-number*  
**no ip ssh port**

## PARAMETERS

**port-number**—Specifies the port number to be used by the SSH server. (Range: 1–65535)

## DEFAULT CONFIGURATION

The default port number is 22.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example specifies that port number 8080 is used by the SSH server.

```
Console(config)# ip ssh port 8080
```

**ip ssh server** The **ip ssh server** Global Configuration mode command enables the device to be configured from an SSH server. Use the **no** form of this command to disable the device configuration from a SSH server,.

**SYNTAX**

**ip ssh server**

**no ip ssh server**

**DEFAULT CONFIGURATION**

Device configuration from an SSH server is enabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the **crypto key generate dsa** and **crypto key generate rsa** Global Configuration mode commands.

**EXAMPLE**

The following example enables configuring the device from a SSH server.

```
Console(config)# ip ssh server
```

**ip ssh pubkey-auth** The **ip ssh pubkey-auth** Global Configuration mode command enables public key authentication of incoming SSH sessions. Use the **no** form of this command to disable this function.

**SYNTAX**

**ip ssh pubkey-auth**

**no ip ssh pubkey-auth**

**DEFAULT CONFIGURATION**

Public Key authentication of incoming SSH sessions is disabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

AAA authentication is independent.

**EXAMPLE**

The following example enables public key authentication for incoming SSH sessions.

```
Console(config)# ip ssh pubkey-auth
```

**crypto key pubkey-chain ssh**

The **crypto key pubkey-chain ssh** Global Configuration mode command enters the SSH Public Key-chain Configuration mode. This mode is used to manually specify other device public keys such as SSH client public keys.

**SYNTAX****crypto key pubkey-chain ssh****DEFAULT CONFIGURATION**

Keys do not exist.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Use this command when you want to manually specify SSH client's public keys.

**EXAMPLE**

The following example enters the SSH Public Key-chain Configuration mode and manually configures the RSA key pair for SSH public key-chain to 'bob'.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob
Console(config-pubkey-key)# key-string rsa
AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPw1
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfw011g
kTwm175QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licg1k02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkmlshRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaTlweFwWx6f+
Rmt5nhhqAtN/4oJfcel66DqVX1gWmN
```

```
zNR4DYDvSzg01DnwCAC8Qh
```

```
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

**user-key** The **user-key** SSH Public Key-string Configuration mode command specifies which SSH public key is manually configured. Use the **no** form of this command to remove an SSH public key.

#### SYNTAX

```
user-key username {rsa | dsa}
```

```
no user-key username
```

#### PARAMETERS

- ◆ **username**—Specifies the remote SSH client username. (Length: 1–48 characters)
- ◆ **rsa**—Specifies that the RSA key pair is manually configured.
- ◆ **dsa**—Specifies that the DSA key pair is manually configured.

#### DEFAULT CONFIGURATION

No SSH public keys exist.

#### COMMAND MODE

SSH Public Key-string Configuration mode

#### USER GUIDELINES

Follow this command with the **key-string** SSH Public Key-String Configuration mode command to specify the key.

Please note that after entering this command, the existing key is deleted even if no new key is defined by the **key-string** command

#### EXAMPLE

The following example enables manually configuring an SSH public key for SSH public key-chain **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAQCVtRwPWl
```

**key-string** The **key-string** SSH Public Key-string Configuration mode command manually specifies an SSH public key.

#### SYNTAX

```
key-string [row key-string]
```

**PARAMETERS**

- ◆ **row**—Specifies the SSH public key row by row.
- ◆ **key-string**—Specifies the key in UU-encoded DER format. UU-encoded DER format is the same format as in the `authorized_keys` file used by OpenSSH. (Length:0–160)

**DEFAULT CONFIGURATION**

Keys do not exist.

**COMMAND MODE**

SSH Public Key-string Configuration mode

**USER GUIDELINES**

Use the **key-string** SSH Public Key-string Configuration mode command without the **row** parameter to specify which SSH public key is to be interactively configured next. Enter a row with no characters to complete the command.

Use the **key-string row** SSH Public Key-string Configuration mode command to specify the SSH public key, row by row. Each row must begin with a **key-string row** command.

The UU-encoded DER format is the same format as in the `authorized_keys` file used by OpenSSH.

**EXAMPLE**

The following example enters public key strings for SSH public key client 'bob'.

```

Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfzSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfw011g
kTwm175QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licg1k02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkmlshRE7Di71+w3fNiOA
6w9o44t6+AINEICCCA4YcF6zMzaTlwefwWx6f+
Rmt5nhhqdAtN/4oJfcel66DqVX1gWmN
zNR4DYDvSzg01DnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9

Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row AAAAB3Nza
Console(config-pubkey-key)# key-string row C1yc2

```

**show ip ssh** The **show ip ssh** Privileged EXEC mode command displays the SSH server configuration.

#### SYNTAX

**show ip ssh**

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example displays the SSH server configuration.

```

Console# show ip ssh

SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.

SSH Public Key Authentication is enabled.

Active incoming sessions:

IP address      SSH username    Version    Cipher    Auth code
-----
172.16.0.1     John Brown      1.5        3DES     HMAC-SHA1
  
```

The following table describes the significant fields shown in the display.

Field	Description
<b>IP address</b>	The client address
<b>SSH username</b>	The user name
<b>Version</b>	The SSH version number
<b>Cipher</b>	The encryption type (3DES, Blowfish, RC4)
<b>Auth Code</b>	The authentication Code (HMAC-MD5, HMAC-SHA1)

**show crypto key pubkey-chain ssh** The **show crypto key pubkey-chain ssh** Privileged EXEC mode command displays SSH public keys stored on the device.

#### SYNTAX

**show crypto key pubkey-chain ssh** [*username username*]  
 [*fingerprint {bubble-babble | hex}*]

#### PARAMETERS

- ◆ **username username**—Specifies the remote SSH client username. (Length: 1–48 characters)

- ◆ **fingerprint {bubble-babble | hex}**—Specifies the fingerprint display format. The possible values are:
  - **bubble-babble**—Specifies that the fingerprint is displayed in Bubble Babble format.
  - **hex**—Specifies that the fingerprint is displayed in hexadecimal format.

#### DEFAULT CONFIGURATION

The default fingerprint format is hexadecimal.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following examples display SSH public keys stored on the device.

```

Console# show crypto key pubkey-chain ssh

Username
-----
bob
john
Fingerprint
-----
9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8

Console# show crypto key pubkey-chain ssh username bob
Username: bob
Key: 005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
    04AEF1BA A54028A6 9ACC01C5 129D99E4
Fingerprint: 9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86

```

**line** The **line** Global Configuration mode command identifies a specific line for configuration and enters the Line Configuration command mode.

#### SYNTAX

```
line {console | telnet | ssh}
```

#### PARAMETERS

- ◆ **console**—Enters the console terminal line mode.
- ◆ **telnet**—Configures the device as a virtual terminal for remote console access (Telnet).
- ◆ **ssh**—Configures the device as a virtual terminal for secured remote console access (SSH).

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example configures the device as a virtual terminal for remote (Telnet) console access.

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

**speed** The **speed** Line Configuration mode command sets the line baud rate. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
speed bps
```

```
no speed
```

#### PARAMETERS

**bps**—Specifies the baud rate in bits per second (bps). Possible values are 2400, 4800, 9600, 19200, 38400, 57600, and 115200.

#### DEFAULT CONFIGURATION

The default speed is 9600 bps.

**COMMAND MODE**

Line Configuration (console) mode

**USER GUIDELINES**

The configured speed is applied when Autobaud is disabled. This configuration applies to the current session only.

**EXAMPLE**

The following example configures the line baud rate as 9600 bits per second.

```
Console(config-line)# speed 9600
```

**autobaud** The **autobaud** Line Configuration mode command sets the line for automatic baud rate detection (autobaud). Use the **no** form of this command to disable automatic baud rate detection.

**SYNTAX**

**autobaud**

**no autobaud**

**DEFAULT CONFIGURATION**

Automatic baud rate detection is disabled.

**COMMAND MODE**

Line Configuration mode

**USER GUIDELINES**

To start communication using Autobaud, press the **Enter** key twice.

**EXAMPLE**

The following example enables autobaud.

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

**exec-timeout** The **exec-timeout** Line Configuration mode command sets the session idle time interval, during which the system waits for user input before automatic logoff. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
exec-timeout minutes [seconds]  
no exec-timeout
```

#### PARAMETERS

- ◆ **minutes**—Specifies the number of minutes. (Range: 0-65535)
- ◆ **seconds**—Specifies the number of seconds. (Range: 0-59)

#### DEFAULT CONFIGURATION

The default idle time interval is 10 minutes.

#### COMMAND MODE

Line Configuration mode

#### USER GUIDELINES

To specify no timeout, enter the **exec-timeout 0 0** command.

#### EXAMPLE

The following example sets the HTTP session idle time interval before automatic logoff to 20 minutes.

```
Console(config)# line console  
Console(config-line)# exec-timeout 20
```

**show line** The **show line** EXEC mode command displays line parameters.

#### SYNTAX

```
show line [console | telnet | ssh]
```

#### PARAMETERS

- ◆ **console**—Displays the console configuration.
- ◆ **telnet**—Displays the Telnet configuration.
- ◆ **ssh**—Displays the SSH configuration.

#### DEFAULT CONFIGURATION

If the line is not specified, all line configuration parameters are displayed.

#### COMMAND MODE

EXEC mode

**EXAMPLE**

The following example displays the line configuration.

```
Console> show line

Console configuration:

Interactive timeout: Disabled
History: 10
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1

Telnet configuration:

Telnet is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10

SSH configuration:

SSH is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10
```

**aaa authentication login** The **aaa authentication login** Global Configuration mode command sets an authentication method applied during login. Use the **no** form of this command to restore the default authentication method.

#### SYNTAX

```
aaa authentication login {default | list-name} method [method2 ...]
no aaa authentication login {default | list-name}
```

#### PARAMETERS

- ◆ **default**—Uses the listed authentication methods that follow this argument as the default method list when a user logs in.
- ◆ **list-name**—Specifies a name for a list of authentication methods activated when a user logs in. (Length: 1–12 characters)
- ◆ **method [method2 ...]**—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. Select one or more methods from the following list:

Keyword	Description
<b>enable</b>	Uses the enable password for authentication.
<b>line</b>	Uses the line password for authentication.
<b>local</b>	Uses the local username database for authentication.
<b>none</b>	Uses no authentication.
<b>radius</b>	Uses the list of all RADIUS servers for authentication.
<b>tacacs</b>	Uses the list of all TACACS+ servers for authentication.

#### DEFAULT CONFIGURATION

The local user database is the default authentication method. This is the same as entering the command **aaa authentication login local**.

If an authentication method is not defined, console users can log in without any authentication verification.

#### COMMAND MODE

Global Configuration mode

**USER GUIDELINES**

The default and additional list names created with the **aaa authentication login** command are used with the **login authentication** command.

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

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds even if all methods return an error.

**EXAMPLE**

The following example sets the authentication login methods.

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

**aaa authentication enable**

The **aaa authentication enable** Global Configuration mode command sets an authentication method for accessing higher privilege levels. To restore the default authentication method, use the **no** form of this command.

**SYNTAX**

```
aaa authentication enable {default | list-name} method [method2 ...]
```

```
no aaa authentication enable {default | list-name}
```

**PARAMETERS**

- ◆ **default**—Uses the listed authentication methods that follow this argument as the default method list, when accessing higher privilege levels.
- ◆ **list-name** —Specifies a name for the list of authentication methods activated when a user accesses higher privilege levels. (Length: 1–12 characters)
- ◆ **method [method2 ...]**—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

Keyword	Description
<b>enable</b>	Uses the enable password for authentication.
<b>line</b>	Uses the line password for authentication.
<b>none</b>	Uses no authentication.
<b>radius</b>	Uses the list of all RADIUS servers for authentication. Uses username "\$enabx\$," where x is the privilege level.
<b>tacacs</b>	Uses the list of all TACACS servers for authentication. Uses username "\$enabx\$," where x is the privilege level.

### DEFAULT CONFIGURATION

The **enable password** command is the default authentication login method. This is the same as entering the command **aaa authentication enable default enable**.

On a console, the enable password is used if a password exists. If no password is set, authentication still succeeds. This is the same as entering the command **aaa authentication enable default enable none**.

### COMMAND MODE

Global Configuration mode

### USER GUIDELINES

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

All **aaa authentication enable default** requests sent by the device to a RADIUS or TACACS+ server include the username **\$enabx\$**, where **x** is the requested privilege level.

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

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds even if all methods return an error.

### EXAMPLE

The following example sets the enable password for authentication for accessing higher privilege levels.

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

**login authentication** The **login authentication** Line Configuration mode command specifies the login authentication method list for a remote Telnet or console session. Use the **no** form of this command to restore the default authentication method.

#### SYNTAX

```
login authentication {default | list-name}
no login authentication
```

#### PARAMETERS

- ◆ **default**—Uses the default list created with the **aaa authentication login** command.
- ◆ **list-name**—Uses the specified list created with the **aaa authentication login** command. (Length: 1–12 characters).

#### DEFAULT CONFIGURATION

The default is the **aaa authentication login** command default.

#### COMMAND MODE

Line Configuration mode

#### EXAMPLE

The following example specifies the login authentication method for a console session.

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

**enable authentication** The **enable authentication** Line Configuration mode command specifies the authentication method for accessing a higher privilege level from a remote Telnet or console. Use the **no** form of this command to restore the default authentication method.

#### SYNTAX

```
enable authentication {default | list-name}
no enable authentication
```

#### PARAMETERS

- ◆ **default**—Uses the default list created with the **aaa authentication enable** command.
- ◆ **list-name**—Uses the specified list created with the **aaa authentication enable** command. (Length: 1–12 characters).

#### DEFAULT CONFIGURATION

The default is the **aaa authentication enable** command default.

**COMMAND MODE**

Line Configuration mode

**EXAMPLE**

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

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

**ip http authentication**

The **ip http authentication** Global Configuration mode command specifies authentication methods for HTTP server access. Use the **no** form of this command to restore the default authentication method.

**SYNTAX**

```
ip http authentication aaa login-authentication method1
[method2...]
```

```
no ip http authentication aaa login-authentication
```

**PARAMETERS**

**method [method2 ...]**—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

Keyword	Description
<b>local</b>	Uses the local username database for authentication.
<b>none</b>	Uses no authentication.
<b>radius</b>	Uses the list of all RADIUS servers for authentication.
<b>tacacs</b>	Uses the list of all TACACS+ servers for authentication.

**DEFAULT CONFIGURATION**

The local user database is the default authentication login method. This is the same as entering the **ip http authentication local** command.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The command is relevant for HTTP and HTTPS server users.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in

the command line to ensure that the authentication succeeds, even if all methods return an error.

#### EXAMPLE

The following example specifies the HTTP access authentication methods.

```
Console(config)# ip http authentication aaa login-authentication radius local
```

**show authentication methods** The **show authentication methods** Privileged EXEC mode command displays information about the authentication methods.

#### SYNTAX

**show authentication methods**

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example displays the authentication configuration.

```
Console# show authentication methods
```

```
Login Authentication Method Lists
```

```
-----
```

```
Default: Radius, Local, Line
```

```
Console_Login: Line, None
```

```
Enable Authentication Method Lists
```

```
-----
```

```
Default: Radius, Enable
```

```
Console_Enable: Enable, None
```

Line	Login Method List	Enable Method List
-----	-----	-----
Console	Console_Login	Console_Enable
Telnet	Default	Default
SSH	Default	Default

```
HTTP: Radius, local
```

```
HTTPS: Radius, local
```

```
Dot1x: Radius
```

**password** The **password** Line Configuration mode command specifies a password on a line, also known as access method, such as a console or Telnet. Use the **no** form of this command to return to the default password.

#### SYNTAX

```
password password [encrypted]  
no password
```

#### PARAMETERS

- ◆ **password**—Specifies the password for this line. (Length: 0–159 characters)
- ◆ **encrypted**—Specifies that the password is encrypted and copied from another device configuration.

#### DEFAULT CONFIGURATION

No password is defined.

#### COMMAND MODE

Line Configuration mode

#### EXAMPLE

The following example specifies the password 'secret' on a console.

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

**enable password** Use the **enable password** Global Configuration mode command to set a local password to control access to normal and privilege levels. Use the **no** form of this command to return to the default password.

#### SYNTAX

```
enable password [level privilege-level] { password | encrypted  
encrypted-password }  
no enable password [level level]
```

#### PARAMETERS

- ◆ **level** *privilege-level*—Level for which the password applies. If not specified the level is 15. (Range: 1–15)
- ◆ **password**—Password for this level. (Range: 0–159 chars)
- ◆ **encrypted-password**—Encrypted password you enter, copied from another device configuration.

#### DEFAULT

Default for **level** is 15.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

```
console(config)# enable password level 15 let-me-in
```

**username** Use the **username** Global Configuration mode command to establish a username-based authentication system. Use the **no** form to remove a user name.

**SYNTAX**

```
username name { nopassword | password password | privilege
  privilege-level | password encrypted encrypted-password }
```

```
username name
```

```
no username name
```

**PARAMETERS**

- ◆ **name**—The name of the user. (Range: 1–20 characters)
- ◆ **nopassword**—No password is required for this user to log in.
- ◆ **password**—The authentication password for the user. (Range: 1–159)
- ◆ **password-encrypted**—Encrypted password you enter, copied from another device configuration.
- ◆ **privilege privilege-level** —Privilege level for which the password applies. If not specified the level is 15. (Range: 1–15)

**DEFAULT**

No user is defined.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

```
console(config)# username tom privilege 15 password 1234
```

**show user accounts** The **show user accounts** Privileged EXEC mode command displays information about the users local database.

**SYNTAX**

```
show user accounts
```

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays information about the users local database.

```

Console# show user accounts

Username      Privilege
-----      -
Bob           15
Robert        15
Smith         15

```

The following table describes the significant fields shown in the display:

Field	Description
<b>Username</b>	The user name.
<b>Privilege</b>	The user's privilege level.

**aaa accounting login** Use the **aaa accounting login** command in Global Configuration mode to enable accounting of device management sessions. Use the **no** form of this command to disable accounting.

**SYNTAX**

**aaa accounting login** *start-stop group radius*

**no aaa accounting login** *start-stop group radius*

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT**

Disabled

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

This command enables the recording of device management sessions (Telnet, serial and WEB but not SNMP).

It records only users that were identified with a username (e.g. a user that was logged in with a line password is not recorded).

If accounting is activated, the device sends a “start”/“stop” messages to a Radius server when a user logs in / logs out respectively.

The device uses the configured priorities of the available Radius servers in order to select the Radius server.

The following table describes the supported Radius accounting Attributes Values, and when they are sent by the switch.

Name	Start	Stop	Description
<b>User-Name (1)</b>	Yes	Yes	User’s identity.
<b>NAS-IP-Address (4)</b>	Yes	Yes	The switch IP address that is used for the session with the Radius server.
<b>Class (25)</b>	Yes	Yes	Arbitrary value is included in all accounting packets for a specific session.
<b>Called-Station-ID (30)</b>	Yes	Yes	The switch IP address that is used for the management session.
<b>Calling-Station-ID (31)</b>	Yes	Yes	The user IP address.
<b>Acct-Session-ID (44)</b>	Yes	Yes	A unique accounting identifier.
<b>Acct-Authentic (45)</b>	Yes	Yes	Indicates how the supplicant was authenticated.
<b>Acct-Session-Time (46)</b>	No	Yes	Indicates how long the user was logged in.
<b>Acct-Terminate-Cause (49)</b>	No	Yes	Reports why the session was terminated.

#### EXAMPLE

```
console(config)# aaa accounting login start-stop group radius
```

**aaa accounting dot1x** To enable accounting of 802.1x sessions, use the **aaa accounting dot1x** Global Configuration mode command. Use the **no** form of this command to disable accounting.

#### SYNTAX

**aaa accounting dot1x** *start-stop group radius*

**no aaa accounting dot1x** *start-stop group radius*

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT

Disabled

#### COMMAND MODE

Global Configuration mode

**USER GUIDELINES**

This command enables the recording of 802.1x sessions.

If accounting is activated, the device sends a "start"/"stop" messages to a Radius server when a user logs in / logs out to the network, respectively.

The device uses the configured priorities of the available Radius servers in order to select the Radius server.

If a new replaces an old supplicant (even if the port state remains authorized), the software sends a "stop" message for the old supplicant and a "start" message for the new supplicant.

In multiple sessions mode (dot1x multiple-hosts authentication), the software sends "start"/"stop" messages for each authenticated supplicant.

In multiple hosts mode (dot1x multiple-hosts), the software sends "start"/"stop" messages only for the supplicant that has been authenticated.

The software does not send "start"/"stop" messages if the port is force-authorized.

The software does not send "start"/"stop" messages for hosts that are sending traffic on the guest VLAN or on the unauthenticated VLANs.

The following table describes the supported Radius accounting Attributes Values and when they are sent by the switch.

Name	Start	Stop	Description
<b>User-Name (1)</b>	Yes	Yes	Supplicant's identity.
<b>NAS-IP-Address (4)</b>	Yes	Yes	The switch IP address that is used for the session with the Radius server.
<b>NAS-Port (5)</b>	Yes	Yes	The switch port from where the supplicant has logged in.
<b>Class (25)</b>	Yes	Yes	Arbitrary value is included in all accounting packets for a specific session.
<b>Called-Station-ID (30)</b>	Yes	Yes	The switch MAC address.
<b>Calling-Station-ID (31)</b>	Yes	Yes	The supplicant MAC address.
<b>Acct-Session-ID (44)</b>	Yes	Yes	A unique accounting identifier.
<b>Acct-Authentic (45)</b>	Yes	Yes	Indicates how the supplicant was authenticated.
<b>Acct-Session-Time (46)</b>	No	Yes	Indicated how long the supplicant was logged in.
<b>Acct-Terminate-Cause (49)</b>	No	Yes	Reports why the session was terminated.
<b>Nas-Port-Type (61)</b>	Yes	Yes	Indicates the supplicant physical port type.

**EXAMPLE**

```
console(config)# aaa accounting dot1x start-stop group radius
```

**show accounting** The **show accounting** EXEC mode command displays information about the accounting status.

**SYNTAX**

**show accounting**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays information about the accounting status.

```
Console# show accounting
```

```
Login: Radius
802.1x: Disabled
```

**passwords strength minimum character-classes** Use the **passwords strength minimum character-classes** Global Configuration mode command to configure the minimal classes required for passwords in the local database. Use the **no** form to remove the requirement.

**SYNTAX**

**passwords strength minimum character-classes** *number*  
**no passwords strength minimum character-classes**

**PARAMETERS**

*number*—The minimal length required for passwords.(Range: 0–4)

**DEFAULT**

0

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The setting is relevant to local users' passwords, line passwords and enable passwords.

The software checks the minimum length requirement when you define a password in an unencrypted format.

The classes are: upper case letters, lower case letters, numbers and special characters.

#### EXAMPLE

```
Console# passwords strength minimum character-classes
```

### passwords strength max-limit repeated- characters

Use the **passwords strength max-limit repeated-characters** Global Configuration mode command to configure the maximum number of characters in the new password that can be repeated consecutively. Use the **no** form to remove the requirement.

#### SYNTAX

```
passwords strength max-limit repeated-characters number  
no passwords strength max-limit repeated-characters
```

#### PARAMETERS

*number*—The maximum number of characters in the new password that can be repeated consecutively. (Range: 1–16)

#### DEFAULT

1

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The setting is relevant to local users' passwords, line passwords and enable passwords. The software checks the maximum number of characters in the new password that can be repeated consecutively.

#### EXAMPLE

```
Console# passwords strength max-limit repeated-characters
```

**radius-server host** Use the **radius-server host** Global Configuration mode command to specify a RADIUS server host. Use the no form of the command to delete the specified RADIUS server host.

#### SYNTAX

```
radius-server host {ipv4-address | ipv6-address | ipv6z-address |
  hostname} [auth-port auth-port-number] [timeout timeout]
  [retransmit retries] [deadtime deadtime] [key key-string] [source
  {ipv4-address | ipv6-address}] [priority priority] [usage {login |
  802.1x | all}]
```

```
no radius-server host {ipv4-address | ipv6-address | hostname}
```

#### Parameters

- ◆ **ipv4-address**—Specifies the RADIUS server host IPv4 address.
- ◆ **ipv6-address**—Specifies the RADIUS server host IPv6 address.
- ◆ **ipv6z-address**—Specifies the RADIUS server host IPv6Z address. The IPv6Z address format is: **{ipv6-link-local-address}%{interface-name}**. The subparameters are:
  - **ipv6-link-local-address**—Specifies the IPv6 Link Local address.
  - **/interface-name**—Specifies the outgoing interface name. The interface name has the format: **vlan{integer} | ch{integer} | isatap{integer} | {physical-port-name}**.
  - The subparameter **integer** has the format: **{decimal-digit} | {integer}{decimal-digit}**. **decimal-digit** has the range 0–9.
- ◆ **hostname**—Specifies the RADIUS server host name. Translation to IPv4 addresses only is supported. (Length: 1–158 characters. Maximum label length: 63 characters)
- ◆ **auth-port auth-port-number**—Specifies the port number for authentication requests. If the port number is set to 0, the host is not used for authentication. (Range: 0–65535)
- ◆ **timeout timeout**—Specifies the timeout value in seconds. (Range: 1–30)
- ◆ **retransmit retries**—Specifies the retransmit value. (Range: 1–10)

- ◆ **deadtime deadtime**—Specifies the length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)
- ◆ **key key-string**—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Length: 0–128 characters)
- ◆ **source {ipv4-address | ipv6-address}**—Specifies the source IPv4 or IPv6 address to use for communication. 0.0.0.0 is interpreted as a request to use the IP address of the outgoing IP interface.
- ◆ **priority priority**—Specifies the order in which servers are used, where 0 has the highest priority. (Range: 0–65535)
- ◆ **usage {login | 802.1x | all}**—Specifies the RADIUS server usage type. The possible values are:
  - **login**—Specifies that the RADIUS server is used for user login parameters authentication.
  - **802.1x**—Specifies that the RADIUS server is used for 802.1x port authentication.
  - **all**—Specifies that the RADIUS server is used for user login parameters authentication and 802.1x port authentication.

#### DEFAULT CONFIGURATION

No RADIUS host is specified; the global **radius-server** command values are the default values.

The default authentication port number is 1812.

If **timeout** is not specified, the global value is used.

If **retransmit** is not specified, the global value is used.

If **key-string** is not specified, the global value is used.

If the **source** value is not specified, the global value is used.

The default usage type is **all**.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

To specify multiple hosts, multiple **radius-server host** commands can be used.

If no host-specific **timeout**, **retries**, **deadtime** or **key-string** values are specified, the global values apply to each RADIUS server host.

The **source** parameter address type must be the same as that of the **host** parameter.

#### EXAMPLE

The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20, and a 20-second timeout period.

```
Console(config)# radius-server host 192.168.10.1 auth-port 20 timeout 20
```

**radius-server key** Use the **radius-server key** Global Configuration mode command to set the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
radius-server key [key-string]  
no radius-server key
```

#### PARAMETERS

**key-string**—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. (Range: 0–128 characters)

#### DEFAULT CONFIGURATION

The key-string is an empty string.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example defines the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.

```
Console(config)# radius-server key enterprise-server
```

**radius-server retransmit** Use the **radius-server retransmit** Global Configuration mode command to specify the number of times the software searches the list of RADIUS server hosts. Use the no form of this command to restore the default configuration.

#### SYNTAX

```
radius-server retransmit retries
no radius-server retransmit
```

#### PARAMETERS

**retries**—Specifies the retransmit value. (Range: 1–10)

#### DEFAULT CONFIGURATION

The software searches the list of RADIUS server hosts 3 times.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example configures the number of times the software searches all RADIUS server hosts as 5.

```
console(config)# radius-server retransmit 5
```

**radius-server source-ip** Use the **radius-server source-ip** Global Configuration mode command to specify the source IP address used for communication with RADIUS servers. Use the no form of this command to restore the default configuration.

#### SYNTAX

```
radius-server source-ip {source}
no radius-server source-ip {source}
```

#### PARAMETERS

**source**—Specifies the source IP address.

#### DEFAULT CONFIGURATION

The source IP address is the IP address of the outgoing IP interface.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

If there is no available IP interface of the configured IP source address, an error message is issued when attempting to communicate with the IP address.

**EXAMPLE**

The following example configures the source IP address used for communication with all RADIUS servers to 10.1.1.1.

```
console(config)# radius-server source-ip 10.1.1.1
```

**radius-server  
source-ipv6**

Use the **radius-server source-ipv6** Global Configuration mode command to specify the source IPv6 address used for communication with RADIUS servers. Use the no form of this command to restore the default configuration.

**SYNTAX**

```
radius-server source-ipv6 {source}
```

```
no radius-server source-ipv6 {source}
```

**PARAMETERS**

**source**—Specifies the source IPv6 address.

**DEFAULT CONFIGURATION**

The source IP address is the IP address of the outgoing IP interface.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

If there is no available IP interface of the configured IP source address, an error message is issued when attempting to communicate with the IP address.

**EXAMPLE**

The following example configures the source IP address used for communication with all RADIUS servers to 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

```
console(config)# radius-server source-ipv6  
3ffe:1900:4545:3:200:f8ff:fe21:67cf
```

**radius-server timeout** Use the **radius-server timeout** Global Configuration mode command to set the time interval during which the device waits for a server host to reply. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
radius-server timeout timeout
no radius-server timeout
```

#### PARAMETERS

**timeout**—Specifies the timeout value in seconds. (Range: 1–30)

#### DEFAULT CONFIGURATION

The default timeout value is 3 seconds.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example sets the timeout interval on all RADIUS servers to 5 seconds.

```
Console(config)# radius-server timeout 5
```

**radius-server deadtime** Use the **radius-server deadtime** Global Configuration mode command to configure the time interval during which unavailable RADIUS servers are skipped over by transaction requests. This improves RADIUS response time when servers are unavailable. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
radius-server deadtime deadtime
no radius-server deadtime
```

#### PARAMETERS

**deadtime**—Specifies the time interval in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)

#### DEFAULT CONFIGURATION

The default deadtime interval is 0.

#### COMMAND MODE

Global Configuration mode

**EXAMPLE**

The following example sets all RADIUS server deadtimes to 10 minutes.

```
Console(config)# radius-server deadtime 10
```

**show radius-servers** Use the **show radius-servers** Privileged EXEC mode command to display the RADIUS server settings.

**SYNTAX**

**show radius-servers**

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays RADIUS server settings.

```
Console# show radius-servers
```

IP address	Port Auth	Port Acct	Time Out	Retrans mit	Dead time	Source IP	Priority	Usage
172.16.1.1	1812	1813	Global	Global	Global	Global	1	All
172.16.1.2	1812	1813	11	8	Global	Global	2	All

```

Global values
-----
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IP: 172.16.8.1

```

**tacacs-server host** Use the **tacacs-server host** Global Configuration mode command to specify a TACACS+ host. Use the **no** form of this command to delete the specified TACACS+ host.

#### SYNTAX

```
tacacs-server host {ip-address | hostname} [single-connection]  
[port port-number] [timeout timeout] [key key-string] [source  
{source}] [priority priority]
```

```
no tacacs-server host {ip-address | hostname}
```

#### PARAMETERS

- ◆ **ip-address**—Specifies the TACACS+ server host IP address.
- ◆ **hostname**—Specifies the TACACS+ server host name. (Length: 1?158 characters. Maximum label length: 63 characters)
- ◆ **single-connection**—Specifies that a single open connection is maintained between the device and the daemon, instead of the device opening and closing a TCP connection to the daemon each time it communicates.
- ◆ **port port-number**—Specifies the server port number. If the port number is 0, the host is not used for authentication. (Range: 0–65535)
- ◆ **timeout timeout**—Specifies the timeout value in seconds. (Range: 1–30)
- ◆ **key key-string**—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter "". (Length: 0?128 characters)
- ◆ **source {source}**—Specifies the source IP to use for the communication. 0.0.0.0 indicates a request to use the outgoing IP interface IP address.
- ◆ **priority priority**—Specifies the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0–65535)

#### DEFAULT CONFIGURATION

No TACACS+ host is specified.

The default **port-number** is 49.

If **timeout** is not specified, the global value is used.

If **key-string** is not specified, the global value is used.

If **source** is not specified, the global value is used.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Multiple **tacacs-server host** commands can be used to specify multiple hosts.

If no host-specific timeout, key, or source values are specified, the global values apply to each host. Example

The following example specifies a TACACS+ host.

```
Console(config)# tacacs-server host 172.16.1.1
```

**tacacs-server key** Use the **tacacs-server key** Global Configuration mode command to set the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. Use the **no** form of this command to disable the key.

#### SYNTAX

**tacacs-server key** *key-string*

**no tacacs-server key**

#### PARAMETERS

**key-string**—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. (Length: 0–128 characters)

#### DEFAULT CONFIGURATION

The default key is an empty string.

#### COMMAND MODE

Global Configuration mode

**EXAMPLE**

The following example sets Enterprise as the authentication encryption key for all TACACS+ servers.

```
Console(config)# tacacs-server key enterprise
```

**tacacs-server timeout**

Use the **tacacs-server timeout** Global Configuration mode command to set the interval during which the device waits for a TACACS+ server to reply. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**tacacs-server timeout** *timeout*

**no tacacs-server timeout**

**PARAMETERS**

**timeout**—Specifies the timeout value in seconds. (Range: 1–30)

**DEFAULT CONFIGURATION**

The default timeout value is 5 seconds.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example sets the timeout value to 30 for all TACACS+ servers.

```
Console(config)# tacacs-server timeout 30
```

**tacacs-server source-ip**

Use the **tacacs-server source-ip** Global Configuration mode command to configure the source IP address to be used for communication with TACACS+ servers. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**tacacs-server source-ip** *{source}*

**no tacacs-server source-ip** *{source}*

**PARAMETERS**

**source**—Specifies the source IP address. (Range: Valid IP address)

**DEFAULT CONFIGURATION**

The default source IP address is the outgoing IP interface address.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

If the configured IP source address has no available IP interface, an error message is issued when attempting to communicate with the IP address.

**EXAMPLE**

The following example specifies the source IP address for all TACACS+ servers.

```
Console(config)# tacacs-server source-ip 172.16.8.1
```

**show tacacs** Use the **show tacacs** Privileged EXEC mode command to display configuration and statistical information for a TACACS+ server.

**SYNTAX**

```
show tacacs [ip-address]
```

**PARAMETERS**

**ip-address**—Specifies the TACACS+ server name or IP address.

**DEFAULT CONFIGURATION**

If **ip-address** is not specified, information for all TACACS+ servers is displayed.

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays configuration and statistical information for all TACACS+ servers.

```
Console# show tacacs
```

IP address	Status	Port	Single Connection	Time Out	Source IP	Priority
-----	-----	---	-----	-----	-----	-----
172.16.1.1	Connected	49	No	Global	Global	1

```
Global values
```

```
-----
```

```
TimeOut: 3
```

```
Source IP: 172.16.8.1
```

**logging on** Use the **logging on** Global Configuration mode command to control error message logging. This command sends debug or error messages to a logging process, which logs messages asynchronously to designated locations for the process that generated the messages. Use the **no** form of this command to disable the logging process.

#### SYNTAX

**logging on**

**no logging on**

#### DEFAULT CONFIGURATION

Message logging is enabled.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The logging process controls the logging messages distribution at various destinations, such as the logging buffer, logging file or syslog server. Logging on and off at these destinations can be individually configured using the **logging buffered**, **logging file**, and **logging** Global Configuration mode commands. However, if the **logging on** command is disabled, no messages are sent to these destinations. Only the console receives messages.

#### EXAMPLE

The following example enables logging error messages.

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

**Logging host** Use the **logging host** global configuration command to log messages to a syslog server. Use the **no** form of this command to delete the syslog server with the specified address from the list of syslogs.

#### SYNTAX

**logging host** {*ipv4-address* | *ipv6-address* | *hostname*} [*port port*]  
[*severity level*] [*facility facility*] [*description text*]

**no logging host** {*ipv4-address* | *ipv6-address* | *hostname*}

**PARAMETERS**

- ◆ **ipv4-address**—IPv4 address of the host to be used as a syslog server.
- ◆ **ipv6-address**—Pv6 address of the host to be used as a syslog server. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.
- ◆ **hostname**—Hostname of the host to be used as a syslog server. Only translation to IPv4 addresses is supported. (Range: 1–158 characters. Maximum label size: 63)
- ◆ **port**—Port number for syslog messages. If unspecified, the port number defaults to 514. (Range: 1–65535)
- ◆ **level**—Limits the logging of messages to the syslog servers to a specified level: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging.
- ◆ **facility**—The facility that is indicated in the message. It can be one of the following values: local0, local1 , local2 , local3 , local4 , local5 , local 6, local7. If unspecified, the port number defaults to local7.
- ◆ **text**—Description of the syslog server. (Range: Up to 64 characters)

**DEFAULT**

No messages are logged to a syslog server host.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

You can use multiple syslog servers.

The format of an IPv6Z address is: *<ipv6-link-local-address>%<interface-name>*

**interface-name** = *vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name> | 0*

**integer** = *<decimal-number> | <integer><decimal-number>*

**decimal-number** = *0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9*

**physical-port-name** = Designated port number, for example 0/16.

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

**EXAMPLES**

```
console(config)# logging host 1.1.1.121
```

```
console(config)# logging host 3000::100
```

**logging console** Use the **logging console** Global Configuration mode command to limit messages logged to the console to messages with a specific severity level. Use the **no** form of this command to disable logging limiting to the console.

#### SYNTAX

**logging console** *level*

**no logging console**

#### PARAMETERS

**level**—Specifies the severity level of logged messages displayed on the console. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

#### DEFAULT CONFIGURATION

The default severity level is informational.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example limits logging messages displayed on the console to messages with severity level errors.

```
Console(config)# logging console errors
```

**logging buffered** Use the **logging buffered** Global Configuration mode command to limit the syslog message display from an internal buffer to messages with a specific severity level, and to define the buffer size. Use the **no** form of this command to cancel using the buffer and returning the buffer size to default

#### SYNTAX

**logging buffered** [*buffer-size*] [*severity-level*]

**no logging buffered**

#### PARAMETERS

*buffer-size*—Specifies the maximum number of messages stored in the history table. (Range: 20–400)

*severity-level*—Specifies the severity level of messages logged in the buffer. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

**DEFAULT CONFIGURATION**

The default severity level is informational.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

All the syslog messages are logged to the internal buffer. This command limits the messages displayed to the user.

**EXAMPLE**

The following example limits the syslog message display from an internal buffer to messages with severity level **debugging**.

```
Console(config)# logging buffered debugging
```

**clear logging** Use the **clear logging** Privileged EXEC mode command to clear messages from the internal logging buffer.

**SYNTAX**

**clear logging**

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example clears messages from the internal logging buffer.

```
Console# clear logging
Clear logging buffer [confirm]
```

**logging file** Use the **logging file** Global Configuration mode command to limit syslog messages sent to the logging file to messages with a specific severity level. Use the **no** form of this command to cancel using the buffer.

**SYNTAX**

**logging file** *level*

**no logging file**

**PARAMETERS**

**level**—Specifies the severity level of syslog messages sent to the logging file. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

**DEFAULT CONFIGURATION**

The default severity level is errors.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example limits syslog messages sent to the logging file to messages with severity level alerts.

```
Console(config)# logging file alerts
```

**clear logging file** Use the **clear logging file** Privileged EXEC mode command to clear messages from the logging file.

**SYNTAX**

**clear logging file**

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example clears messages from the logging file.

```
Console# clear logging file
Clear Logging File [y/n]
```

**aaa logging** Use the **aaa logging** Global Configuration mode command to enable logging AAA login events. Use the **no** form of this command to disable logging AAA login events.

**SYNTAX**

**aaa logging** *{login}*  
**no aaa logging** *{login}*

**PARAMETERS**

**login**—Enables logging messages related to successful AAA login events, unsuccessful AAA login events and other AAA login-related events.

**DEFAULT CONFIGURATION**

Logging of AAA login events is enabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

This command enables logging messages related to successful login events, unsuccessful login events and other login-related events. Other types of AAA events are not subject to this command.

**EXAMPLE**

The following example enables logging messages related to AAA login events.

```
Console(config)# aaa logging login
```

**file-system logging** Use the **file-system logging** Global Configuration mode command to enable the logging of file system events. Use the **no** form of this command to disable logging file system events.

**SYNTAX**

**file-system logging** {*copy* | *delete-rename*}

**no file-system logging** {*copy* | *delete-rename*}

**PARAMETERS**

- ◆ **copy**—Specifies logging messages related to file copy operations.
- ◆ **delete-rename**—Specifies logging messages related to file deletion and renaming operations.

**DEFAULT CONFIGURATION**

Logging file system events is enabled.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example enables logging messages related to file copy operations.

```
Console(config)# file-system logging copy
```

**management logging** Use the **management logging** Global Configuration mode command to enable logging Management Access List (ACL) deny events. Use the **no** form of this command to disable logging management access list events.

**SYNTAX**

**management logging** {*deny*}

**no management logging** {*deny*}**PARAMETERS**

**deny**—Enables logging messages related to management ACL deny actions.

**DEFAULT CONFIGURATION**

Logging management ACL deny events is enabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Other management ACL events are not subject to this command.

**EXAMPLE**

The following example enables logging messages related to management ACL deny actions.

```
Console(config)# management logging deny
```

**show logging** Use the **show logging** Privileged EXEC mode command to display the logging status and the syslog messages stored in the internal buffer.

**SYNTAX****show logging****COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the logging status and the syslog messages stored in the internal buffer.

```
console# show logging
Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200 Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged

Application filtering control
Application          Event                      Status
-----
AAA                  Login                      Enabled
File system          Copy                       Enabled
File system          Delete-Rename             Enabled
Management ACL       Deny                      Enabled

Aggregation: Disabled.
```

```

Aggregation aging time: 300 Sec

01-Jan-2010 05:29:46 :%INIT-I-Startup: Warm Startup
01-Jan-2010 05:29:02 :%LINK-I-Up: Vlan 1
01-Jan-2010 05:29:02 :%LINK-I-Up: te48
01-Jan-2010 05:29:02 :%LINK-I-Up: te47
01-Jan-2010 05:29:00 :%LINK-W-Down: te48

```

**show logging file** Use the **show logging file** Privileged EXEC mode command to display the logging status and the syslog messages stored in the logging file.

#### SYNTAX

**show logging file**

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example displays the logging status and the syslog messages stored in the logging file.

```

Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200 Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged

Application filtering control
Application          Event                Status
-----
AAA                  Login                Enabled
File system          Copy                  Enabled
File system          Delete-Rename        Enabled
Management ACL       Deny                  Enabled

Aggregation: Disabled.
Aggregation aging time: 300 Sec

01-Jan-2010 05:57:00 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error

01-Jan-2010 05:56:36 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error

01-Jan-2010 05:55:37 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error

01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_read: key_from_blob
bgEgGnt9
z6NHgZwKI5xKqF7cBtdl1xmFgSEWuDhho5UedydAjVkKS5XR2... failed

01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_from_blob: invalid key
type.

```

```
01-Jan-2010 05:56:34 :%SSHD-E-ERROR: SSH error: bad sigbloblen 58 !=
SIGBLOB_LEN
console#
```

**show syslog-servers** Use the **show syslog-servers** Privileged EXEC mode command to display the syslog server settings.

#### SYNTAX

**show syslog-servers**

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example displays the syslog server settings.

```
console# show syslog-servers

Device Configuration
-----

IP address      Port    Severity  Facility Description
-----
1.1.1.121      514     info      local7
3000::100      514     info      local7

console#
```

# REMOTE NETWORK MONITORING (RMON) COMMANDS

**show rmon statistics** Use the **show rmon statistics** EXEC mode command to display RMON Ethernet statistics.

## SYNTAX

```
show rmon statistics {interface-id}
```

## PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

## COMMAND MODE

EXEC mode

## EXAMPLE

The following example displays RMON Ethernet statistics for tengigabitethernet port 0/1.

```
console# show rmon statistics tel
Port tel
Dropped: 0
Octets: 0                               Packets: 0
Broadcast: 0                             Multicast: 0
CRC Align Errors: 0                       Collisions: 0
Undersize Pkts: 0                         Oversize Pkts: 0
Fragments: 0                              Jabbers: 0
64 Octets: 0                              65 to 127 Octets: 1
128 to 255 Octets: 1                      256 to 511 Octets: 1
512 to 1023 Octets: 0                     1024 to max Octets: 0
```

The following table describes the significant fields displayed.

Field	Description
<b>Dropped</b>	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times this condition was detected.
<b>Octets</b>	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
<b>Packets</b>	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
<b>Broadcast</b>	The total number of good packets received and directed to the broadcast address. This does not include multicast packets.

Field	Description
<b>Multicast</b>	The total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.
<b>CRC Align Errors</b>	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
<b>Collisions</b>	The best estimate of the total number of collisions on this Ethernet segment.
<b>Undersize Pkts</b>	The total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
<b>Oversize Pkts</b>	The total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
<b>Fragments</b>	The total number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
<b>Jabbers</b>	The total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
<b>64 Octets</b>	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
<b>65 to 127 Octets</b>	The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
<b>128 to 255 Octets</b>	The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
<b>256 to 511 Octets</b>	The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
<b>512 to 1023 Octets</b>	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
<b>1024 to max</b>	The total number of packets (including bad packets) received that were between 1024 octets and the maximum frame size in length inclusive (excluding framing bits but including FCS octets).

**rmon collection stats** Use the **rmon collection stats** Interface Configuration mode command to enable Remote Monitoring (RMON) MIB history group of statistics on an interface. Use the **no** form of this command to remove a specified RMON history group of statistics.

#### SYNTAX

**rmon collection stats** *index* [*owner ownername*] [*buckets bucket-number*] [*interval seconds*]

**no rmon collection stats** *index*

**PARAMETERS**

- ◆ **index**—The requested group of statistics index.(Range: 1–65535)
- ◆ **owner ownername**—Records the name of the owner of the RMON group of statistics. If unspecified, the name is an empty string. (Range: Valid string)
- ◆ **buckets bucket-number**—A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50.(Range: 1–50)
- ◆ **interval seconds**—The number of seconds in each polling cycle. If unspecified, defaults to 1800 (Range: 1–3600).

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode. Cannot be configured for a range of interfaces (range context).

**show rmon collection stats** Use the **show rmon collection stats** EXEC mode command to display the requested RMON history group statistics.

**SYNTAX**

**show rmon collection stats** [*interface-id*]

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays all RMON history group statistics.

```

Console# show rmon collection stats

```

Index	Interface	Interval	Requested Samples	Granted Samples	Owner
1	te1	30	50	50	CLI
2	te1	1800	50	50	Manager

The following table describes the significant fields shown in the display.

Field	Description
<b>Index</b>	An index that uniquely identifies the entry.
<b>Interface</b>	The sampled Ethernet interface.

Field	Description
<b>Interval</b>	The interval in seconds between samples.
<b>Requested Samples</b>	The requested number of samples to be saved.
<b>Granted Samples</b>	The granted number of samples to be saved.
<b>Owner</b>	The entity that configured this entry.

**show rmon history** Use the **show rmon history** EXEC mode command to display RMON Ethernet history statistics.

#### SYNTAX

```
show rmon history index {throughput | errors | other} [period
seconds]
```

#### PARAMETERS

- ◆ **index**—Specifies the set of samples to display. (Range: 1–65535)
- ◆ **throughput**—Displays throughput counters.
- ◆ **errors**—Displays error counters.
- ◆ **other**—Displays drop and collision counters.
- ◆ **period seconds**—Specifies the period of time in seconds to display. (Range: 1–2147483647)

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following examples display RMON Ethernet history statistics for index 1.

```
Console# show rmon history 1 throughput

Sample Set: 1                      Owner: CLI
Interface: tel                      Interval: 1800
Requested samples: 50              Granted samples: 50

Maximum table size: 500

Time          Octets      Packets    Broadcast  Multicast  Util
-----
Jan 18 2005  303595962  357568    3289       7287       19%
 21:57:00    287696304  275686    2789       5878       20%
Jan 18 2005
 21:57:30
```

```

Console# show rmon history 1 errors

Sample Set: 1                Owner: Me
Interface: tel               Interval: 1800
Requested samples: 50        Granted samples: 50

Maximum table size: 500 (800 after reset)

Time                CRC Align  Undersize  Oversize  Fragments  Jabbers
-----
Jan 18 2005         1          1          0          49          0
  21:57:00         1          1          0          27          0
Jan 18 2005
  21:57:30

```

```

Console# show rmon history 1 other

Sample Set: 1                Owner: Me
Interface: tel               Interval: 1800
Requested samples: 50        Granted samples: 50

Maximum table size: 500

Time                Dropped    Collisions
-----
Jan 18 2005 21:57:00    3          0
Jan 18 2005 21:57:30    3          0

```

The following table describes significant fields shown in the display:

Field	Description
<b>Time</b>	Date and Time the entry is recorded.
<b>Octets</b>	The total number of octets of data (including those in bad packets and excluding framing bits but including FCS octets) received on the network.
<b>Packets</b>	The number of packets (including bad packets) received during this sampling interval.
<b>Broadcast</b>	The number of good packets received during this sampling interval that were directed to the broadcast address.
<b>Multicast</b>	The number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.
<b>Utilization</b>	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
<b>CRC Align</b>	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
<b>Undersize</b>	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.

Field	Description
<b>Oversize</b>	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
<b>Fragments</b>	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
<b>Jabbers</b>	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
<b>Dropped</b>	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is the number of times this condition has been detected.
<b>Collisions</b>	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

**rmon alarm** Use the **rmon alarm** Global Configuration mode command to configure alarm conditions. Use the **no** form of this command to remove an alarm.

#### SYNTAX

```
rmon alarm index mib-object-id interval rthreshold fthreshold revent  
fevent [type {absolute | delta}]  
[startup {rising | rising-falling | falling}] [owner name]
```

```
no rmon alarm index
```

#### PARAMETERS

- ◆ **index**—Specifies the alarm index. (Range: 1–65535)
- ◆ **mib-object-id**—Specifies the object identifier of the variable to be sampled. (Valid OID)
- ◆ **interval**—Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 1–4294967295)
- ◆ **rthreshold**—Specifies the rising threshold value. (Range: 0–4294967295)
- ◆ **fthreshold**—Specifies the falling threshold value. (Range: 0–4294967295)
- ◆ **revent**—Specifies the index of the event triggered when a rising threshold is crossed. (Range: 0–65535)
- ◆ **fevent**—Specifies the index of the event triggered when a falling threshold is crossed. (Range: 0–65535)

- ◆ **type {absolute | delta}**—Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. The possible values are:
  - **absolute**—Specifies that the selected variable value is compared directly with the thresholds at the end of the sampling interval.
  - **delta**—Specifies that the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.
- ◆ **startup {rising | rising-falling | falling}**—Specifies the alarm that may be sent when this entry becomes valid. The possible values are:
  - **rising**—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to **rthreshold**, a single rising alarm is generated.
  - **rising-falling**—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to **rthreshold**, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to **fthreshold**, a single falling alarm is generated.
  - **fallin** —Specifies that if the first sample (after this entry becomes valid) is less than or equal to **fthreshold**, a single falling alarm is generated.
- ◆ **owner name**—Specifies the name of the person who configured this alarm. (Valid string)

#### DEFAULT CONFIGURATION

The default method type is **absolute**.

The default startup direction is **rising-falling**.

If the owner **name** is not specified, it defaults to an empty string.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example configures an alarm with index 1000, MIB object ID, sampling interval 360000 seconds (100 hours), rising threshold value 1000000, falling threshold value 1000000, rising threshold event index 10, falling threshold event index 10, absolute method type and rising-falling alarm.

```
console(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000
1000000 10 20
```

**show rmon alarm-table** Use the **show rmon alarm-table** EXEC mode command to display a summary of the alarms table.

#### SYNTAX

**show rmon alarm-table**

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the alarms table.

```

Console# show rmon alarm-table

Index      OID                      Owner
-----
1          1.3.6.1.2.1.2.2.1.10.1  CLI
2          1.3.6.1.2.1.2.2.1.10.1  Manager
3          1.3.6.1.2.1.2.2.1.10.9  CLI

```

The following table describes the significant fields shown in the display:

Field	Description
<b>Index</b>	An index that uniquely identifies the entry.
<b>OID</b>	Monitored variable OID.
<b>Owner</b>	The entity that configured this entry.

**show rmon alarm** Use the **show rmon alarm** EXEC mode command to display alarm configuration.

#### SYNTAX

**show rmon alarm** *number*

#### PARAMETERS

**number**—Specifies the alarm index. (Range: 1–65535)

#### COMMAND MODE

EXEC mode

**EXAMPLE**

The following example displays RMON 1 alarms.

```

Console# show rmon alarm 1

Alarm 1
-----
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI

```

The following table describes the significant fields shown in the display:

Field	Description
<b>Alarm</b>	Alarm index.
<b>OID</b>	Monitored variable OID.
<b>Last Sample Value</b>	The value of the statistic during the last sampling period. For example, if the sample type is <b>delta</b> , this value is the difference between the samples at the beginning and end of the period. If the sample type is <b>absolute</b> , this value is the sampled value at the end of the period.
<b>Interval</b>	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
<b>Sample Type</b>	The method of sampling the variable and calculating the value compared against the thresholds. If the value is <b>absolute</b> , the variable value is compared directly with the thresholds at the end of the sampling interval. If the value is <b>delta</b> , the variable value at the last sample is subtracted from the current value, and the difference is compared with the thresholds.
<b>Startup Alarm</b>	The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising-falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising-falling, then a single falling alarm is generated.
<b>Rising Threshold</b>	The sampled statistic rising threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
<b>Falling Threshold</b>	The sampled statistic falling threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
<b>Rising Event</b>	The event index used when a rising threshold is crossed.
<b>Falling Event</b>	The event index used when a falling threshold is crossed.
<b>Owner</b>	The entity that configured this entry.

**rmon event** Use the **rmon event** Global Configuration mode command to configure an event. Use the **no** form of this command to remove an event.

#### SYNTAX

```
rmon event index {none | log | trap | log-trap} [community text]
[description text] [owner name]
```

```
no rmon event index
```

#### PARAMETERS

- ◆ **index**—Specifies the event index. (Range: 1–65535)
- ◆ **none**—Specifies that no notification is generated by the device for this event.
- ◆ **log**—Specifies that a notification entry is generated in the log table by the device for this event.
- ◆ **trap**—Specifies that an SNMP trap is sent to one or more management stations by the device for this event.
- ◆ **log-trap**—Specifies that an entry is generated in the log table and an SNMP trap is sent to one or more management stations by the device for this event.
- ◆ **community text**—Specifies the SNMP community to which an SNMP trap is sent. (Octet string; length: 0–127 characters)
- ◆ **description text**—Specifies a comment describing this event. (Length: 0–127 characters)
- ◆ **owner name**—Specifies the name of the person who configured this event. (Valid string)

#### DEFAULT CONFIGURATION

If the owner name is not specified, it defaults to an empty string.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example configures an event identified as index 10, for which the device generates a notification in the log table.

```
Console(config)# rmon event 10 log
```

**show rmon events** Use the **show rmon events** EXEC mode command to display the RMON event table.

#### SYNTAX

**show rmon events**

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the RMON event table.

```

Console# show rmon events

Index  Description      Type      Community  Owner      Last time sent
-----  -----
1      Errors           Log       router     CLI        Jan18 2006 23:58:17
2      High Broadcast   Log-Trap  router     Manager    Jan18 2006 23:59:48

```

The following table describes significant fields shown in the display:

Field	Description
<b>Index</b>	A unique index that identifies this event.
<b>Description</b>	A comment describing this event.
<b>Type</b>	The type of notification that the device generates about this event. Can have the following values: <b>none</b> , <b>log</b> , <b>trap</b> , <b>log-trap</b> . In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
<b>Community</b>	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
<b>Owner</b>	The entity that configured this event.
<b>Last time sent</b>	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

**show rmon log** Use the **show rmon log** EXEC mode command to display the RMON log table.

#### SYNTAX

**show rmon log** [*event*]

#### PARAMETERS

**event**—Specifies the event index. (Range: 0–65535)

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following examples display the RMON log table.

```

Console# show rmon log
Maximum table size: 500 (800 after reset)

Event          Description                               Time
-----          -
1              MIB Var.:                               Jan 18 2006 23:48:19
              1.3.6.1.2.1.2.2.1.10.53
              , Delta, Rising, Actual
              Val: 800, Thres.Set:
              100, Interval (sec):1

```

**rmon table-size** Use the **rmon table-size** Global Configuration mode command to configure the maximum size of RMON tables. Use the no form of this command to return to the default configuration.

**SYNTAX**

**rmon table-size** *{history entries | log entries}*

**no rmon table-size** *{history | log}*

**PARAMETERS**

- ◆ **history entries**—Specifies the maximum number of history table entries. (Range: 20–270)
- ◆ **log entries**—Specifies the maximum number of log table entries. (Range: 20–100)

**DEFAULT CONFIGURATION**

The default history table size is 270 entries.

The default log table size is 200 entries.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The configured table size takes effect after the device is rebooted.

**EXAMPLE**

The following example configures the maximum size of RMON history tables to 100 entries.

```
Console(config)# rmon table-size history 100
```

**aaa authentication dot1x** Use the **aaa authentication dot1x** Global Configuration mode command to specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1x. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
aaa authentication dot1x default method [method2 ...]
no aaa authentication dot1x default
```

#### PARAMETERS

**method** [**method2** ...]—Specify at least one method from the following list:

Keyword	Description
<b>radius</b>	Uses the list of all RADIUS servers for authentication
<b>none</b>	Uses no authentication

#### DEFAULT CONFIGURATION

The default method is Radius.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Additional methods of authentication are used only if the previous method returns an error and not if the request for authentication is denied. Specify **none** as the final method in the command line to ensure that authentication succeeds even if all methods return an error.

#### EXAMPLE

The following example uses the **aaa authentication dot1x default** command with no authentication.

```
Console(config)# aaa authentication dot1x default none
```

**dot1x system-auth-control** Use the **dot1x system-auth-control** Global Configuration mode command to enable 802.1x globally. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
dot1x system-auth-control
no dot1x system-auth-control
```

#### DEFAULT CONFIGURATION

All the ports are in FORCE\_AUTHORIZED state.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example enables 802.1x globally.

```
Console(config)# dot1x system-auth-control
```

**dot1x port-control** Use the **dot1x port-control** Interface Configuration (Ethernet) mode command to enable manual control of the port authorization state. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
dot1x port-control {auto | force-authorized | force-unauthorized}[time-range time-range-name]
no dot1x port-control
```

#### PARAMETERS

- ◆ **auto**—Enables 802.1x authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the device and the client.
- ◆ **force-authorized**—Disables 802.1x authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1x-based client authentication.
- ◆ **force-unauthorized**—Denies all access through this interface by forcing the port to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through the interface.
- ◆ **time-range-name**—Specifies a time range. When the Time Range is not in effect, the port state is Unauthorized. (Range: 1–32 characters)

**DEFAULT CONFIGURATION**

The port is in the force-authorized state.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in **auto** state that are connected to end stations), in order to proceed to the forwarding state immediately after successful authentication.

**EXAMPLE**

The following example enables 802.1x authentication on tengigabitethernet port 0/15.

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# dot1x port-control auto
```

**dot1x reauthentication**

Use the **dot1x reauthentication** Interface Configuration mode command to enable periodic re-authentication of the client. Use the **no** form of this command to return to the default setting.

**SYNTAX**

**dot1x reauthentication**

**no dot1x reauthentication**

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT**

Periodic re-authentication is disabled.

**COMMAND MODE**

Interface configuration (Ethernet)

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# dot1x reauthentication
```

**dot1x timeout reauth-period** Use the **dot1x timeout reauth-period** Interface Configuration mode command to set the number of seconds between re-authentication attempts. Use the **no** form of this command to return to the default setting.

#### SYNTAX

```
dot1x timeout reauth-period seconds
no dot1x timeout reauth-period
```

#### PARAMETERS

**seconds**—Number of seconds between re-authentication attempts. (Range: 30–4294967295)

#### DEFAULT

3600

#### COMMAND MODE

Interface Configuration (Ethernet) mode

#### EXAMPLE

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# dot1x timeout reauth-period 5000
```

**dot1x re-authenticate** The **dot1x re-authenticate** Privileged EXEC mode command manually initiates re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.

#### SYNTAX

```
dot1x re-authenticate [interface-id]
```

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following command manually initiates re-authentication of 802.1x-enabled tengigabitethernet port 0/15.

```
Console# dot1x re-authenticate tengigabitethernet 0/15
```

**dot1x timeout quiet-period** Use the **dot1x timeout quiet-period** Interface Configuration (Ethernet) mode command to set the time interval that the device remains in a quiet state following a failed authentication exchange (for example, the client provided an invalid password). Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
dot1x timeout quiet-period seconds
no dot1x timeout quiet-period
```

#### PARAMETERS

**seconds**—Specifies the time interval in seconds that the device remains in a quiet state following a failed authentication exchange with the client. (Range: 0–65535 seconds)

#### DEFAULT CONFIGURATION

The default quiet period is 60 seconds.

#### COMMAND MODE

Interface Configuration (Ethernet) mode

#### USER GUIDELINES

During the quiet period, the device does not accept or initiate authentication requests.

The default value of this command should only be changed to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide faster response time to the user, a smaller number than the default value should be entered.

#### EXAMPLE

The following example sets the time interval that the device remains in the quiet state following a failed authentication exchange to 3600 seconds.

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# dot1x timeout quiet-period 3600
```

**dot1x timeout tx-period** Use the **dot1x timeout tx-period** Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
dot1x timeout tx-period seconds
no dot1x timeout tx-period
```

#### PARAMETERS

**seconds**—Specifies the time interval in seconds during which the device waits for a response to an EAP-request/identity frame from the client before resending the request. (Range: 1–65535 seconds)

#### DEFAULT CONFIGURATION

The default timeout period is 30 seconds.

#### COMMAND MODE

Interface Configuration (Ethernet) mode

#### USER GUIDELINES

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

#### EXAMPLE

The following command sets the time interval during which the device waits for a response to an EAP request/identity frame to 3600 seconds.

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# dot1x timeout tx-period 3600
```

**dot1x max-req** Use the **dot1x max-req** Interface Configuration mode command to set the maximum number of times that the device sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client before restarting the authentication process. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
dot1x max-req count
no dot1x max-req
```

**PARAMETERS**

**count**—Specifies the maximum number of times that the device sends an EAP request/identity frame before restarting the authentication process. (Range: 1–10)

**DEFAULT CONFIGURATION**

The default maximum number of attempts is 2.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**EXAMPLE**

The following example sets the maximum number of times that the device sends an EAP request/identity frame to 6

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# dot1x max-req 6
```

**dot1x timeout supp-timeout**

Use the **dot1x timeout supp-timeout** Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request frame from the client before resending the request. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
dot1x timeout supp-timeout seconds
no dot1x timeout supp-timeout
```

**PARAMETERS**

**seconds**—Specifies the time interval in seconds during which the device waits for a response to an EAP request frame from the client before resending the request. (Range: 1–65535 seconds)

**DEFAULT CONFIGURATION**

The default timeout period is 30 seconds.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**EXAMPLE**

The following example sets the time interval during which the device waits for a response to an EAP request frame from the client before resending the request to 3600 seconds.

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# dot1x timeout supp-timeout 3600
```

**dot1x timeout server-timeout**

Use the **dot1x timeout server-timeout** Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response from the authentication server. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
dot1x timeout server-timeout seconds
no dot1x timeout server-timeout
```

**PARAMETERS**

**seconds**—Specifies the time interval in seconds during which the device waits for a response from the authentication server. (Range: 1–65535 seconds)

**DEFAULT CONFIGURATION**

The default timeout period is 30 seconds.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

The actual timeout period can be determined by comparing the value specified by the **dot1x timeout server-timeout** command to the result of multiplying the number of retries specified by the **radius-server retransmit** command by the timeout period specified by the **radius-server timeout** command, and selecting the lower of the two values.

**EXAMPLE**

The following example sets the time interval between retransmission of packets to the authentication server to 3600 seconds.

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# dot1x timeout server-timeout 3600
```

**show dot1x** Use the **show dot1x** Privileged EXEC mode command to display the 802.1x device or specified interface status.

### SYNTAX

**show dot1x** [*interface interface-id*]

### PARAMETERS

**interface-id**—Specify an interface ID. The interface ID must be an Ethernet port.

### COMMAND MODE

Privileged EXEC mode

### EXAMPLE

The following examples display the status of 802.1x-enabled Ethernet ports.

```
Console# show dot1x
802.1x is enabled
```

Port	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
te1	Auto	Authorized	Ena	3600	Bob
te2	Auto	Authorized	Ena	3600	John
te3	Auto	Unauthorized	Ena	3600	Clark
te4	Force-auth	Authorized	Dis	3600	n/a
te5	Force-auth	Unauthorized	Dis	3600	n/a

\* Port is down or not present.

```
Console# show dot1x interface te3
```

802.1x is enabled.

Port	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
te3	Auto	Unauthorized	Ena	3600	Clark

```
Time-range:          work-hours (Inactive now)
Quiet period:        60 Seconds
Tx period:           30 Seconds
Max req:             2
Supplicant timeout:  30 Seconds
```

```

Server timeout:                30 Seconds
Session Time (HH:MM:SS):      08:19:17
MAC Address:                   00:08:78:32:98:78
Authentication Method:         Remote
Termination Cause:            Supplicant logoff

```

## Authenticator State Machine

```
State:                          HELD
```

## Backend State Machine

```
State:                          IDLE
Authentication success:         9
Authentication fails:          1
```

The following table describes the significant fields shown in the display.

Field	Description
<b>Port</b>	The port number.
<b>Admin mode</b>	The port admin mode. Possible values: Force-auth, Force-unauth, Auto.
<b>Oper mode</b>	The port oper mode. Possible values: Authorized, Unauthorized or Down.
<b>Reauth Control</b>	Reauthentication control.
<b>Reauth Period</b>	Reauthentication period.
<b>Username</b>	The username representing the supplicant identity. This field shows the username if the port control is auto. If the port is Authorized, it displays the username of the current user. If the port is Unauthorized, it displays the last user authenticated successfully.
<b>Quiet period</b>	The number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
<b>Tx period</b>	The number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request.
<b>Max req</b>	The maximum number of times that the device sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.
<b>Supplicant timeout</b>	The number of seconds that the device waits for a response to an EAP-request frame from the client before resending the request.
<b>Server timeout</b>	The number of seconds that the device waits for a response from the authentication server before resending the request.
<b>Session Time</b>	The amount of time (HH:MM:SS) that the user is logged in.
<b>MAC address</b>	The supplicant MAC address.
<b>Authentication Method</b>	The authentication method used to establish the session.
<b>Termination Cause</b>	The reason for the session termination.
<b>State</b>	The current value of the Authenticator PAE state machine and of the Backend state machine.

Field	Description
<b>Authentication success</b>	The number of times the state machine received a Success message from the Authentication Server.
<b>Authentication fails</b>	The number of times the state machine received a Failure message from the Authentication Server.

**show dot1x users** Use the **show dot1x users** Privileged EXEC mode command to display active 802.1x authenticated users for the device.

#### SYNTAX

**show dot1x users** [*username username*]

#### PARAMETERS

**username**—Specifies the supplicant username (Length: 1–160 characters)

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example displays 802.1x users.

```
Switch# show dot1x users
Port Username      Session          Auth      MAC      VLAN  Filter
                Time          Method    Address
-----
te1 Bob            1d 03:08:58     Remote    0008.3b79.8787  3
te2 John          08:19:17        None      0008.3b89.3127  2    OK

Port Username      Session          Auth      MAC      VLAN  Filter
                Time          Method    Address
-----
te1 Bob            1d 09:07:38     Remote    0008.3b79.8787  3    OK
te1 Bernie        03:08:58         Remote    0008.3b79.3232  9    OK
te2 John          08:19:17        Remote    0008.3b89.3127  2
te3 Paul          02:12:48         Remote    0008.3b89.8237  8    Warning

Switch# show dot1x users username Bob
Port Username      Session          Auth      MAC      VLAN  Filter
                Time          Method    Address
-----
te1 Bob            1d 09:07:38     Remote    0008.3b79.8787  3    OK
Filter ID #1: Supplicant-IPv4
Filter ID #2: Supplicant-IPv6

Switch# show dot1x users username Bernie
Port Username      Session          Auth      MAC      VLAN  Filter
                Time          Method    Address
-----
te1 Bernard        03:08:58         Remote    0008.3b79.3232  9    OK
Filter ID #1: Supplicant-IPv4
```

**show dot1x statistics** Use the **show dot1x statistics** Privileged EXEC mode command to display 802.1x statistics for the specified interface.

#### SYNTAX

**show dot1x statistics interface** *interface-id*

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example displays 802.1x statistics for tengigabitethernet port 0/1.

```

Console# show dot1x statistics interface tengigabitethernet 0/1

EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:08:78:32:98:78

```

The following table describes the significant fields shown in the display:

Field	Description
<b>EapolFramesRx</b>	The number of valid EAPOL frames of any type that have been received by this Authenticator.
<b>EapolFramesTx</b>	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
<b>EapolStartFramesRx</b>	The number of EAPOL Start frames that have been received by this Authenticator.
<b>EapolLogoffFramesRx</b>	The number of EAPOL Logoff frames that have been received by this Authenticator.
<b>EapolRespIdFramesRx</b>	The number of EAP Resp/Id frames that have been received by this Authenticator.
<b>EapolRespFramesRx</b>	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
<b>EapolReqIdFramesTx</b>	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
<b>EapolReqFramesTx</b>	The number of EAP Request frames (other than Req/Id frames) that have been transmitted by this Authenticator.

Field	Description
<b>InvalidEapolFramesRx</b>	The number of EAPOL frames that have been received by this Authenticator for which the frame type is not recognized.
<b>EapLengthErrorFramesRx</b>	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
<b>LastEapolFrameVersion</b>	The protocol version number carried in the most recently received EAPOL frame.
<b>LastEapolFrameSource</b>	The source MAC address carried in the most recently received EAPOL frame.

**dot1x auth-not-req** Use the **dot1x auth-not-req** Interface Configuration (VLAN) mode command to enable unauthorized devices access to the VLAN. Use the **no** form of this command to disable access to the VLAN.

#### SYNTAX

```
dot1x auth-not-req
no dot1x auth-not-req
```

#### DEFAULT CONFIGURATION

Access is enabled.

#### COMMAND MODE

Interface Configuration (VLAN) mode

#### USER GUIDELINES

An access port cannot be a member in an unauthenticated VLAN.

The native VLAN of a trunk port cannot be an unauthenticated VLAN.

For a general port, the PVID can be an unauthenticated VLAN (although only tagged packets are accepted in the unauthorized state).

#### EXAMPLE

The following example enables unauthorized devices access to VLAN 5.

```
Console(config)# interface vlan 5
Console(config-if)# dot1x auth-not-req
```

**dot1x host-mode** Use the **dot1x host-mode** Interface Configuration mode command to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port. Use the **no** form of this command to return to the default setting.

#### SYNTAX

```
dot1x host-mode {multi-host | single-host | multi-sessions}
```

**PARAMETERS**

- ◆ **multi-host**—Enable multiple-hosts mode.
- ◆ **single-host**—Enable single-hosts mode.
- ◆ **multi-sessions**—Enable multiple-sessions mode.

**DEFAULT**

Default mode is multi-host.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

In multiple hosts mode only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.

In multiple sessions mode each host must be successfully authorized in order to grant network access. Please note that packets are NOT encrypted, and after success full authentication filtering is based on the source MAC address only.

Port security on a port can't be enabled in single-host mode and in multiple-sessions mode.

It is recommended to enable reauthentication when working in multiple-sessions mode in order to detect User Logout for users that hadn't sent Logoff.

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# dot1x host-mode multi-host
console(config-if)# dot1x host-mode single-host
console(config-if)# dot1x host-mode multi-sessions
```

**dot1x violation-mode**

Use the **dot1x violation-mode** Interface Configuration (Ethernet) mode command to configure the action to be taken, when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. Use the **no** form of this command to return to default.

**SYNTAX**

```
dot1x violation-mode {restrict | protect | shutdown}
no dot1x violation-mode
```

**PARAMETERS**

- ◆ **restrict**—Generates a trap when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. The

minimum time between the traps is 1 second. Those frames are forwarded but their source address are not learned.

- ◆ **protect**—Discard frames with source addresses not the supplicant address.
- ◆ **shutdown**—Discard frames with source addresses not the supplicant address and shutdown the port

#### DEFAULT CONFIGURATION

Protect

#### COMMAND MODE

Interface Configuration (Ethernet) mode

#### USER GUIDELINES

The command is relevant for single-host mode.

The command is not relevant for multiple-hosts mode.

The command is relevant for multiple-sessions mode, but you should note that since PCs are sending traffic prior to successful 802.1X authentication, this command might not be useful in this mode.

BPDU message whose MAC address is not the supplicant MAC address wouldn't be discarded in the protect mode.

BPDU message whose MAC address is not the supplicant MAC address would cause a shutdown in the shutdown mode.

#### EXAMPLE

```
console(config)# interface tengigabitethernet tel
console(config-if)# dot1x violation-mode protect
```

**dot1x guest-vlan** Use the **dot1x guest-vlan** Interface Configuration (VLAN) mode command to define a guest VLAN. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
dot1x guest-vlan
no dot1x guest-vlan
```

#### DEFAULT CONFIGURATION

No VLAN is defined as a guest VLAN.

#### COMMAND MODE

Interface Configuration (VLAN) mode

**USER GUIDELINES**

Use the **dot1x guest-vlan enable** Interface Configuration mode command to enable unauthorized users on an interface to access the guest VLAN.

If the guest VLAN is defined and enabled, the port automatically joins the guest VLAN when the port is unauthorized and leaves it when the port becomes authorized. To be able to join or leave the guest VLAN, the port should not be a static member of the guest VLAN.

**EXAMPLE**

The following example defines VLAN 2 as a guest VLAN.

```
Console# configure
Console(config)# interface vlan 2
Console(config-if)# dot1x guest-vlan
```

**dot1x guest-vlan  
timeout**

Use the **dot1x guest-vlan timeout** Global Configuration mode command to set the time delay between enabling 802.1x (or port up) and adding a port to the guest VLAN. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
dot1x guest-vlan timeout timeout
no dot1x guest-vlan timeout
```

**PARAMETERS**

**timeout**—Specifies the time delay in seconds between enabling 802.1x (or port up) and adding the port to the guest VLAN. (Range: 30–180)

**DEFAULT CONFIGURATION**

The guest VLAN is applied immediately.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

This command is relevant if the guest VLAN is enabled on the port. Configuring the timeout adds delay from enabling 802.1X (or port up) to the time the device adds the port to the guest VLAN.

**EXAMPLE**

The following example sets the delay between enabling 802.1x and adding a port to a guest VLAN to 60 seconds.

```
Console(config)# dot1x guest-vlan timeout 60
```

**dot1x guest-vlan enable** Use the **dot1x guest-vlan enable** Interface Configuration (Ethernet) mode command to enable unauthorized users on the interface access to the guest VLAN. Use the **no** form of this command to disable access.

#### SYNTAX

```
dot1x guest-vlan enable
no dot1x guest-vlan enable
```

#### DEFAULT CONFIGURATION

The default configuration is disabled.

#### COMMAND MODE

Interface Configuration (Ethernet) mode

#### USER GUIDELINES

A device can have only one global guest VLAN. The guest VLAN is defined using the **dot1x guest-vlan** Interface Configuration mode command.

#### EXAMPLE

The following example enables unauthorized users on tengigabitethernet port 0/1 to access the guest VLAN.

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# dot1x guest-vlan enable
```

**dot1x mac-authentication** Use the **dot1x mac-authentication** Interface Configuration (Ethernet) mode command to enable authentication based on the station's MAC address. Use the **no** form of this command to disable access.

#### SYNTAX

```
dot1x mac-authentication {mac-only | mac-and-802.1x}
no dot1x mac-authentication
```

#### PARAMETERS

- ◆ **mac-only**—Enables authentication based on the station's MAC address only. 802.1X frames are ignored.
- ◆ **mac-and-802.1x**—Enables 802.1X authentication and MAC address authentication on the interface.

#### DEFAULT CONFIGURATION

Authentication based on the station's MAC address is disabled.

#### COMMAND MODE

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

The guest VLAN must be enabled when MAC authentication is enabled.

Static MAC addresses cannot be authorized. Do not change an authenticated MAC address to a static address.

It is not recommended to delete authenticated MAC addresses.

Reauthentication must be enabled when working in this mode.

**EXAMPLE**

The following example enables authentication based on the station's MAC address on tengigabitethernet port 0/1.

```
Console(config)# interface te1
Console(config-if)# dot1x mac-authentication mac-only
```

**dot1x radius-attributes vlan**

Use the **dot1x radius-attributes vlan** Interface Configuration mode command, to enable user-based VLAN assignment. Use the **no** form of this command to disable user-based VLAN assignment.

**SYNTAX**

```
dot1x radius-attributes vlan
no dot1x radius-attributes vlan
```

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT**

Disabled

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

The configuration of this command is allowed only when the port is Forced Authorized.

Radius attributes are supported only in the multiple sessions mode (multiple hosts with authentication)

When Radius attributes are enabled and the Radius Accept message does not contain the supplicant's VLAN as an attribute, then the supplicant is rejected.

Packets to the supplicant are sent untagged.

After successful authentication the port remains member in the unauthenticated VLANs and in the Guest VLAN. Other static VLAN

configuration is not applied on the port. If the supplicant VLAN does not exist on the switch, the supplicant is rejected.

### EXAMPLE

```
console(config)# interface tel
console(config-if)# dot1x radius-attributes vlan
```

**show dot1x advanced** Use the **show dot1x advanced** Privileged EXEC mode command to display 802.1x advanced features for the device or specified interface.

### SYNTAX

**show dot1x advanced** [*interface-id*]

### PARAMETERS

**interface-id**—Specify an interface ID. The interface ID must be an Ethernet port.

### COMMAND MODE

Privileged EXEC mode

### EXAMPLE

The following example displays 802.1x advanced features for the device.

```
console# show dot1x advanced
Guest VLAN: 3978
Unauthenticated VLANs: 91, 92
Interface Multiple Guest  MAC          VLAN      Legacy-  Policy
           Hosts      VLAN    Authentication  Assignment  supp Mode  Assignment
-----
tel1  Disabled Enabled MAC-and-802.1X  Enabled    Enable    Disabled
tel2  Enabled  Disabled Disabled        Enabled    Enable    Disabled

Switch# show dot1x advanced tengigabitethernet 0/1

Interface Multiple Guest  MAC          VLAN      Legacy-  Policy
           Hosts      VLAN    Authentication  Assignment  sup Mode  Assignment
-----
tel1  Disabled Enabled MAC-and-802.1X  Enabled    Enable
Legacy-Supp mode is disabled
Policy assignment resource err handling: Accept
Single host parameters
Violation action: Discard
Trap: Enabledx
Status: Single-host locked
Violations since last trap: 9
```

# ETHERNET CONFIGURATION COMMANDS

**interface** Use the **interface** Global Configuration mode command to configure an interface and enter interface configuration mode.

## SYNTAX

**interface interface-id**

## PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**interface range** Use the **interface range** command to execute a command on multiple ports at the same time.

## SYNTAX

**interface range interface-id-list**

## PARAMETERS

**interface-id-list**—Specify list of interface IDs. The interface ID can be one of the following types: Ethernet port or Port-channel

## USER GUIDELINES

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

## EXAMPLE

```
console(config)# interface range tel-20
```

**shutdown** Use the **shutdown** Interface Configuration (Ethernet, Port-channel) mode command to disable an interface. Use the **no** form of this command to restart a disabled interface.

## SYNTAX

**shutdown**

**no shutdown**

**DEFAULT CONFIGURATION**

The interface is enabled.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**EXAMPLE**

The following example disables tengigabitethernet port 0/5 operations.

```
Console(config)# interface te5
Console(config-if)# shutdown
Console(config-if)#
```

The following example restarts the disabled Ethernet port.

```
Console(config)# interface te5
Console(config-if)# no shutdown
Console(config-if)
```

**description** Use the **description** Interface Configuration (Ethernet, Port-channel) mode command to add a description to an interface. Use the **no** form of this command to remove the description.

**SYNTAX**

```
description string
no description
```

**PARAMETERS**

**string**—Specifies a comment or a description of the port to assist the user. (Length: 1–64 characters)

**DEFAULT CONFIGURATION**

The interface does not have a description.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**EXAMPLE**

The following example adds the description 'SW#3' to tengigabitethernet port 0/5.

```
Console(config)# interface tengigabitethernet 0/5
Console(config-if)# description SW#3
```

**speed** Use the **speed** Interface Configuration (Ethernet, Port-channel) mode command to configure the speed of a given Ethernet interface when not using auto-negotiation. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
speed {10 | 100 | 1000 | 10000}
no speed
```

#### PARAMETERS

- ◆ **10**—Forces 10 Mbps operation.
- ◆ **100**—Forces 100 Mbps operation.
- ◆ **1000**—Forces 1000 Mbps operation.
- ◆ **10000**—Forces 10000 Mbps operation.

#### DEFAULT CONFIGURATION

The port operates at its maximum speed capability.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-channel) mode

#### USER GUIDELINES

The **no speed** command in a Port-channel context returns each port in the Port-channel to its maximum capability.

#### EXAMPLE

The following example configures the speed of tengigabitethernet port 0/5 to 100 Mbps operation.

```
Console(config)# interface tengigabitethernet 0/5
Console(config-if)# speed 100
```

**flowcontrol** Use the **flowcontrol** Interface Configuration (Ethernet, Port-channel) mode command to configure the flow control on a given interface. Use the **no** form of this command to disable flow control.

#### SYNTAX

```
flowcontrol {auto | on | off}
no flowcontrol
```

#### PARAMETERS

- ◆ **aut**—Specifies auto-negotiation.
- ◆ **on**—Enables flow control.

- ◆ **off**—Disables flow control.

#### DEFAULT CONFIGURATION

Flow control is enabled.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-channel) mode

#### USER GUIDELINES

Use the **negotiation** command to enable **flow control auto**.

#### EXAMPLE

The following example enables flow control on port `te1`

```
Console(config)# interface tengigabitethernet 0/1
Console(config-if)# flowcontrol on
```

**port jumbo-frame** Use the **port jumbo-frame** Global Configuration mode command to enable jumbo frames on the device. Use the **no** form of this command to disable jumbo frames.

#### SYNTAX

```
port jumbo-frame
no port jumbo-frame
```

#### DEFAULT CONFIGURATION

Jumbo frames are disabled on the device.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

This command takes effect only after resetting the device.

#### EXAMPLE

The following example enables jumbo frames on the device.

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

**clear counters** Use the **show interfaces counters** EXEC mode command to display traffic seen by all the physical interfaces or by a specific interface.

#### SYNTAX

```
show interfaces counters [interface-id] [detailed]
```

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**detailed**—Displays information for non-present ports in addition to present ports.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example clears the statistics counters for tengigabitethernet port 0/5.

```
Console# clear counters tengigabitethernet 0/5.
```

**set interface active** Use the **set interface active** EXEC mode command to reactivate an interface that was shut down.

**SYNTAX**

```
set interface active { interface-id }
```

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

This command is used to activate interfaces that were configured to be active, but were shut down by the system.

**EXAMPLE**

The following example reactivates tengigabitethernet port 0/1.

```
Console# set interface active tengigabitethernet 0/1
```

**errdisable recovery cause** Use the **errdisable recovery cause** Global Configuration mode command to enable automatic re-activation of an interface after Err-Disable shutdown. Use the **no** form of this command to disable automatic re-activation.

#### SYNTAX

```
errdisable recovery cause {all | port-security | dot1x-src-address |
acl-deny | stp-bpdu-guard | stp-loopback-guard }
no errdisable recovery cause {all | port-security | dot1x-src-address
| acl-deny | stp-bpdu-guard | stp-loopback-guard }
```

#### PARAMETERS

**all** -Enables the error recovery mechanism for all the reasons

**port-security** - Enables the error recovery mechanism for the Port security Err-Disable state.

**dot1x-src-address**- Enables the error recovery mechanism for the 802.1x Err-Disable state.

**acl-deny**- Enables the error recovery mechanism for the ACL Deny Err-Disable state.

**stp-bpdu-guard**- Enables the error recovery mechanism for the STP BPDU Guard Err-Disable state.

**stp-loopback-guard** - Enables the error recovery mechanism for the STP Loopback Guard Err-Disable state.

#### DEFAULT CONFIGURATION

Automatic re-activation is disabled.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example enables automatic re-activation of an interface after Loopback Detection Err-Disable shutdown.

```
Console(config)# errdisable recovery cause loopback-detection
```

**errdisable recovery interval** Use the **errdisable recovery interval** Global Configuration mode command timeout interval to set the error recovery timeout interval. Use the **no** form of this command to return to the default configuration.

#### SYNTAX

```
errdisable recovery interval seconds
no errdisable recovery interval
```

#### PARAMETERS

**seconds**—Specifies the error recovery timeout interval in seconds. (Range: 30–86400)

#### DEFAULT CONFIGURATION

The default error recovery timeout interval is 300 seconds.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example sets the error recovery timeout interval to 10 minutes.

```
Console(config)# errdisable recovery interval 600
```

**show interfaces configuration** Use the **show interfaces configuration** EXEC mode command to display the configuration for all configured interfaces or for a specific interface.

#### SYNTAX

```
show interfaces configuration [interface-id ]
```

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the configuration of all configured interfaces:

```
console# show interfaces configuration
```

Port	Type	Duplex	Speed	Neg	Flow control	Admin State	Back Pressure	Mdix Mode
te1	1G-Copper	Full	10000	Disabled	Off	Up	Disabled	Off

```

te2 1G-Copper Full 1000 Disabled Off Up Disabled Off
      Flow Admin
Ch   Type   Speed Neg   Control State
-----
Po1                Disabled Off Up

```

**show interfaces status** Use the **show interfaces status** EXEC mode command to display the status of all configured interfaces or of a specific interface.

#### SYNTAX

**show interfaces status** [*interface-id*][*detailed*]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**detailed**—Displays information for non-present ports in addition to present ports.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the status of all configured interfaces.

```

console# show interfaces status
Port   Type      Duplex Speed Neg   Flow Link  Back  Mdix
      ctrl State Pressure Mode
-----
te1 1G-Copper Full 1000 Disabled Off Up Disabled Off
te2 1G-Copper -- -- -- -- Down -- --
      Flow Link
Ch   Type      Duplex Speed Neg   ctrl State
-----
Po1 1G Full 10000 Disabled Off Up

```

**show interfaces advertise** Use the **show interfaces advertise** EXEC mode command to display auto-negotiation advertisement information for all configured interfaces or for a specific interface.

#### SYNTAX

**show interfaces advertise** [*interface-id* |

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

#### COMMAND MODE

EXEC mode

**EXAMPLES**

The following examples display auto-negotiation information.

```

Console# show interfaces advertise

Port      Type           Neg           Operational Link Advertisement
----      -
te1       1G-Copper     Enable       1000f, 100f, 10f, 10h
te2       1G-Copper     Enable       1000f

Console# show interfaces advertise tengigabitethernet 0/1
Port:te1
Type: 1G-Copper
Link state: Up
Auto Negotiation: enabled

                               10h    10f    100h   100f   1000f
                               ---    ---    ----   ----   -----
Admin Local link Advertisement  yes   yes   yes   yes   yes
Oper Local link Advertisement  yes   yes   yes   yes   yes
Remote Local link Advertisement no    no    yes   yes   yes
Priority Resolution             -     -     -     -     yes

Console# show interfaces advertise tengigabitethernet 0/1

Port: te1
Type: 1G-Copper
Link state: Up
Auto negotiation: disabled.

```

**show interfaces description** Use the **show interfaces description** EXEC mode command to display the description for all configured interfaces or for a specific interface.

**SYNTAX**

**show interfaces description** [*interface-id*]

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the description of all configured interfaces.

```

Console# show interfaces description

Port          Descriptions
-----
te1           -----
te1           Port that should be used for management only
te2
te1
te1
te2

Ch            Description
----
Po1           Output

```

**show interfaces counters** Use the **show interfaces counters** EXEC mode command to display traffic seen by all the physical interfaces or by a specific interface.

**SYNTAX**

**show interfaces counters** [*interface-id*]

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays traffic seen by all the physical interfaces.

```

console# show interfaces counters tengigabitethernet 0/
Port          InUcastPkts  InMcastPkts  InBcastPkts  InOctets
-----
te1           0            0            0            0
Port          OutUcastPkts OutMcastPkts OutBcastPkts OutOctets
-----
te1           0            1            35           7051
Alignment Errors: 0
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0

```

```
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

The following table describes the fields shown in the display.

Field	Description
<b>InOctets</b>	The number of received octets.
<b>InUcastPkts</b>	The number of received unicast packets.
<b>InMcastPkts</b>	The number of received multicast packets.
<b>InBcastPkts</b>	The number of received broadcast packets.
<b>OutOctets</b>	The number of transmitted octets.
<b>OutUcastPkts</b>	The number of transmitted unicast packets.
<b>OutMcastPkts</b>	The number of transmitted multicast packets.
<b>OutBcastPkts</b>	The number of transmitted broadcast packets.
<b>FCS Errors</b>	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
<b>Single Collision Frames</b>	The number of frames that are involved in a single collision, and are subsequently transmitted successfully.
<b>Multiple Collision Frames</b>	The number of frames that are involved in more than one collision and are subsequently transmitted successfully.
<b>SQE Test Errors</b>	The number of times that the SQE TEST ERROR is received. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6.
<b>Deferred Transmissions</b>	The number of frames for which the first transmission attempt is delayed because the medium is busy.
<b>Late Collisions</b>	The number of times that a collision is detected later than one slotTime into the transmission of a packet.
<b>Excessive Collisions</b>	The number of frames for which transmission fails due to excessive collisions.
<b>Oversize Packets</b>	The number of frames received that exceed the maximum permitted frame size.
<b>Internal MAC Rx Errors</b>	The number of frames for which reception fails due to an internal MAC sublayer receive error.
<b>Received Pause Frames</b>	The number of MAC Control frames received with an opcode indicating the PAUSE operation.
<b>Transmitted Pause Frames</b>	The number of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

**show port jumbo-frame** Use the **show port jumbo-frame** EXEC mode command to display the configuration of jumbo frames.

#### SYNTAX

**show port jumbo-frame**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the configuration of jumbo frames on the device.

```
Console# show port jumbo-frame

Jumbo frames are disabled
Jumbo frames will be enabled after reset
```

**show errdisable recovery** Use the **show errdisable recovery** EXEC mode command to display the Err-Disable configuration.

**SYNTAX**

**show errdisable recovery**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the Err-Disable configuration.

```
console# show errdisable recovery
Timer interval: 300 Seconds

          Reason                Automatic Recovery
-----
port-security                    Disable
dot1x-src-address                Disable
acl-deny                         Enable
stp-bpdu-guard                  Disable
stp-loopback-guard              Disable
```

**show errdisable interfaces** Use the **show errdisable interfaces** EXEC mode command to display the Err-Disable state of all interfaces or of a specific interface.

**SYNTAX**

**show errdisable interfaces** [*interface-id*]

**PARAMETERS**

- ◆ **interface**—Interface number
- ◆ **Port-channel-number**—Port channel index.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the Err-Disable state of all interfaces.

```

console# show errdisable interfaces
Interface          Reason                Automatic recovery
-----
tel                port-security        No
tel2 acl-deny      Yes

```

**storm-control broadcast enable**

Use the **storm-control broadcast enable** Interface Configuration mode command to enable storm control. Use the **no** form of this command to disable storm control.

**SYNTAX**

**storm-control broadcast enable**  
**no storm-control broadcast enable**

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

Disabled

**COMMAND MODE**

Interface Configuration mode(Ethernet)

**USER GUIDELINES**

- ◆ Use the **storm-control broadcast level** Interface Configuration command to set the maximum rate.
- ◆ Use the **storm-control include-multicast** Interface Configuration command to also count multicast packets and optionally unknown unicast packets in the storm control calculation.
- ◆ Storm control and rate-limit (of unicast packets) cannot be enabled simultaneously on the same port.

**EXAMPLE**

```

console(config)# interface tengigabitethernet 0/1
console(config-if)# storm-control broadcast enable

```

**storm-control broadcast level kbps** Use the **storm-control broadcast level** Interface Configuration mode command to configure the maximum rate of broadcast. Use the **no** form of this command to return to default.

#### SYNTAX

```
storm-control broadcast level kbps kbps
no storm-control broadcast level
```

#### PARAMETERS

**kbps**—Maximum number of kilo bits per second of broadcast traffic on a port. (Range 3K–10G)

#### DEFAULT CONFIGURATION

1000

#### COMMAND MODE

Interface Configuration mode (Ethernet)

#### USER GUIDELINES

Use the **storm-control broadcast enable** Interface Configuration command to enable storm control.

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

#### EXAMPLE

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# storm-control broadcast level kbps 12345
```

**storm-control include-multicast** Use the **storm-control include-multicast** Interface Configuration mode command to count multicast packets in the broadcast storm control. Use the **no** form of this command to disable counting of multicast packets in the broadcast storm control.

#### SYNTAX

```
storm-control include-multicast [unknown-unicast]
no storm-control include-multicast
```

#### PARAMETERS

This command has no arguments or keywords.

**unknown-unicast**—Specifies also the count of unknown unicast packets.

#### DEFAULT CONFIGURATION

Disabled

**COMMAND MODE**

Interface Configuration mode (Ethernet)

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# storm-control include-multicast
```

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

**SYNTAX**

**show storm-control** [*interface-id* ]

**PARAMETERS**

interface-id—Specifies the interface.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

```
console# show storm-control
Port  State  Rate [Kbits/Sec]  Included
-----
tel  Enabled  12345              Broadcast, Multicast,
                               Unknown unicast
te2  Disabled 100000             Broadcast
```

**USER GUIDELINES**

Use the **storm-control broadcast enable** Interface Configuration command to enable storm control.

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

If the suppression level in percentage is translated (for the current port's speed) to a rate that is lower than the minimum rate, the minimum rate would be set.

**EXAMPLE**

```
console(config)# interface tel
console(config-if)# storm-control broadcast level kbps 12345
```

**show fiber-ports optical-transceiver** Use the **show fiber-ports optical-transceiver** EXEC mode command to display the optical transceiver diagnostics.

#### SYNTAX

```
show fiber-ports optical-transceiver [interface interface-id]
[detailed]
```

#### Parameters

- ◆ **interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.
- ◆ **detailed**—Displays detailed diagnostics.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following examples display the optical transceiver diagnostics results.

```
console# show fiber-ports optical-transceiver
```

Port	Temp	Voltage	Current	Output Power	Input Power	LOS
te1	W	OK	OK	OK	OK	OK
te2	OK	OK	OK	E	OK	OK

```
Temp          - Internally measured transceiver temperature
Voltage       - Internally measured supply voltage
Current       - Measured TX bias current
Output Power  - Measured TX output power in milliWatts
Input Power   - Measured RX received power in milliWatts
LOS          - Loss of signal
N/A - Not Available, N/S - Not Supported,
W - Warning, E - Error
```

```
console# show fiber-ports optical-transceiver detailed
```

Port	Temp [C]	Voltage [Volt]	Current [mA]	Output Power [mWatt]	Input Power [mWatt]	LOS
gi0/1	Copper					
gi0/26	Copper					
gi0/27	28	3.32	7.26	3.53	3.68	No
gi0/28	29	3.33	6.50	3.53	3.71	No

```
Temp          - Internally measured transceiver temperature
Voltage       - Internally measured supply voltage
Current       - Measured TX bias current
```

Output Power - Measured TX output power in milliWatts  
Input Power - Measured RX received power in milliWatts  
LOS - Loss of signal  
N/A - Not Available, N/S - Not Supported, W - Warning, E - Error

---

**channel-group** Use the **channel-group** Interface Configuration (Ethernet) mode command to associate a port with a port-channel. Use the **no** form of this command to remove a port from a port-channel.

#### SYNTAX

```
channel-group port-channel mode {on | auto}
```

```
no channel-group
```

#### PARAMETERS

- ◆ **port-channel**—Specifies the port channel number for the current port to join.
- ◆ **mode {on | auto}**—Specifies the mode of joining the port channel. The possible values are:
  - **on**—Forces the port to join a channel without an LACP operation.
  - **auto**—Forces the port to join a channel as a result of an LACP operation.

#### DEFAULT CONFIGURATION

The port is not assigned to a port-channel.

#### COMMAND MODE

Interface Configuration (Ethernet) mode

#### EXAMPLE

The following example forces port `te1` to join port-channel 1 without an LACP operation.

```
Console(config)# interface tengigabitethernet 0/1  
Console(config-if)# channel-group 1 mode on
```

**port-channel load-balance** Use the **port-channel load-balance** Global Configuration mode command to configure the load balancing policy of the port channeling. Use the **no** form of this command to reset to default.

#### SYNTAX

```
port-channel load-balance {src-dst-mac | src-dst-ip | src-dst-mac-ip | }
no port-channel load-balance
```

#### PARAMETERS

- ◆ **src-dst-mac**—Port channel load balancing is based on the source and destination MAC address.
- ◆ **src-dst-ip**—Port channel load balancing is based on the source and destination IP address.
- ◆ **src-dst-mac-ip**—Port channel load balancing is based on the source and destination of MAC and IP addresses.

#### DEFAULT CONFIGURATION

src-dst-mac is the default option.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

In **src-dst-mac-ip-port** load balancing policy, fragmented packets might be reordered.

#### EXAMPLE

```
console#
console# configure
console(config)# port-channel load-balance src-dst-mac
console(config)# port-channel load-balance src-dst-ip
console(config)# port-channel load-balance src-dst-mac-ip
console(config)# port-channel load-balance src-dst-mac-ip-port
console(config)#
```

**show interfaces port-channel** Use the **show interfaces port-channel** EXEC mode command to display port-channel information for all port channels or for a specific port channel.

#### SYNTAX

```
show interfaces port-channel [interface-id]
```

#### PARAMETERS

**interface-id**—Specify an interface ID. The interface ID must be a Port Channel.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays information on all port-channels.

```

console# show interfaces port-channel
Load balancing: src-dst-mac.
Gathering information...
Channel  Ports
-----  -----
Po1      Active: te1,Inactive: te2-3
Po2      Active: te25 Inactive: te24
Po3

console# show interfaces switchport te10
Gathering information...

Name: te10
Switchport: enable
Administrative Mode: access
Operational Mode: down
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs Enabled: 1
                               2-4094 (Inactive)
General PVID: 1
General VLANs Enabled: none
General Egress Tagged VLANs Enabled: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: disabled
Customer Mode VLAN: none
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs Enabled: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN Enabled: none
DVA: disable

```

**bridge multicast filtering** Use the **bridge multicast filtering** Global Configuration mode command to enable the filtering of multicast addresses. Use the **no** form of this command to disable multicast address filtering.

#### SYNTAX

**bridge multicast filtering**  
**no bridge multicast filtering**

#### DEFAULT CONFIGURATION

Multicast address filtering is disabled. All multicast addresses are flooded to all ports.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

If multicast devices exist on the VLAN, do not change the unregistered multicast addresses' states to drop on the device ports.

If multicast devices exist on the VLAN and IGMP-snooping is not enabled, the **bridge multicast forward-all** command should be used to enable forwarding all multicast packets to the multicast switches.

#### EXAMPLE

The following example enables bridge multicast filtering.

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

**bridge multicast mode** Use the **bridge multicast mode** Interface Configuration (VLAN) mode command to configure the multicast bridging mode. Use the **no** form of this command to return to the default configuration.

#### SYNTAX

**bridge multicast mode** {*mac-group* | *ip-group* | *ip-src-group*}  
**no bridge multicast mode**

**PARAMETERS**

- ◆ **mac-group**—Specifies that multicast bridging is based on the packet's VLAN and MAC address.
- ◆ **ipv4-group**—Specifies that multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN and IPv4 destination address for IPv4 packets.
- ◆ **ipv4-src-group**—Specifies that multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN, IPv4 destination address and IPv4 source address for IPv4 packets.

**DEFAULT CONFIGURATION**

The default mode is mac-group.

**COMMAND MODE**

Interface Configuration (VLAN) mode

**USER GUIDELINES**

Use the mac-group mode when using a Network Management System that uses a MIB based on the multicast MAC address. Otherwise, it is recommended to use the ipv4-group or ipv4-src-group mode because there is no overlapping of IPv4 multicast addresses in these modes.

For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries in the FDB, as described in the following table:

FDB mode	CLI commands	
<b>mac-group</b>	bridge multicast address	bridge multicast forbidden address
<b>ipv4-group</b>	bridge multicast ip-address	bridge multicast forbidden ip-address
<b>ipv4-src-group</b>	bridge multicast source group	bridge multicast forbidden source group

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the IGMP version that is used in the network:

FDB mode	IGMP version 2	IGMP version 3
<b>mac-group</b>	MAC group address	MAC group address
<b>ipv4-group</b>	IP group address	IP group address
<b>ipv4-src-group</b>	(*)	IP source and group addresses

(\*) Note that (\*,G) cannot be written to the FDB if the mode is **ipv4-src-group**. In that case, no new FDB entry is created, but the port is added to the static (S,G) entries (if they exist) that belong to the requested group. It is recommended to set the FDB mode to ipv4-group or mac-group for IGMP version 2.

If an application on the device requests (\*,G), the operating FDB mode is changed to ipv4-group.

#### EXAMPLE

The following example configures the multicast bridging mode as ipv4-group on VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast mode ipv4-group
```

### bridge multicast address

Use the **bridge multicast address** Interface Configuration (VLAN) mode command to register a MAC-layer multicast address in the bridge table and statically add or remove ports to or from the group. Use the **no** form of this command to unregister the MAC address.

#### SYNTAX

```
bridge multicast address {mac-multicast-address} [[add | remove]
  {ethernet interface-list | port-channel port-channel-list}]
no bridge multicast address {mac-multicast-address}
```

#### PARAMETERS

- ◆ **mac-multicast-address**—Specifies the group MAC multicast address.
- ◆ **add**—Adds ports to the group.
- ◆ **remove**—Removes ports from the group.
- ◆ **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ◆ **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

#### DEFAULT CONFIGURATION

No multicast addresses are defined.

If **ethernet interface-list** or **port-channel port-channel-list** is specified without specifying **add** or **remove**, the default option is **add**.

#### COMMAND MODE

Interface Configuration (VLAN) mode

#### USER GUIDELINES

To register the group in the bridge database without adding or removing ports or port channels, specify the **mac-multicast-address** parameter only.

Static multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

#### EXAMPLE

The following example registers the MAC address to the bridge table:

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
```

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

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03 add te1-2
```

### bridge multicast forbidden address

Use the **bridge multicast forbidden address** Interface Configuration (VLAN) mode command to forbid adding or removing a specific multicast address to or from specific ports. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
bridge multicast forbidden address {mac-multicast-address} {add
| remove} {ethernet interface-list | port-channel port-channel-list}
no bridge multicast forbidden address {mac-multicast-address}
```

#### PARAMETERS

- ◆ **mac-multicast-address**—Specifies the group MAC multicast address.
- ◆ **add**—Forbids adding ports to the group.
- ◆ **remove**—Forbids removing ports from the group.
- ◆ **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ◆ **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

#### DEFAULT CONFIGURATION

No forbidden addresses are defined.

#### COMMAND MODE

Interface Configuration (VLAN) mode

**USER GUIDELINES**

Before defining forbidden ports, the multicast group should be registered.

You can execute the command before the VLAN is created.

**EXAMPLE**

The following example forbids MAC address 0100.5e02.0203 on port 9 within VLAN 8.

```

Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 0100.5e.02.0203
Console(config-if)# bridge multicast forbidden address 0100.5e02.0203 add te9

```

**bridge multicast  
forbidden ip-  
address**

Use the **bridge multicast forbidden ip-address** Interface Configuration (VLAN) mode command to forbid adding or removing a specific IP multicast address to or from specific ports. Use the no form of this command to restore the default configuration.

**SYNTAX**

```

bridge multicast forbidden ip-address {ip-multicast-address} {add
| remove} {ethernet interface-list | port-channel port-channel-list}
no bridge multicast forbidden ip-address {ip-multicast-address}

```

**PARAMETERS**

- ◆ **ip-multicast-address**—Specifies the group IP multicast address.
- ◆ **add**—Forbids adding ports to the group.
- ◆ **remove**—Forbids removing ports from the group.
- ◆ **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ◆ **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

**DEFAULT CONFIGURATION**

No forbidden addresses are defined.

**COMMAND MODE**

Interface Configuration (VLAN) mode

**USER GUIDELINES**

Before defining forbidden ports, the multicast group should be registered.

You can execute the command before the VLAN is created.

**EXAMPLE**

The following example registers IP address 239.2.2.2, and forbids the IP address on port `te9` within VLAN 8.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast ip-address 239.2.2.2
Console(config-if)# bridge multicast forbidden ip-address 239.2.2.2 add te9
```

**bridge multicast source group**

Use the **bridge multicast source group** Interface Configuration (VLAN) mode command to register a source IP address - multicast IP address pair to the bridge table, and statically add or remove ports to or from the source-group. Use the `no` form of this command to unregister the source-group-pair.

**SYNTAX**

```
bridge multicast source ip-address group ip-multicast-address
[[add | remove] { ethernet interface-list | port-channel port-channel-list}]
```

```
no bridge multicast source ip-address group ip-multicast-address
```

**PARAMETERS**

- ◆ **ip-address**—Specifies the source IP address.
- ◆ **ip-multicast-address**—Specifies the group IP multicast address.
- ◆ **add**—Adds ports to the group for the specific source IP address.
- ◆ **remove**—Removes ports from the group for the specific source IP address.
- ◆ **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ◆ **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

**DEFAULT CONFIGURATION**

No multicast addresses are defined.

If **ethernet interface-list** or **port-channel port-channel-list** is specified without specifying **add** or **remove**, the default option is **add**.

**COMMAND MODE**

Interface Configuration (VLAN) mode

**USER GUIDELINES**

You can execute the command before the VLAN is created.

**EXAMPLE**

The following example registers a source IP address - multicast IP address pair to the bridge table:

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast source 239.2.2.2 group 239.2.2.2
```

### bridge multicast forbidden source group

Use the **bridge multicast forbidden source group** Interface Configuration (VLAN) mode command to forbid adding or removing a specific IP source address - multicast address pair to or from specific ports. Use the no form of this command to return to the default configuration.

**SYNTAX**

```
bridge multicast forbidden source ip-address group ip-multicast-  
address {add | remove} {ethernet interface-list | port-channel  
port-channel-list}
```

```
no bridge multicast forbidden source ip-address group ip-  
multicast-address
```

**PARAMETERS**

- ◆ **ip-address**—Specifies the source IP address.
- ◆ **ip-multicast-address**—Specifies the group IP multicast address.
- ◆ **add**—Forbids adding ports to the group for the specific source IP address.
- ◆ **remove**—Forbids removing ports from the group for the specific source IP address.
- ◆ **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ◆ **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

**DEFAULT CONFIGURATION**

No forbidden addresses are defined.

**COMMAND MODE**

Interface Configuration (VLAN) mode

**USER GUIDELINES**

Before defining forbidden ports, the multicast group should be registered.

You can execute the command before the VLAN is created.

**EXAMPLE**

The following example registers a source IP address - multicast IP address pair to the bridge table, and forbids adding the pair to tengigabitethernet port te9 on VLAN 8:

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast source 13.16.1.1 group 239.2.2.2
Console(config-if)# bridge multicast forbidden source 13.16.1.1 group
239.2.2.2 add te9
```

**bridge multicast  
ipv6 mode**

Use the **bridge multicast ipv6 mode** Interface Configuration (VLAN) mode command to configure the multicast bridging mode for ipv6 multicast packets. Use the no form of this command to return to the default configuration.

**SYNTAX**

**bridge multicast ipv6 mode** {*mac-group* | *ip-group* | *ip-src-group*}  
**no bridge multicast ipv6 mode**

**PARAMETERS**

- ◆ **mac-group**—Specifies that multicast bridging is based on the packet's VLAN and MAC address.
- ◆ **ip-group**—Specifies that multicast bridging is based on the packet's VLAN and IPv6 destination address for IPv6 packets.
- ◆ **ip-src-group**—Specifies that multicast bridging is based on the packet's VLAN, IPv6 destination address and IPv6 source address for IPv6 packets.

**DEFAULT CONFIGURATION**

The default mode is mac-group.

**COMMAND MODE**

Interface Configuration (VLAN) mode

**USER GUIDELINES**

Use the **mac-group** mode when using a Network Management System that uses a MIB based on the multicast MAC address.

For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries for IPv6 multicast addresses in the FDB, as described in the following table:

FDB mode	CLI commands	
<b>mac-group</b>	bridge multicast address	bridge multicast forbidden address

FDB mode	CLI commands	
<b>ipv4-group</b>	bridge multicast ipv6 ip-address	bridge multicast ipv6 forbidden ip-address
<b>ipv4-src-group</b>	bridge multicast ipv6 source group	bridge multicast ipv6 forbidden source group

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the MLD version that is used in the network:

FDB mode	MLD version 1	MLD version 2
<b>mac-group</b>	MAC group address	MAC group address
<b>ipv4-group</b>	IP group address	IP group address
<b>ipv4-src-group</b>	(*)	IP source and group addresses

(\*) Note that (\*,G) cannot be written to the FDB if the mode is **ip-src-group**. In that case, no new FDB entry is created, but the port is added to the (S,G) entries (if they exist) that belong to the requested group. If an application on the device requests (\*,G), the operating FDB mode is changed to **ip-group**.

- ◆ You can execute the command before the VLAN is created.

#### EXAMPLE

The following example configures the multicast bridging mode as **ip-group** on VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast ipv6 mode ip-group
```

### bridge multicast ipv6 forbidden ip- address

Use the **bridge multicast ipv6 forbidden ip-address** Interface Configuration (VLAN) mode command to forbid adding or removing a specific IPv6 multicast address to or from specific ports. To restore the default configuration, use the **no** form of this command.

#### SYNTAX

```
bridge multicast ipv6 forbidden ip-address {ipv6-multicast-address} {add | remove} {ethernet interface-list | port-channel port-channel-list}
```

```
no bridge multicast ipv6 forbidden ip-address {ipv6-multicast-address}
```

#### PARAMETERS

- ◆ **ipv6-multicast-address**—Specifies the group IPv6 multicast address.
- ◆ **add**—Forbids adding ports to the group.

- ◆ **remove**—Forbids removing ports from the group.
- ◆ **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ◆ **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

#### DEFAULT CONFIGURATION

No forbidden addresses are defined.

#### COMMAND MODE

Interface Configuration (VLAN) mode

#### USER GUIDELINES

Before defining forbidden ports, the multicast group should be registered.

You can execute the command before the VLAN is created.

#### EXAMPLE

The following example registers an IPv6 multicast address, and forbids the IPv6 address on port 9 within VLAN 8.

```
console(config)# interface vlan 8
Console(config-if)# bridge multicast ipv6 ip-address FE02:0:0:0:4:4:4
Console(config-if)# bridge multicast ipv6 forbidden ip-address
FE02:0:0:0:4:4:4 add te9
```

### bridge multicast ipv6 source group

Use the **bridge multicast ipv6 source group** Interface Configuration (VLAN) mode command to register a source IPv6 address - multicast IPv6 address pair to the bridge table, and statically add or remove ports to or from the source-group. Use the **no** form of this command to unregister the source-group-pair.

#### SYNTAX

```
bridge multicast ipv6 source ipv6-source-address group ipv6-multicast-address [[add | remove] { ethernet interface-list | port-channel port-channel-list}]
```

```
no bridge multicast ipv6 source ipv6-address group ipv6-multicast-address
```

#### PARAMETERS

- ◆ **ipv6-source-address**—Specifies the source IPv6 address.
- ◆ **ipv6-multicast-address**—Specifies the group IPv6 multicast address.
- ◆ **add**—Adds ports to the group for the specific source IPv6 address.

- ◆ **remove**—Removes ports from the group for the specific source IPv6 address.
- ◆ **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ◆ **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

#### DEFAULT CONFIGURATION

No multicast addresses are defined.

If **ethernet interface-list** or **port-channel port-channel-list** is specified without specifying **add** or **remove**, the default option is **add**.

You can execute the command before the VLAN is created.

#### COMMAND MODE

Interface Configuration (VLAN) mode

#### EXAMPLE

The following example registers a source IPv6 address - multicast IPv6 address pair to the bridge table:

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast source FE02:0:0:0:4:4:4 group
FE02:0:0:0:4:4:4
```

### bridge multicast ipv6 forbidden source group

Use the **bridge multicast ipv6 forbidden source group** Interface Configuration (VLAN) mode command to forbid adding or removing a specific IP source address - multicast address pair to or from specific ports. Use the **no** form of this command to return to the default configuration.

#### SYNTAX

```
bridge multicast ipv6 forbidden source ipv6-source-address group
ipv6-multicast-address {add | remove} {interface-list | port-
channel port-channel-list}
```

```
no bridge multicast ipv6 forbidden source ipv6-address group
ipv6-multicast-address
```

#### PARAMETERS

- ◆ **ipv6-source-address**—Specifies the source IPv6 address.
- ◆ **ipv6-multicast-address**—Specifies the group IPv6 multicast address.
- ◆ **add**—Forbids adding ports to the group for the specific source IPv6 address.

- ◆ **remove**—Forbids removing ports from the group for the specific source IPv6 address.
- ◆ **interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ◆ **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

#### DEFAULT CONFIGURATION

No forbidden addresses are defined.

#### COMMAND MODE

Interface Configuration (VLAN) mode

#### USER GUIDELINES

Before defining forbidden ports, the multicast group should be registered.

You can execute the command before the VLAN is created.

#### EXAMPLE

The following example registers a source IPv6 address - multicast IPv6 address pair to the bridge table, and forbids adding the pair to tengigabitethernet 0/9 on VLAN 8:

```

Console(config)# interface vlan 8
Console(config-if)# bridge multicast source FE02:0:0:0:4:4:4 group
FE02:0:0:0:4:4:4
Console(config-if)# bridge multicast forbidden source FE02:0:0:0:4:4:4 group
FE02:0:0:0:4:4:4 add te9

```

### bridge multicast unregistered

Use the **bridge multicast unregistered** Interface Configuration (Ethernet, Port-Channel) mode command to configure the forwarding state of unregistered multicast addresses. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```

bridge multicast unregistered {forwarding | filtering}
no bridge multicast unregistered

```

#### PARAMETERS

- ◆ **forwarding**—Forwards unregistered multicast packets.
- ◆ **filtering**—Filters unregistered multicast packets.

#### DEFAULT CONFIGURATION

Unregistered multicast addresses are forwarded.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-Channel) mode

**USER GUIDELINES**

Do not enable unregistered multicast filtering on ports that are connected to routers, because the 224.0.0.x address range should not be filtered. Note that routers do not necessarily send IGMP reports for the 224.0.0.x range.

You can execute the command before the VLAN is created.

**EXAMPLE**

The following example specifies that unregistered multicast packets are filtered on tengigabitethernet port 0/1:

```
Console(config)# interface te1
Console(config-if)# bridge multicast unregistered filtering
```

**bridge multicast forward-all**

Use the **bridge multicast forward-all** Interface Configuration (VLAN) mode command to enable forwarding all multicast packets for a range of ports or port channels. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**bridge multicast forward-all** {*add* | *remove*} {*ethernet interface-list* | *port-channel port-channel-list*}

**no bridge multicast forward-all**

**PARAMETERS**

- ◆ **add**—Forces forwarding of all multicast packets.
- ◆ **remove**—Does not force forwarding of all multicast packets.
- ◆ **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ◆ **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

**DEFAULT CONFIGURATION**

Forwarding of all multicast packets is disabled.

**COMMAND MODE**

Interface Configuration (VLAN) mode

**EXAMPLE**

The following example enables all multicast packets on port te8 to be forwarded.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forward-all add te8
```

### bridge multicast forbidden forward- all

Use the **bridge multicast forbidden forward-all** Interface Configuration (VLAN) mode command to forbid a port to dynamically join multicast groups. Use the no form of this command to restore the default configuration.

**SYNTAX**

**bridge multicast forbidden forward-all** *{add | remove}* *{ethernet interface-list | port-channel port-channel-list}*

**no bridge multicast forbidden forward-all**

**PARAMETERS**

- ◆ **add**—Forbids forwarding of all multicast packets.
- ◆ **remove**—Does not forbid forwarding of all multicast packets.
- ◆ **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ◆ **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

**DEFAULT CONFIGURATION**

Ports are not forbidden to dynamically join multicast groups.

**COMMAND MODE**

Interface Configuration (VLAN) mode

**USER GUIDELINES**

Use this command to forbid a port to dynamically join (by IGMP, for example) a multicast group.

The port can still be a multicast router port.

**EXAMPLE**

The following example forbids forwarding of all multicast packets to te1 within VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forbidden forward-all add ethernet te1
```

**mac address-table static**

Use the **mac address-table static** Global Configuration mode command to add MAC-layer station source address to the MAC address table. Use the **no** form of this command to delete the MAC address.

**SYNTAX**

```
mac address-table static mac-address vlan vlan-id interface
interface-id [permanent | delete-on-reset | delete-on-timeout |
secure ]
```

```
no mac address-table static [mac-address] vlan vlan-id
```

**PARAMETERS**

**mac-address**—AC address (Range: Valid MAC address)

**vlan-id**—Specify the VLAN

**interface-id**—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel (Range: Valid Ethernet port, Valid Port-channel number)

**permanent**—The address can only be deleted by the **no bridge address** command.

**delete-on-reset**—The address is deleted after reset.

**delete-on-timeout**—The address is deleted after aged out.

**secure**—The address is deleted after the port changes mode to unlock learning (no port security command). Available only when the port is in learning locked mode.

**DEFAULT CONFIGURATION**

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

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

```
console(config)# mac address-table static 00:3f:bd:45:5a:b1 vlan 1 te1
```

**clear mac address-table** Use the **clear mac address-table** Privileged EXEC command to remove learned or secure entries from the forwarding database.

#### SYNTAX

```
clear mac address-table dynamic [ interface interface-id ]
clear mac address-table secure interface interface-id
```

#### PARAMETERS

**interface interface-id**—Delete all dynamic address on the specified interface. The interface ID can be one of the following types: Ethernet port or port-channel.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

```
console# clear mac address-table dynamic
```

**mac address-table aging-time** Use the **mac address-table aging-time** global configuration command to set the aging time of the address table. Use the **no** form of this command to restore the default.

#### SYNTAX

```
mac address-table aging-time seconds
no mac address-table aging-time
```

#### PARAMETERS

**seconds**—Time is number of seconds. (Range:10–300)

#### DEFAULT CONFIGURATION

300

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

```
console(config)# mac address-table aging-time 600
```

**port security** Use the **port security** Interface Configuration (Ethernet, Port-channel) mode command to enable port security on an interface. Use the **no** form of this command to disable port security on an interface.

#### SYNTAX

```
port security [forward | discard | discard-shutdown] [trap seconds]  
no port security
```

#### PARAMETERS

- ◆ **forward**—Forwards packets with unlearned source addresses, but does not learn the address.
- ◆ **discard**—Discards packets with unlearned source addresses.
- ◆ **discard-shutdown**—Discards packets with unlearned source addresses and shuts down the port.
- ◆ **trap seconds**—Sends SNMP traps and specifies the minimum time interval in seconds between consecutive traps. (Range: 1–1000000)

#### DEFAULT CONFIGURATION

The feature is disabled

The default mode is discard.

#### COMMAND MODE

Interface Configuration (Ethernet, port-channel) mode

#### EXAMPLE

The following example forwards all packets to port te1 without learning addresses of packets from unknown sources and sends traps every 100 seconds if a packet with an unknown source address is received.

```
console(config)# tengigabitethernet 0/1  
Console(config-if)# port security forward trap 100
```

**port security mode** Use the **port security mode** Interface Configuration (Ethernet, port-channel) mode command configures the port security learning mode. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
port security mode {lock | max-addresses }  
no port security mode
```

#### PARAMETERS

- ◆ **lock**—Saves the current dynamic MAC addresses associated with the port and disables learning, relearning and aging.

- ◆ **max-addresses**—Deletes the current dynamic MAC addresses associated with the port and learns up to the maximum number of addresses allowed on the port. Relearning and aging are enabled.

#### DEFAULT CONFIGURATION

The default port security mode is lock.

#### COMMAND MODE

Interface Configuration (Ethernet, port-channel) mode

#### EXAMPLE

The following example sets the port security mode to dynamic for tengigabitethernet interface 0/7.

```
Console(config)# interface tengigabitethernet 0/7
Console(config-if)# port security mode dynamic
```

**port security max** Use the **port security mode** Interface Configuration (Ethernet, Port-channel) mode command to configure the maximum number of addresses that can be learned on the port while the port is in port security max-addresses mode. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
port security max {max-addr}
no port security max
```

#### PARAMETERS

**max-addr**—Specifies the maximum number of addresses that can be learned on the port. (Range: 0–128)

#### DEFAULT CONFIGURATION

This default maximum number of addresses is 1.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-channel) mode

#### USER GUIDELINES

This command is relevant in port security max-addresses mode only.

#### EXAMPLE

```
Console(config)# interface tengigabitethernet 0/1
Console(config-if)# port security max 20
```

**port security routed secure-address** Use the **port security routed secure-address** Interface Configuration (Ethernet, Port-channel) mode command to add a MAC-layer secure address to a routed port. Use the no form of this command to delete a MAC address from a routed port.

#### SYNTAX

```
port security routed secure-address mac-address
no port security routed secure-address [mac-address]
```

#### PARAMETERS

**mac-address**—Specifies the MAC address.

#### DEFAULT CONFIGURATION

No addresses are defined.

#### COMMAND MODE

Interface Configuration (Ethernet, port-channel) mode. It cannot be configured for a range of interfaces (range context).

#### USER GUIDELINES

This command enables adding secure MAC addresses to a routed port in port security mode. The command is available when the port is a routed port and in port security mode. The address is deleted if the port exits the security mode or is not a routed port.

This command is required because the **bridge address** command cannot be executed on internal VLANs.

#### EXAMPLE

The following example adds the MAC-layer address 66:66:66:66:66:66 to tengigabitethernet port 0/1.

```
Console(config)# interface tengigabitethernet 0/1
Console(config-if)# port security routed secure-address 66:66:66:66:66:66
```

**show mac address-table** Use the **show mac address-table** EXEC command to view entries in the MAC address table.

#### SYNTAX

```
show mac address-table [dynamic | static | secure] [vlan vlan]
[interface interface-id] [address mac-address]
```

#### PARAMETERS

- ◆ **dynamic**—Displays only dynamic MAC address table entries.
- ◆ **static**—Displays only static MAC address table entries.
- ◆ **secure**—Displays only secure MAC address table entries.

- ◆ **vlan**—Specifies VLAN, such as VLAN 1.
- ◆ **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- ◆ **mac-address**—MAC address.

#### DEFAULT

#### COMMAND MODE

EXEC mode

#### USER GUIDELINES

Internal usage VLANs (VLANs that are automatically allocated on routed ports) are presented in the VLAN column by a port number and not by a VLAN ID.

#### EXAMPLE

```

Console# show mac address-table
Aging time is 300 sec
VLAN          MAC Address          Port          Type
-----
1             00:00:26:08:13:23    0             self
1             00:3f:bd:45:5a:b1    te1           static
1             00:a1:b0:69:63:f3    te24          dynamic
2             00:a1:b0:69:63:f3    te24          dynamic

Console# show mac address-table 00:3f:bd:45:5a:b1
Aging time is 300 sec
VLAN          MAC Address          Port          Type
-----
1             00:3f:bd:45:5a:b1    te9           static

```

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

#### SYNTAX

**show mac address-table count** [*vlan vlan* | *interface interface-id*]

#### PARAMETERS

- ◆ **vlan**—Specifies VLAN.
- ◆ **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

#### COMMAND MODE

EXEC mode

**EXAMPLE**

```

Console# show mac address-table count

Capacity: 8192
Free: 8083
Used: 109

Static addresses: 2
Secure addresses: 1
Dynamic addresses: 97
Internal addresses: 9

```

**show bridge multicast mode** Use the **show bridge multicast mode** EXEC mode command to display the multicast bridging mode for all VLANs or for a specific VLAN.

**SYNTAX**

```
show bridge multicast mode [vlan vlan-id]
```

**PARAMETERS**

**vlan vlan-id**—Specifies the VLAN ID.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the multicast bridging mode for all VLANs.

```

Console# show bridge multicast mode

VLAN      IPv4 Multicast mode          IPv6 Multicast mode
          Admin      Oper      Admin      Oper
-----  -
1         MAC-GROUP  MAC-GROUP  MAC-GROUP  MAC-GROUP
11        IPv4-GROUP IPv4-GROUP IPv6-GROUP  IPv6-GROUP
12        IPv4-SRC-GROUP IPv4-SRC-GROUP IPv6-SRC-GROUP IPv6-SRC-GROUP

```

**show bridge multicast address-table** Use the **show bridge multicast address-table** EXEC mode command to display multicast MAC address or IP address table information.

**SYNTAX**

```
show bridge multicast address-table [vlan vlan-id] [address {mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address}] [format {ip | mac}] [source {ipv4-source-address | ipv6-source-address}]
```

**PARAMETERS**

◆ **vlan vlan-id**—Specifies the VLAN ID.

- ◆ **address {mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address}**—Specifies the multicast address. The possible values are:
  - ◆ **mac-multicast-address**—Specifies the MAC multicast address.
  - ◆ **ipv4-multicast-address**—Specifies the IPv4 multicast address.
  - ◆ **ipv6-multicast-address**—Specifies the IPv6 multicast address.
- ◆ **format {ip | mac}**—Specifies the multicast address format. The possible values are:
  - ◆ **ip**—Specifies that the multicast address is an IP address.
  - ◆ **mac**—Specifies that the multicast address is a MAC address.
- ◆ **source {ipv4-source-address | ipv6-source-address}**—Specifies the source address. The possible values are:
  - **ipv4-address**—Specifies the source IPv4 address.
  - **ipv6-address**—Specifies the source IPv6 address.

#### DEFAULT CONFIGURATION

If the format is not specified, it defaults to mac.

#### COMMAND MODE

EXEC mode

#### USER GUIDELINES

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000 through 0100.5e7f.ffff.

Multicast Router ports (defined statically or discovered dynamically) are members in all MC groups.

Ports that were defined via **bridge multicast forbidden forward-all** command are displayed in all forbidden MC entries.

#### EXAMPLE

The following example displays bridge multicast address information.

```
Console# show bridge multicast address-table
```

```
Multicast address table for VLANs in MAC-GROUP bridging mode:
```

Vlan	MAC Address	Type	Ports
8	01:00:5e:02:02:03	Static	1-2

```
Forbidden ports for multicast addresses:
```

```

Vlan    MAC Address      Ports
-----
8       01:00:5e:02:02:03  te9

```

Multicast address table for VLANs in IPv4-GROUP bridging mode:

```

Vlan    MAC Address      Type           Ports
-----
1       224.0.0.251      Dynamic       te12

```

Forbidden ports for multicast addresses:

```

Vlan    MAC Address      Ports
-----
1       232.5.6.5
1       233.22.2.6

```

Multicast address table for VLANs in IPv4-SRC-GROUP bridging mode:

```

Vlan  Group Address  Source address  Type       Ports
-----
1     224.2.2.251    11.2.2.3      Dynamic    te11

```

Forbidden ports for multicast addresses:

```

Vlan  Group Address  Source Address  Ports
-----
8     239.2.2.2      *              te9
8     239.2.2.2      1.1.1.11      te9

```

Multicast address table for VLANs in IPv6-GROUP bridging mode:

```

VLAN  IP/MAC Address  Type           Ports
-----
8     ff02::4:4:4    Static         te1-2,te7,Po1

```

Forbidden ports for multicast addresses:

```

VLAN  IP/MAC Address  Ports
-----
8     ff02::4:4:4    te9

```

Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:

```

Vlan  Group Address  Source address  Type       Ports
-----
8     ff02::4:4:4    *              Static     tel-2,te7,Po1
8     ff02::4:4:4    fe80::200:7ff:fe00:200  Static

```

Forbidden ports for multicast addresses:

```

Vlan  Group Address  Source address  Ports
-----
8     ff02::4:4:4    *              te9
8     ff02::4:4:4    fe80::200:7ff:fe00:200  te9

```

**show bridge multicast address-table static** Use the **show bridge multicast address-table static** EXEC mode command to display the statically configured multicast addresses.

#### SYNTAX

```
show bridge multicast address-table static [vlan vlan-id] [address mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address] [source ipv4-source-address | ipv6-source-address] [all | mac | ip]
```

#### PARAMETERS

- ◆ **vlan vlan-id**—Specifies the VLAN ID.
- ◆ **address {mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address}**—Specifies the multicast address. The possible values are:
  - **mac-multicast-address**—Specifies the MAC multicast address.
  - **ipv4-multicast-address**—Specifies the IPv4 multicast address.
  - **ipv6-multicast-address**—Specifies the IPv6 multicast address.
- ◆ **source {ipv4-source-address | ipv6-source-address}**—Specifies the source address. The possible values are:
  - **ipv4-address**—Specifies the source IPv4 address.
  - **ipv6-address**—Specifies the source IPv6 address.

#### DEFAULT CONFIGURATION

When all/mac/ip is not specified, all entries (mac and ip) will be displayed.

#### COMMAND MODE

EXEC mode

#### USER GUIDELINES

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000-- 0100.5e7f.ffff.

#### EXAMPLE

The following example displays the statically configured multicast addresses.

```
Console# show bridge multicast address-table static

MAC-GROUP table

Vlan      MAC Address      Ports
----      -
1         0100.9923.8787   te1, te2
```

Forbidden ports for multicast addresses:

Vlan	MAC Address	Ports
----	-----	-----

IPv4-GROUP Table

Vlan	IP Address	Ports
----	-----	-----
1	231.2.2.3	te1, te2
19	231.2.2.8	te1-8
19	231.2.2.8	te9-11

Forbidden ports for multicast addresses:

Vlan	IP Address	Ports
----	-----	-----
1	231.2.2.3	te8
19	231.2.2.8	te8

IPv4-SRC-GROUP Table:

Vlan	Group Address	Source address	Ports
----	-----	-----	-----

Forbidden ports for multicast addresses:

Vlan	Group Address	Source address	Ports
----	-----	-----	-----

IPv6-GROUP Table

Vlan	IP Address	Ports
----	-----	-----
191	FF12::8	te1-8

Forbidden ports for multicast addresses:

Vlan	IP Address	Ports
----	-----	-----
11	FF12::3	te8
191	FF12::8	te8

IPv6-SRC-GROUP Table:

Vlan	Group Address	Source address	Ports
----	-----	-----	-----
192	FF12::8	FE80::201:C9A9:FE40:8988	te1-8

Forbidden ports for multicast addresses:

Vlan	Group Address	Source address	Ports
----	-----	-----	-----
192	FF12::3	FE80::201:C9A9:FE40:8988	te8

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

**SYNTAX**

**show bridge multicast filtering** *vlan-id*

**PARAMETERS**

**vlan-id**—Specifies the VLAN ID. (Range: Valid VLAN)

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the multicast configuration for VLAN 1.

```

Console# show bridge multicast filtering 1

Filtering: Enabled

VLAN: 1

Port          Forward-All Static   Status
-----
te1           Forbidden           Filter
te2           Forward             Forward(s)
te3           -                   Forward(d)

```

**show bridge multicast unregistered** Use the **show bridge multicast unregistered** EXEC mode command to display the unregistered multicast filtering configuration.

**SYNTAX**

**show bridge multicast unregistered** [*interface-id*]

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the unregistered multicast configuration.

```
Console# show bridge multicast unregistered
```

```
Port          Unregistered
-----
te1           Forward
te2           Filter
te3           Filter
```

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

**SYNTAX**

```
show ports security [interface-id]
```

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the port-lock status of all ports.

```
console# show ports security
```

```
Port   Status   Learning   Action   Max   Trap   Frequency
-----
te1    Enabled  Max-      Discard  3    Enabled  100
        Addresses
te2    Disabled Max-      -        28   -        -
        Addresses
te3    Enabled  Lock      Discard,  8    Disabled -
        Shutdown
```

The following table describes the fields shown above.

Field	Description
<b>Port</b>	The port number.
<b>Status</b>	The port security status. The possible values are: Enabled or Disabled.
<b>Mode</b>	The port security mode.

Field	Description
<b>Action</b>	The action taken on violation.
<b>Maximum</b>	The maximum number of addresses that can be associated on this port in the Max-Addresses mode.
<b>Trap</b>	The status of SNMP traps. The possible values are: Enable or Disable.
<b>Frequency</b>	The minimum time interval between consecutive traps.

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

#### SYNTAX

**show ports security addresses** [*interface-id*]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example displays dynamic addresses in all currently locked ports.

```

Console# show ports security addresses

Port          Status      Learning      Current      Maximum
----          -
te1           Enabled     Max-addresses 2            3
te2           Disabled    Max-addresses -            128
te3           Enabled     Lock          NA           NA

```

**port monitor** Use the **port monitor** Interface Configuration (Ethernet) mode command to start a port monitoring session. Use the **no** form of this command to stop a port monitoring session.

#### SYNTAX

**port monitor** *src-interface-id* [*rx* | *tx*]

**no port monitor** *src-interface-id*

**port monitor** *vlan* *vlan-id*

**no port monitor** *vlan* *vlan-id*

#### PARAMETERS

- ◆ **rx**—Monitors received packets only. If no option is specified, it monitors both rx and tx.
- ◆ **tx**—Monitors transmitted packets only. If no option is specified, it monitors both rx and tx.
- ◆ **vlan** **vlan-id**—VLAN number
- ◆ **src-interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

#### DEFAULT CONFIGURATION

Monitors both received and transmitted packets.

#### COMMAND MODE

Interface Configuration (Ethernet) mode. It cannot be configured for a range of interfaces (range context).

#### USER GUIDELINES

This command enables port copy between Source Port (src-interface) to a Destination Port (The port in context).

The analyzer port for port ingress traffic mirroring should be the same port for all mirrored ports.

The analyzer port for port egress traffic mirroring should be the same port for all mirrored ports.

The analyzer port for VLAN mirroring should be the same for all the mirrored VLANs, and should be the same port as the analyzer port for port ingress mirroring traffic.

Following are restrictions apply for ports that are configured to be source ports:

- ◆ The port cannot be a destination port.

The following restrictions apply to ports that are configured to be monitor ports:

- ◆ The port can't be source port.
- ◆ The port isn't member in port-channel.
- ◆ IP interface is not configured on the port.
- ◆ GVRP is not enabled on the port.
- ◆ The port is not a member in any VLAN, except for the default VLAN (will be automatically removed from the default VLAN).
- ◆ L2 protocols are not active on the copy dest. Port: LLDP, LBD, STP, LACP.

The following restrictions apply to ports that are configured to be monitor ports:

- ◆ The port cannot be source port.
- ◆ The port is not a member in port-channel.



**NOTE:** In this mode some traffic duplication on the analyzer port may be observed. For example:

- Port 2 is being egress monitored by port 4.
- Port 2 & 4 are members in VLAN 3.
- Unknown Unicast packet sent to VLAN 3 will egress from port 4 twice, one instance as normal forward and another instance as mirrored from port 2.
- Moreover, if port 2 is an untagged member in VLAN 3 and port 4 is a tagged member then both instances will look different (one tagged and the other is not).

**NOTE:** When the port is configured to 802.1X auto mode it will forward any mirrored traffic regardless of the .1X state. However, it will operate as a normal network port (forward traffic) only after authorization is done.

**NOTE:** Mirrored traffic is exposed to STP state, i.e. if the port is in STP blocking, it will not egress any mirrored traffic.

---

**EXAMPLE**

The following example copies traffic for both directions (Tx and Rx) from the source port 2 to destination port 1.

```
Console(config)# interface te1
Console(config-if)# port monitor te2
```

**show ports monitor** Use the **show ports monitor** EXEC mode command to display the port monitoring status.

**SYNTAX**

**show ports monitor**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the port monitoring status.

```
Console# show ports monitor
Port monitor mode: Monitor-only
Source port      Destination Port      Type      Status
-----
te8              te1                   RX, TX    Active
te2              te1                   RX, TX    Active
te18             te1                   Rx        Active
VLAN 9           te1                   N/A      Active
```

**port monitor mode** Use the **port monitor mode** Global Configuration mode command to define the monitoring mode. Use the **no** form of this command to return to default.

**SYNTAX**

**port monitor mode** {*monitor-only* | *network*}

**no port monitor mode**

**PARAMETERS**

- ◆ **monitor-only**—Specifies that the monitor port acts only as a monitor port. Other network traffic is discarded at ingress and egress.
- ◆ **network**—Specifies that the monitor port acts also as a network port.

**DEFAULT CONFIGURATION**

Product-specific

### COMMAND MODE

Global Configuration mode

### USER GUIDELINES

Once the port monitor mode is defined, no changing between modes is allowed. Any mode change will have to first go through un-defining the monitor port.

### EXAMPLE

```
console(config)# port monitor mode network
```

**sflow receiver** Use the **sflow receiver** Global Configuration mode command to define sFlow collector. Use the **no** form of this command to remove the definition of the collector.

#### SYNTAX

```
sflow receiver index {ipv4-address | ipv6-address | hostname} [port  
port] [max-datagram-size bytes]
```

```
no sflow receiver index
```

#### PARAMETERS

- ◆ **index**—The index of the receiver. (Range: 1–8)
- ◆ **ipv4-address**—Pv4 address of the host to be used as an sFlow Collector.
- ◆ **ipv6-address**—IPv6 address of the host to be used as an sFlow Collector. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.
- ◆ **hostname**—Hostname of the host to be used as an sFlow Collector. Only translation to IPv4 addresses is supported.
- ◆ **port**—Port number for syslog messages. If unspecified, the port number defaults to 6343. The range is 1-65535.
- ◆ **bytes**—Specifies the maximum number of bytes that can be sent in a single sample datagram. If unspecified, it defaults to 1400.

#### DEFAULT

No receiver is defined.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

If the IP address of the sFlow receiver is set to 0.0.0.0, no sFlow datagrams are sent.

**sflow flow-sampling** Use the **sflow flow-sampling** Interface Configuration mode command to enable sFlow Flow sampling and configure the average sampling rate of a specific port. Use the **no** form of this command to disable Flow sampling.

#### SYNTAX

```
sflow flow-sampling rate receiver-index [max-header-size bytes]
no sflow flow-sampling
```

#### PARAMETERS

- ◆ **rate**—Specifies the average sampling rate (Range: 1, 1024–1073741823.)
- ◆ **receiver-index**—Index of the receiver/collector (Range: 1–8.)
- ◆ **bytes**—Specifies the maximum number of bytes that would be copied from the sampled packet. If unspecified, defaults to 128. (Range: 20–256.)

#### DEFAULT

Disabled

#### COMMAND MODE

Interface Configuration (Ethernet) mode

#### USER GUIDELINES

A new sampling rate configuration is not immediately loaded to the hardware. It will be loaded to the hardware only after the next packet is sampled (based on the current sampling rate).

**sflow counters-sampling** Use the **sflow counters-sampling** Interface Configuration mode command to enable sFlow Counters sampling and to configure the maximum interval of a specific port. Use the **no** form of this command to disable sFlow Counters sampling.

#### SYNTAX

```
sflow counters-sampling interval receiver-index
no sflow counters-sampling
```

#### PARAMETERS

- ◆ **interval**—Specifies the maximum number of seconds between successive samples of the interface counters. (Range: 1, 15–86400.)
- ◆ **receiver-index**—Index of the receiver/collector. (Range: 1–8.)

#### DEFAULT

Disabled

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**clear sflow statistics** Use the **clear sFlow statistics** EXEC mode command to clear sFlow statistics.

**SYNTAX**

```
clear sflow statistics [interface-id]
```

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

If no interface is specified by the user, the command clears all the sFlow statistics counters (including datagrams sent). If an interface is specified by the user, the command clears only the counter of the specific interface.

**show sflow configuration** Use the **show sflow configuration** EXEC mode command to display the sFlow configuration for ports that are enabled for Flow sampling or Counters sampling.

**SYNTAX**

```
show sflow configuration [interface-id]
```

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

```

Console # show sflow configuration
Receivers
Index      IP Address      Port      Max Datagram Size
-----
1          0.0.0.0         6343      1400
2          172.16.1.2     6343      1400
3          0.0.0.0         6343      1400
4          0.0.0.0         6343      1400
5          0.0.0.0         6343      1400
6          0.0.0.0         6343      1400
7          0.0.0.0         6343      1400
8          0.0.0.0         6343      1400
Interfaces
Inter- Flow      Counters Max Header Flow      Counters Collector

```

face	Sampling	Sampling	Size	Collector	Index	Index
te1	1/2048	60 sec	128	1		1
te2	1/4096	Disabled	128	0		2

**show sflow statistics** Use the **show sflow statistics** EXEC mode command to display the sFlow statistics for ports that are enabled for Flow sampling or Counters sampling.

#### SYNTAX

**show sflow statistics** [*interface-id*]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

#### COMMAND MODE

EXEC modev

#### EXAMPLE

```

Console # show sflow statistics
Total sFlow datagrams sent to collectors: 100

Interface      Packets sampled      datagrams sent to collector
-----
1/1            30                   50
1/2            10                   10
1/3            0                    10
1/4            0                    0

```

## LINK LAYER DISCOVERY PROTOCOL (LLDP) COMMANDS

**lldp run** Use the **lldp run** Global Configuration mode command to enable Link Layer Discovery Protocol (LLDP). To disable LLDP, use the **no** form of this command.

### SYNTAX

**lldp run**  
**no lldp run**

### PARAMETERS

This command has no arguments or keywords.

### DEFAULT

Enabled

### COMMAND MODE

Global Configuration mode

### EXAMPLE

```
console(config)# lldp run
```

**lldp transmit** Use the **lldp transmit** Interface Configuration mode command to enable transmitting Link Layer Discovery Protocol (LLDP) on an interface. Use the **no** form of this command to stop transmitting LLDP on an interface.

### SYNTAX

**lldp transmit**  
**no lldp transmit**

### PARAMETERS

This command has no arguments or keywords.

### DEFAULT

Enabled

### COMMAND MODE

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

LLDP manages LAG ports individually. LLDP sends separate advertisements on each port in a LAG.

LLDP operation on a port is not dependent on the STP state of a port. I.e. LLDP frames are sent on blocked ports.

If a port is controlled by 802.1X, LLDP would operate only if the port is authorized.

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# lldp transmit
```

**lldp receive** Use the **lldp receive** Interface Configuration mode command to enable receiving Link Layer Discovery Protocol (LLDP) on an interface. Use the **no** form of this command to stop receiving LLDP on an interface.

**SYNTAX**

**lldp receive**

**no lldp receive**

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT**

Enabled

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

LLDP manages LAG ports individually. LLDP data received through LAG ports is stored individually per port.

LLDP operation on a port is not dependent on the STP state of a port. I.e. LLDP frames are received on blocked ports.

If a port is controlled by 802.1X, LLDP would operate only if the port is authorized.

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# lldp receive
```

**Ildp timer** Use the **ildp timer** Global Configuration mode command to specify how often the software sends Link Layer Discovery Protocol (LLDP) updates. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**ildp timer** *seconds*

**no ildp timer**

#### PARAMETERS

**seconds**—Specifies, in seconds, how often the software sends LLDP updates. (Range: 5?32768 seconds)

#### DEFAULT CONFIGURATION

The default update interval is 30 seconds.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example sets the interval for sending LLDP updates to 60 seconds.

```
Console(config)# ildp timer 60
```

**Ildp hold-multiplier** Use the **ildp hold-multiplier** Global Configuration mode command to set the time interval during which the receiving device holds a Link Layer Discovery Protocol (LLDP) packet before discarding it. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**ildp hold-multiplier** *number*

**no ildp hold-multiplier**

#### PARAMETERS

**number**—Specifies the LLDP packet hold time interval as a multiple of the LLDP timer value. (Range: 2use the **no** form of this command10)

#### DEFAULT CONFIGURATION

The default LLDP hold multiplier is 4.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The actual Time-To-Live (TTL) value of LLDP frames is expressed by the following formula:

$TTL = \min(65535, \text{LLDP-Timer} * \text{LLDP-HoldMultiplier})$

For example, if the value of the LLDP timer is 30 seconds, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field of the LLDP header.

#### EXAMPLE

The following example sets the LLDP packet hold time interval to 90 seconds.

```
Console(config)# lldp timer 30
Console(config)# lldp hold-multiplier 3
```

**lldp reinit** Use the **lldp reinit** Global Configuration mode command to specify the minimum time an LLDP port waits before reinitializing LLDP transmission. Use the **no** form of this command to revert to the default setting.

#### SYNTAX

**lldp reinit seconds**

**no lldp reinit**

#### PARAMETERS

**seconds**—Specifies the minimum time in seconds an LLDP port waits before reinitializing LLDP transmission.(Range: 1–10)

#### DEFAULT

2 seconds

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

```
console(config)# lldp reinit 4
```

**lldp tx-delay** Use the **lldp tx-delay** Global Configuration mode command to set the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**lldp tx-delay seconds**

**no lldp tx-delay**

**PARAMETERS**

**seconds**—Specifies the delay in seconds between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. (Range: 1?8192 seconds)

**DEFAULT CONFIGURATION**

The default LLDP frame transmission delay is 2 seconds.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

It is recommended that the tx-delay be less than 0.25 of the LLDP timer interval.

**EXAMPLE**

The following example sets the LLDP transmission delay to 10 seconds.

```
Console(config)# lldp tx-delay 10
```

**lldp optional-tlv** Use the **lldp optional-tlv** Interface Configuration (Ethernet) mode command to specify which optional TLVs from the basic set are transmitted. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
lldp optional-tlv tlv [tlv2 ... tlv5]
```

```
no lldp optional-tlv
```

**PARAMETERS**

**tlv**—Specifies TLV that should be included. Available optional TLVs are: port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size.

**DEFAULT CONFIGURATION**

No optional TLV is transmitted.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**EXAMPLE**

The following example specifies that the port description TLV is transmitted on tengigabitethernet port 0/2.

```
Console(config)# interface tengigabitethernet 0/2
Console(config-if)# lldp optional-tlv port-desc
```

**lldp management-address** Use the **lldp management-address** Interface Configuration (Ethernet) mode command to specify the management address advertised from an interface. Use the **no** form of this command to stop advertising management address information.

#### SYNTAX

```
lldp management-address {ip-address | none | automatic
[interface-id] }
```

```
no lldp management-address
```

#### PARAMETERS

- ◆ **ip-address**—Specifies the static management address to advertise.
- ◆ **none**—Specifies that no address is advertised.
- ◆ **automatic**—Specifies that the software would automatically choose a management address to advertise from all the IP addresses of the product. In case of multiple IP addresses the software chooses the lowest IP address among the dynamic IP addresses. If there are no dynamic addresses, the software chooses the lowest IP address among the static IP addresses.
- ◆ **automatic interface-id**—Specifies that the software automatically chooses a management address to advertise from the IP addresses that are configured (associated) for the interface ID. In case of multiple IP addresses, the software chooses the lowest IP address among the dynamic IP addresses of the interface. If there are no dynamic addresses, the software chooses the lowest IP address among the static IP addresses of the interface. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN. Note that if the port or port-channel are members in a VLAN that has an IP address, that address is not included because the address is associated with the VLAN.

#### DEFAULT CONFIGURATION

No IP address is advertised.

The default advertisement is **automatic**.

#### COMMAND MODE

Interface Configuration (Ethernet) mode

#### USER GUIDELINES

Each port can advertise one IP address.

**EXAMPLE**

The following example sets the LLDP management address advertisement mode to **automatic** on tengigabitethernet port 0/2.

```
Console(config)# interface tengigabitethernet 0/2
Console(config)# lldp management-address automatic
```

**Ildp notifications** Use the **lldp notifications** Interface Configuration (Ethernet) mode command to enable or disable sending Link Layer Discovery Protocol (LLDP) notifications on an interface. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
lldp notifications {enable | disable}
no lldp notifications
```

**PARAMETERS**

- ◆ **enable**—Enables sending LLDP notifications.
- ◆ **disable**—Disables sending LLDP notifications.

**DEFAULT CONFIGURATION**

Sending LLDP notifications is disabled.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**EXAMPLE**

The following example enables sending LLDP notifications on tengigabitethernet port 0/5.

```
Console(config)# interface tengigabitethernet 0/5
Console(config)# lldp notifications 10
```

**Ildp notifications interval** Use the **lldp notifications interval** Global Configuration mode command to configure the maximum transmission rate of LLDP notifications. Use the **no** form of this command to return to the default.

**SYNTAX**

```
lldp notifications interval seconds
no lldp notifications interval
```

**PARAMETERS**

**seconds**—The device should not send more than one notification in the indicated period. (Range: 5–3600)

**DEFAULT**

5 seconds

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

```
console(config)# lldp notification interval 10
```

**Ildp optional-tlv 802.1** Use the **lldp optional-tlv** Interface Configuration mode command to specify which optional TLVs from the basic set to transmit. Use the **no** form of this command revert to the default setting.

**SYNTAX**

**lldp optional-tlv 802.1** *pvid*

**no lldp optional-tlv 802.1** *pvid*

**lldp optional-tlv 802.1 ppvid add** *ppvid*

**lldp optional-tlv 802.1 ppvid remove** *ppvid*

**lldp optional-tlv 802.1 vlan-name add** *vlan-id*

**lldp optional-tlv 802.1 vlan-name remove** *vlan-id*

**lldp optional-tlv 802.1 protocol add** {*stp* | *rstp* | *mstp* | *pause* | *802.1x* | *lacp* | *gvrp*}

**lldp optional-tlv 802.1 protocol remove** {*stp* | *rstp* | *mstp* | *pause* | *802.1x* | *lacp* | *gvrp*}

**PARAMETERS**

*pvid*—Advertises the PVID of the port.

- ◆ *ppvid*—Adds/removes PPVID for advertising. PPVID 0 can be used to advertise the PPVIDs capabilities of the interface.(Range: 0–4094)
- ◆ *vlan*—Adds/removse VLAN ID for advertising. (Range: 1–4094)

**DEFAULT**

No optional TLV is transmitted.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**lldp med enable** Use the **lldp med enable** Interface Configuration (Ethernet) mode command to enable Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) on an interface. Use the **no** form of this command to disable LLDP MED on an interface.

#### SYNTAX

**lldp med enable** [*tlv ... tlv4*]

**no lldp med enable**

#### PARAMETERS

**tlv**—Specifies the TLV that should be included. Available TLVs are: network-policy, location, and poe-pse, inventory. The capabilities TLV is always included if LLDP-MED is enabled.

#### DEFAULT CONFIGURATION

LLDP MED is disabled.

#### COMMAND MODE

Interface Configuration (Ethernet) mode

#### EXAMPLE

The following example enables LLDP MED with the **location** TLV on tengigabitethernet port 0/3.

```
Console(config)# interface tengigabitethernet 0/3
Console(config)# lldp med enable location
```

**lldp med notifications topology-change** Use the **lldp med notifications topology-change** Interface Configuration (Ethernet) mode command to enable sending LLDP MED topology change notifications. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**lldp med notifications topology-change** {*enable* | *disable*}

**no lldp med notifications topology-change**

#### PARAMETERS

- ◆ **enable**—Enables sending LLDP MED topology change notifications.
- ◆ **disable**—Disables sending LLDP MED topology change notifications.

#### DEFAULT CONFIGURATION

Disable is the default.

#### COMMAND MODE

Interface Configuration (Ethernet) mode

**EXAMPLE**

The following example enables sending LLDP MED topology change notifications on tengigabitethernet port 0/2.

```
Console(config)# interface tengigabitethernet 0/2
Console(config)# lldp med notifications topology-change enable
```

**lldp med fast-start repeat-count**

Use the **lldp med fast-start repeat-count** Global Configuration mode command to configure the number of times the fast start LLDPDU is being sent during the activation of the fast start mechanism defined by LLDP-MED. Use the **no** form of this command return to default.

**SYNTAX**

**lldp med fast-start repeat-count** *number*  
**no lldp med fast-start repeat-count**

**PARAMETERS**

**number**—Specifies the number of times the fast start LLDPDU is being sent during the activation of the fast start mechanism.

**DEFAULT**

3

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

```
console(config)# lldp med fast-start repeat-count 4
```

**lldp med network-policy (global)**

Use the **lldp med network-policy** Global Configuration mode command to define LLDP MED network policy. Use the **no** form of this command to remove LLDP MED network policy.

**SYNTAX**

**lldp med network-policy** *number application [vlan id] [vlan-type {tagged | untagged}] [up priority] [dscp value]*  
**no lldp med network-policy** *number*

**PARAMETERS**

- ◆ **number**—Network policy sequential number.
- ◆ **application**—The name or the number of the primary function of the application defined for this network policy. Available application names

are: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling.

- ◆ **vlan id**—VLAN identifier for the application.
- ◆ **vlan-type**—Specifies if the application is using a Tagged or an Untagged VLAN.
- ◆ **up priority**—User Priority (Layer 2 priority) to be used for the specified application.
- ◆ **dscp value**—DSCP value to be used for the specified application.

#### DEFAULT

No Network policy is defined.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Use the **lldp med network-policy** Interface Configuration command to attach a network policy to a port.

Up to 32 network policies can be defined.

#### EXAMPLE

```
console(config)# lldp med network-policy 1 voice-signaling vlan 1
```

### lldp med network-policy (interface)

Use the **lldp med network-policy** Interface Configuration (Ethernet) mode command to attach or remove an LLDP MED network policy on an interface. Use the **no** form of this command to remove all the LLDP MED network policies from the interface.

#### SYNTAX

```
lldp med network-policy {add | remove} number
no lldp med network-policy number
```

#### PARAMETERS

- ◆ **number**—Specifies the network policy sequential number.
- ◆ **add**—Attaches the specified network policy to the interface.
- ◆ **remove**—Removes the specified network policy from the interface.

#### DEFAULT CONFIGURATION

No network policy is attached to the interface.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

For each port, only one network policy per application (voice, voice-signaling, etc.) can be defined.

**EXAMPLE**

The following example attaches LLDP MED network policy 1 to tengigabitethernet port 0/1.

```
Console(config)# interface tengigabitethernet 0/1
Console(config-if)# lldp med network-policy add 1
```

**clear lldp table** Use the **clear lldp table** command in Privileged EXEC mode to restart the LLDP RX state machine and clear the neighbors table.

**SYNTAX**

**clear lldp table** [*interface-id*]

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

```
console# clear lldp table tengigabitethernet 0/1
```

**lldp med location** Use the **lldp med location** Interface Configuration (Ethernet) mode command to configure the location information for the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) for an interface. Use the **no** form of this command to delete location information for an interface.

**SYNTAX**

**lldp med location** {{*coordinate data*} | {*civic-address data*} | {*ecs-elin data*}}

**no lldp med location** {*coordinate* | *civic-address* | *ecs-elin*}

**PARAMETERS**

- ◆ **coordinate**—Specifies the location data as coordinates.
- ◆ **civic-address**—Specifies the location data as a civic address.

- ◆ **ecs-elin**—Specifies the location data as an Emergency Call Service Emergency Location Identification Number (ECS ELIN).
- ◆ **data**—Specifies the location data in the format defined in ANSI/TIA 1057: dotted hexadecimal data: Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. (Length: coordinate: 16 bytes. Civic-address: 6-160 bytes. Ecs-elin: 10-25 bytes)

#### DEFAULT CONFIGURATION

The location is not configured.

#### COMMAND MODE

Interface Configuration (Ethernet) mode

#### EXAMPLE

The following example configures the LLDP MED location information on tengigabitethernet port 0/2 as a civic address.

```
console(config)# interface te2
console(config-if)# lldp med location civic-address 616263646566
```

### show lldp configuration

Use the **show lldp configuration** Privileged EXEC mode command to display the Link Layer Discovery Protocol (LLDP) configuration for all interfaces or for a specific interface.

#### SYNTAX

**show lldp configuration** [*interface-id*]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example sets the LLDP re-initialization delay to 10 seconds.

```
Switch# show lldp configuration
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds

LLDP packets handling: Filtering

Port      State  Optional TLVs  Address  Notifications
```

```

-----
te1 RX,TX PD, SN, SD, SC      172.16.1.1   Disabled
te2 TX      PD, SN           172.16.1.1   Disabled
te3 RX,TX PD, SN, SD, SC      None         Disabled
te5 RX,TX D, SN, SD, SC       automatic    Disabled
te6 RX,TX PD, SN, SD, SC      auto vlan 1  Disabled
te7 RX,TX PD, SN, SD, SC      auto g1      Disabled
te8          RX,TX PD, SN, SD, SC auto ch1     Disabled
Switch# show lldp configuration te1
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering

Port State   Optional TLVs   Address   Notifications
-----
te1 RX, TX    PD, SN, SD, SC  72.16.1.1  Disabled

802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size

802.1 optional TLVs
PVID: Enabled
PPVIDs: 0, 1, 92
VLANs: 1, 92
Protocols: 802.1x

```

The following table describes the significant fields shown in the display:

Field	Description
<b>Timer</b>	The time interval between LLDP updates.
<b>Hold multiplier</b>	The amount of time (as a multiple of the timer interval) that the receiving device holds a Link Layer Discovery Protocol (LLDP) packet before discarding it.
<b>Reinit timer</b>	The minimum time interval an LLDP port waits before re-initializing an LLDP transmission.
<b>Tx delay</b>	The delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.
<b>Port</b>	The port number.
<b>State</b>	The port's LLDP state.
<b>Optional TLVs</b>	Optional TLVs that are advertised. Possible values are: PD - Port description SN - System name SD - System description SC - System capabilities
<b>Address</b>	The management address that is advertised.
<b>Notifications</b>	Indicates whether LLDP notifications are enabled or disabled.

**show lldp med configuration** Use the **show lldp med configuration** Privileged EXEC mode command to display the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) configuration for all interfaces or for a specific interface.

#### SYNTAX

```
show lldp med configuration [interface-id]
```

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following examples display the LLDP MED configuration for all interfaces and for tengigabitethernet port 0/1.

#### EXAMPLE

The following examples display the LLDP MED configuration for all interfaces and for tengigabitethernet port 0/1.

```
console# show lldp med configuration

Fast Start Repeat Count: 4.
Network policy 1
-----
Application type: voiceSignaling
VLAN ID: 1 untagged
Layer 2 priority: 0
DSCP: 0

Port      Capabilities  Network policy  Location  Notifications  Inventory
-----
te1      Yes           Yes             Yes       Enabled        Yes
te2      Yes           Yes             No        Enabled        No
te3      No            No              No        Enabled        No

console# show lldp med configuration tengigabitethernet 0/1

Port      Capabilities  Network policy  Location  Notifications  Inventory
-----
te1      Yes           Yes             Yes       Enabled        Yes

Network policies:
Location:
Civic-address: 61:62:63:64:65:66
```

**show lldp local tlvs-overloading** Use the **show lldp local tlvs-overloading** EXEC mode command to display the status of TLVs overloading of the Link Layer Discovery Protocol (LLDP).

#### SYNTAX

```
show lldp local tlvs-overloading [interface-id]
```

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

#### COMMAND MODE

EXEC mode

#### USER GUIDELINES

The command calculates the overloading status of the current LLDP configuration, and not for the last LLDP packet that was sent.

#### EXAMPLE

```
Switch# show lldp local tlvs-overloading
Ports with LLDP TLV overloading are: tel, te9
Switch# show lldp local tlvs-overloading
No LLDP TLV overloading.
Switch# show lldp local tlvs-overloading tel
TLVs Group          Bytes      Status
-----
Mandatory            31         Transmitted
LLDP-MED Capabilities 9          Transmitted
LLDP-MED Location   200        Transmitted
802.1 1360          Overloading

Total: 1600 bytes
Left: 100 bytes
```

**show lldp local** Use the **show lldp local** Privileged EXEC mode command to display the Link Layer Discovery Protocol (LLDP) information that is advertised from a specific port.

#### SYNTAX

```
show lldp local interface-id
```

#### PARAMETERS

**Interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

#### COMMAND MODE

Privileged EXEC mode

**EXAMPLE**

The following examples display LLDP information that is advertised from tengigabitethernet ports 0/1 and 0/2.

```
Switch# show lldp local tel
Device ID: 0060.704C.73FF
Port ID: tel
Capabilities: Bridge
System Name: ts-7800-1
System description:
Port description:
Management address: 172.16.1.8
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex, 1000BASE-T
full duplex
Operational MAU type: 1000BaseTFD
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522

802.3 EEE
Local Tx: 30 usec
Local Rx: 25 usec
Remote Tx Echo: 30 usec
Remote Rx Echo: 25 usec

802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2 (VLAN2)
802.1 Protocol: 88 8E 01

LLDP-MED capabilities: Network Policy, Location Identification
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice
Flags: Tagged VLAN
VLAN ID: 2
Layer 2 priority: 0
DSCP: 0

LLDP-MED Power over Ethernet
Device Type: Power Sourcing Entity
Power source: Primary Power Source
Power priority: High
Power value: 9.6 Watts

LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01

LLDP-MED Inventory
Hardware Revision: B1
Firmware Revision: A1
Software Revision: 3.8
Serial number: 7978399
Manufacturer name: Manufacturer
Model name: Model 1
Asset ID: Asset 123
```

```
Switch# show lldp local te2

LLDP is disabled.
```

**show lldp neighbors** Use the **show lldp neighbors** Privileged EXEC mode command to display information about neighboring devices discovered using Link Layer Discovery Protocol (LLDP). The information can be displayed for all interfaces or for a specific interface.

#### SYNTAX

**show lldp neighbors** [*interface-id*]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

#### COMMAND MODE

Privileged EXEC mode

#### USER GUIDELINES

There are no guidelines for this command.

A TLV value that cannot be displayed as an ASCII string is displayed as an hexadecimal string.

#### EXAMPLE

The following examples display information about neighboring devices discovered using LLDP.

Location information, if it exists, is also displayed.

```
Switch# show lldp neighbors

Port  Device ID          Port ID  System Name  Capabilities  TTL
-----
te1  00:00:00:11:11:11   te1     ts-7800-2   B              90
te1  00:00:00:11:11:11 D te1     ts-7800-2   B              90
te2  00:00:26:08:13:24  te3     ts-7900-1   B, R          90
te3  00:00:26:08:13:24  te2     ts-7900-2   W              90

Switch# show lldp neighbors te1

Device ID: 00:00:00:11:11:11
Port ID: te
System Name: ts-7800-2
Capabilities: B
System description:
Port description:
Management address: 172.16.1.1
Time To Live: 90 seconds

802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported.
Auto-negotiation status: Enabled.
```

Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex, 1000BASE-T full duplex.

Operational MAU type: 1000BaseTFD

#### 802.3 Power via MDI

MDI Power support Port Class: PD

PSE MDI Power Support: Not Supported

PSE MDI Power State: Not Enabled

PSE power pair control ability: Not supported.

PSE Power Pair: Signal

PSE Power class: 1

#### 802.3 Link Aggregation

Aggregation capability: Capable of being aggregated

Aggregation status: Not currently in aggregation

Aggregation port ID: 1

#### 802.3 Maximum Frame Size: 1522

#### 802.3 EEE

Remote Tx: 25 usec

Remote Rx: 30 usec

Local Tx Echo: 30 usec

Local Rx Echo: 25 usec

#### 802.1 PVID: 1

802.1 PPVID: 2 supported, enabled

802.1 VLAN: 2(VLAN2)

802.1 Protocol: 88 8E 01

LLDP-MED capabilities: Network Policy.

LLDP-MED Device type: Endpoint class 2.

#### LLDP-MED Network policy

Application type: Voice

Flags: Unknown policy

VLAN ID: 0

Layer 2 priority: 0

DSCP: 0

#### LLDP-MED Power over Ethernet

Device Type: Power Device

Power source: Primary power

Power priority: High

Power value: 9.6 Watts

#### LLDP-MED Inventory

Hardware revision: 2.1

Firmware revision: 2.3

Software revision: 2.7.1

Serial number: LM759846587

Manufacturer name: VP

Model name: TR12

Asset ID: 9

#### LLDP-MED Location

Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01

The following table describes significant LLDP fields shown in the display:

Field	Description
<b>Port</b>	The port number.
<b>Device ID</b>	The neighbor device's configured ID (name) or MAC address.
<b>Port ID</b>	The neighbor device's port ID.
<b>System name</b>	The neighbor device's administratively assigned name.
<b>Capabilities</b>	The capabilities discovered on the neighbor device. Possible values are: B - Bridge R - Router W - WLAN Access Point T - Telephone D - DOCSIS cable device H - Host r - Repeater O - Other
<b>System description</b>	The neighbor device's system description.
<b>Port description</b>	The neighbor device's port description.
<b>Management address</b>	The neighbor device's management address.
<b>Auto-negotiation support</b>	The auto-negotiation support status on the port. (Supported or Not Supported)
<b>Auto-negotiation status</b>	The active status of auto-negotiation on the port. (Enabled or Disabled)
<b>Auto-negotiation Advertised Capabilities</b>	The port speed/duplex/flow-control capabilities advertised by the auto-negotiation.
<b>Operational MAU type</b>	The port MAU type.
<b>LLDP MED</b>	
<b>Capabilities</b>	The sender's LLDP-MED capabilities.
<b>Device type</b>	The device type. Indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, to which Endpoint Class it belongs.
<b>LLDP MED - Network Policy</b>	
<b>Application type</b>	The primary function of the application defined for this network policy.
<b>Flags</b>	Flags. The possible values are: Unknown policy: Policy is required by the device, but is currently unknown. Tagged VLAN: The specified application type is using a Tagged VLAN. Untagged VLAN: The specified application type is using an Untagged VLAN.
<b>VLAN ID</b>	The VLAN identifier for the application.
<b>Layer 2 priority</b>	The Layer 2 priority used for the specified application.
<b>DSCP</b>	The DSCP value used for the specified application.
<b>LLDP MED - Power Over Ethernet</b>	
<b>Power type</b>	The device power type. The possible values are: Power Sourcing Entity (PSE) or Power Device (PD).

Field	Description
<b>Power Source</b>	The power source utilized by a PSE or PD device. A PSE device advertises its power capability. The possible values are: Primary power source and Backup power source. A PD device advertises its power source. The possible values are: Primary power, Local power, Primary and Local power.
<b>Power priority</b>	The PD device priority. A PSE device advertises the power priority configured for the port. A PD device advertises the power priority configured for the device. The possible values are: Critical, High and Low.
<b>Power value</b>	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.
<b>LLDP MED - Location</b>	
<b>Coordinates, Civic address, ECS ELIN.</b>	The location information raw data.

**show lldp statistics** Use the **show lldp statistics** EXEC mode command to display the Link Layer Discovery Protocol (LLDP) statistics.

#### SYNTAX

**show lldp statistics** [*interface-id*]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

```
Switch# show lldp statistics
Contax(config-if)# do show lldp statistics
Tables Last Change Time: 14-Oct-2010 32:08:18
Tables Inserts: 26
Tables Deletes: 2
Tables Dropped: 0
Tables Ageouts: 1
```

Port	TX Frames		RX Frames		RX Discarded	TLVs Unrecognized
	RX Ageouts	Total	Total	Discarded Errors		
te1	0	730	850	0	0	0
te2	0	0	0	0	0	0
te3	0	730	0	0	0	0
te4	0	0	0	0	0	0
te5	0	0	0	0	0	0

te6	8	7	0	0	0	0
		1				
te/7	0	0	0	0	0	0
		0				
te8	0	0	0	0	0	0
		0				
te9	730	0	0	0	0	0
		0				
te10	0	0	0	0	0	0
		0				

---

**spanning-tree** Use the **spanning-tree** Global Configuration mode command to enable spanning-tree functionality. Use the **no** form of this command to disable the spanning-tree functionality.

#### SYNTAX

**spanning-tree**  
**no spanning-tree**

#### DEFAULT CONFIGURATION

Spanning-tree is enabled.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example enables spanning-tree functionality.

```
Console(config)# spanning-tree
```

**spanning-tree mode** Use the **spanning-tree mode** Global Configuration mode command to configure the spanning-tree protocol currently running. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**spanning-tree mode** {*stp* | *rstp* | *mst*}  
**no spanning-tree mode**

#### PARAMETERS

- **stp**—Specifies that the Spanning Tree Protocol (STP) is enabled.
- **rstp**—Specifies that the Rapid Spanning Tree Protocol (RSTP) is enabled.
- **mst**—Specifies that the Multiple Spanning Tree Protocol (MSTP) is enabled.

#### DEFAULT CONFIGURATION

The default is RSTP.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP, and uses STP when the neighbor device uses STP.

**EXAMPLE**

The following example configures the spanning-tree protocol as RSTP.

```
console(config)# spanning-tree mode mstp
```

**spanning-tree forward-time**

Use the **spanning-tree forward-time** Global Configuration mode command to configure the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**spanning-tree forward-time** *seconds*

**no spanning-tree forward-time**

**PARAMETERS**

**seconds**—Specifies the spanning-tree forward time in seconds. (Range: 4–30)

**DEFAULT CONFIGURATION**

The default forwarding time for the IEEE Spanning Tree Protocol (STP) is 15 seconds.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

When configuring the forwarding time, the following relationship should be maintained:

$$2 * (\text{Forward-Time} - 1) \geq \text{Max-Age}$$

**EXAMPLE**

The following example configures the spanning tree bridge forwarding time to 25 seconds.

```
Console(config)# spanning-tree forward-time 25
```

**spanning-tree hello-time**

Use the **spanning-tree hello-time** Global Configuration mode command to configure the spanning tree bridge Hello time, which is how often the device broadcasts Hello messages to other devices. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**spanning-tree hello-time** *seconds*

**no spanning-tree hello-time**

**PARAMETERS**

**seconds**—Specifies the spanning-tree Hello time in seconds. (Range: 1–10)

**DEFAULT CONFIGURATION**

The default Hello time for IEEE Spanning Tree Protocol (STP) is 2 seconds.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

When configuring the Hello time, the following relationship should be maintained:

$$\text{Max-Age} \geq 2 * (\text{Hello-Time} + 1)$$

**EXAMPLE**

The following example configures the spanning-tree bridge hello time to 5 seconds.

```
Console(config)# spanning-tree hello-time 5
```

**spanning-tree max-age** Use the **spanning-tree max-age** Global Configuration mode command to configure the spanning-tree bridge maximum age. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**spanning-tree max-age** *seconds*  
**no spanning-tree max-age**

#### PARAMETERS

**seconds**—Specifies the spanning-tree bridge maximum age in seconds. (Range: 6–40)

#### DEFAULT CONFIGURATION

The default maximum age for IEEE Spanning Tree Protocol (STP) is 20 seconds.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

When configuring the maximum age, the following relationships should be maintained:

$$2 * (\text{Forward-Time} - 1) \geq \text{Max-Age}$$

$$\text{Max-Age} \geq 2 * (\text{Hello-Time} + 1)$$

#### EXAMPLE

The following example configures the spanning-tree bridge maximum age to 10 seconds.

```
Console(config)# spanning-tree max-age 10
```

**spanning-tree priority** Use the **spanning-tree priority** Global Configuration mode command to configure the device spanning-tree priority, which is used to determine which bridge is selected as the root bridge. Use the **no** form of this command to restore the default device spanning-tree priority.

#### SYNTAX

**spanning-tree priority** *priority*  
**no spanning-tree priority**

#### PARAMETERS

**priority**—Specifies the bridge priority. (Range: 0–61440)

**DEFAULT CONFIGURATION**

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree.

**EXAMPLE**

The following example configures the spanning-tree priority to 12288.

```
Console(config)# spanning-tree priority 12288
```

**spanning-tree  
disable**

Use the **spanning-tree disable** Interface Configuration (Ethernet, port-channel) mode command to disable the spanning tree on a specific port. Use the **no** form of this command to enable the spanning tree on a port.

**SYNTAX**

**spanning-tree disable**

**no spanning-tree disable**

**DEFAULT CONFIGURATION**

Spanning tree is enabled on all ports.

**COMMAND MODE**

Interface Configuration (Ethernet, port-channel) mode

**EXAMPLE**

The following example disables the spanning tree on tengigabitethernet port 0/5

```
Console(config)# interface tengigabitethernet 0/5
Console(config-if)# spanning-tree disable
```

**spanning-tree cost** Use the **spanning-tree cost** Interface Configuration (Ethernet, port-channel) mode command to configure the spanning-tree path cost for a port. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**spanning-tree cost** *cost*  
**no spanning-tree cost**

#### PARAMETERS

**cost**—Specifies the port path cost. (Range: 1–200000000)

#### DEFAULT CONFIGURATION

Default path cost is determined by port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

#### COMMAND MODE

Interface Configuration (Ethernet, port-channel) mode

#### EXAMPLE

The following example configures the spanning-tree cost on tengigabitethernet port 0/15 to 35000.

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# spanning-tree cost 35000
```

**spanning-tree port-priority** Use the **spanning-tree port-priority** Interface Configuration (Ethernet, port-channel) mode command to configure the port priority. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**spanning-tree port-priority** *priority*  
**no spanning-tree port-priority**

#### PARAMETERS

**priority**—Specifies the port priority. (Range: 0–240)

#### DEFAULT CONFIGURATION

The default port priority for IEEE Spanning Tree Protocol (STP) is 128.

**COMMAND MODE**

Interface Configuration (Ethernet, port-channel) mode

**USER GUIDELINES**

The priority value must be a multiple of 16.

**EXAMPLE**

The following example configures the spanning priority on tengigabitethernet port 0/15 to 96

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# spanning-tree port-priority 96
```

**spanning-tree portfast**

Use the **spanning-tree portfast** Interface Configuration (Ethernet, port-channel) mode command to enable the PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the standard forward time delay. Use the **no** form of this command to disable the PortFast mode.

**SYNTAX**

**spanning-tree portfast [auto]**

**no spanning-tree portfast**

**PARAMETERS**

**auto**—Specifies that the software waits for 3 seconds (with no BPDUs received on the interface) before putting the interface into the PortFast mode.

**DEFAULT CONFIGURATION**

PortFast mode is disabled.

**COMMAND MODE**

Interface Configuration (Ethernet, port-channel) mode

**EXAMPLE**

The following example enables the PortFast mode on tengigabitethernet port 0/15.

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# spanning-tree portfast
```

**spanning-tree link-type** Use the **spanning-tree link-type** Interface Configuration (Ethernet, port-channel) mode command to override the default link-type setting determined by the port duplex mode, and enable Rapid Spanning Tree Protocol (RSTP) transitions to the forwarding state. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
spanning-tree link-type {point-to-point | shared}
no spanning-tree spanning-tree link-type
```

#### PARAMETERS

- ◆ **point-to-point**—Specifies that the port link type is point-to-point.
- ◆ **shared**—Specifies that the port link type is shared.

#### DEFAULT CONFIGURATION

The device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

#### COMMAND MODE

Interface Configuration (Ethernet, port-channel) mode

#### EXAMPLE

The following example enables shared spanning-tree on tengigabitethernet port 0/15.

```
Console(config)# interface tengigabitethernet 0/15
Console(config-if)# spanning-tree link-type shared
```

**spanning-tree pathcost method** Use the **spanning-tree pathcost method** Global Configuration mode command to set the default path cost method. Use the **no** form of this command to return to the default configuration.

#### SYNTAX

```
spanning-tree pathcost method {long | short}
no spanning-tree pathcost method
```

#### PARAMETERS

- ◆ **long**—Specifies that the default port path costs are within the range: 1–200,000,000.
- ◆ **short**—Specifies that the default port path costs are within the range: 1–65,535.

#### DEFAULT CONFIGURATION

Short path cost method.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

This command applies to all the spanning tree instances on the switch.

- ◆ If the short method is chosen, the switch use for the default cost values in the range 1 through 65,535.
- ◆ If the long method is chosen, the switch use for the default cost values in the range 1 through 200,000,000.

**EXAMPLE**

The following example sets the default path cost method to Long.

```
Console(config)# spanning-tree pathcost method long
```

**spanning-tree bpd  
(Global)**

Use the **spanning-tree bpd** Global Configuration mode command to define BPDU handling when the spanning tree is disabled globally or on a single interface. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
spanning-tree bpd {filtering | flooding | bridging}  
no spanning-tree bpd
```

**PARAMETERS**

- ◆ **filtering**—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- ◆ **flooding**—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to all ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.
- ◆ **bridging**—Specifies that BPDU packets, whether untagged or tagged, are flooded and are subject to ingress and egress VLAN rules when the spanning tree is disabled globally. This mode is not relevant if the spanning tree is disabled only on a group of ports.

**DEFAULT CONFIGURATION**

The default setting is **flooding**.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The **filtering** and **flooding** modes are relevant when the spanning tree is disabled globally or on a single interface.

The **bridging** mode is relevant only when the spanning tree is disabled globally.

The BPDU handling mode cannot be changed to **bridging** if the spanning tree is globally enabled.

The spanning tree cannot be globally enabled if the BPDU handling mode is **bridging**.

**EXAMPLE**

The following example defines the BPDU packet handling mode as **flooding** when the spanning tree is disabled on an interface.

```
Console(config)# spanning-tree bpdn flooding
```

**spanning-tree bpdn (Interface)**

Use the **spanning-tree bpdn** Interface Configuration (Ethernet, Port-channel) mode command to define BPDU handling when the spanning tree is disabled on a single interface. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**spanning-tree bpdn** {*filtering* | *flooding*}

**no spanning-tree bpdn**

**PARAMETERS**

- ◆ **filtering**—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- ◆ **flooding**—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

**DEFAULT CONFIGURATION**

The **spanning-tree bpdn (Global)** command determines the default configuration.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**USER GUIDELINES**

If the **spanning-tree bpdn (Global)** command is supported and the **bridging** mode is supported:

If the global BPDU handling mode is **bridging**, the operational BPDU handling mode is bridging for all the ports (The per-interface BPDU handling configuration is kept as a shadow configuration).

#### EXAMPLE

The following example defines the BPDU packet as **flooding** when the spanning tree is disabled on tengigabitethernet port 0/3.

```
Console(config)# interface tengigabitethernet 0/3
Console(config-if)# spanning-tree bpdu flooding
```

### spanning-tree guard root

use the **spanning-tree guard root** Interface Configuration (Ethernet, Port-channel) mode command to enable root guard on all spanning-tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. Use the **no** form of this command to disable the root guard on the interface.

#### SYNTAX

```
spanning-tree guard root
no spanning-tree guard root
```

#### DEFAULT CONFIGURATION

Root guard is disabled.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-channel) mode

#### USER GUIDELINES

Root guard can be enabled when the device operates in STP, RSTP and MSTP modes.

When root guard is enabled, the port changes to the alternate state if the spanning-tree calculations select the port as the root port.

#### EXAMPLE

The following example prevents tengigabitethernet port 0/1 from being the root port of the device..

```
Console(config)# interface tengigabitethernet 0/1
Console(config-if)# spanning-tree guard root
```

**spanning-tree bpduguard** Use the **spanning-tree bpduguard** Interface Configuration (Ethernet, port-channel) mode command to shut down an interface when it receives a bridge protocol data unit (BPDU). Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
spanning-tree bpduguard {enable | disable}
no spanning-tree bpduguard
```

#### PARAMETERS

**enable**—Enables BPDU Guard.

**disable**—Disables BPDU Guard.

#### DEFAULT CONFIGURATION

BPDU Guard is disabled.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-channel) mode

#### USER GUIDELINES

The command can be enabled when the spanning tree is enabled (useful when the port is in the PortFast mode) or disabled.

#### EXAMPLE

The following example shuts down Ethernet port 0/5 when it receives a BPDU.

```
Console(config)# interface tengigabitethernet 0/5
Console(config-if)# spanning-tree bpduguard enable
```

**clear spanning-tree detected-protocols** Use the **clear spanning-tree detected-protocols** Privileged EXEC command to restart the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface

#### SYNTAX

```
clear spanning-tree detected-protocols [interface interface-id]
```

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

#### COMMAND MODE

Privileged EXEC mode

#### USER GUIDELINES

This feature should be used only when working in RSTP or MSTP mode.

**EXAMPLE**

```
console# clear spanning-tree detected-protocols
```

**spanning-tree mst priority** Use the **spanning-tree mst priority** Global Configuration mode command to configure the device priority for the specified spanning-tree instance. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**spanning-tree mst** *instance-id* *priority* *priority*

**no spanning-tree mst** *instance-id* *priority*

**PARAMETERS**

- ◆ **instance-id**—Specifies the spanning-tree instance ID. (Range:1-7)
- ◆ **priority**—Specifies the device priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. (Range: 0-61440)

**DEFAULT CONFIGURATION**

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree.

**EXAMPLE**

The following example configures the spanning tree priority of instance 1 to 4096.

```
Console(config)# spanning-tree mst 1 priority 4096
```

**spanning-tree mst max-hops** Use the **spanning-tree mst max-hops** Global Configuration mode command to configure the number of hops in an MST region before the BDPDU is discarded and the port information is aged out. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
spanning-tree mst max-hops hop-count
no spanning-tree mst max-hops
```

#### PARAMETERS

**hop-count**—Specifies the number of hops in an MST region before the BDPDU is discarded. (Range: 1–40)

#### DEFAULT CONFIGURATION

The default number of hops is 20.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
Console(config)# spanning-tree mst max-hops 10
```

**spanning-tree mst port-priority** Use the **spanning-tree mst port-priority** Interface Configuration (Ethernet, port-channel) mode command to configure the priority of a port. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
spanning-tree mst instance-id port-priority priority
no spanning-tree mst instance-id port-priority
```

#### PARAMETERS

- ◆ **instance-id**—Specifies the spanning tree instance ID. (Range: 1–15)
- ◆ **priority**—Specifies the port priority. (Range: 0–240 in multiples of 16)

#### DEFAULT CONFIGURATION

The default port priority for IEEE Spanning Tree Protocol (STP) is 128.

#### COMMAND MODE

Interface Configuration (Ethernet, port-channel) mode

#### USER GUIDELINES

The priority value must be a multiple of 16.

**EXAMPLE**

The following example configures the port priority of port te1 to 144.

```
Console(config)# interface tengigabitethernet 0/1
Console(config-if)# spanning-tree mst 1 port-priority 144
```

**spanning-tree mst cost**

Use the **spanning-tree mst cost** Interface Configuration (Ethernet, Port-channel) mode command to configure the path cost for multiple spanning-tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**spanning-tree mst** *instance-id* **cost** *cost*

**no spanning-tree mst** *instance-id* **cost**

**PARAMETERS**

- ◆ **instance-id**—Specifies the spanning-tree instance ID. (Range: 1–15)
- ◆ **cost**—Specifies the port path cost. (Range: 1–200000000)

**DEFAULT CONFIGURATION**

Default path cost is determined by the port speed and path cost method (long or short) as shown below:

Interface	Long	Short
<b>Port-channel</b>	20,000	4
<b>Gigabit Ethernet (1000 Mbps)</b>	20,000	4
<b>Fast Ethernet (100 Mbps)</b>	200,000	19
<b>Ethernet (10 Mbps)</b>	2,000,000	100

**COMMAND MODE**

Interface Configuration (Ethernet, port-channel) mode

**EXAMPLE**

The following example configures the MSTP instance 1 path cost for tengigabitethernet port 0/9 to 4.

```
Console(config)# interface tengigabitethernet 0/9
Console(config-if)# spanning-tree mst 1 cost 4
```

**spanning-tree mst configuration** Use the **spanning-tree mst configuration** Global Configuration mode command to enable configuring an MST region by entering the Multiple Spanning Tree (MST) mode.

#### SYNTAX

**spanning-tree mst configuration**

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

For two or more switches to be in the same MST region, they need to contain the same VLAN mapping, the same configuration revision number, and the same name.

#### EXAMPLE

The following example configures an MST region.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 1 vlan 10-20
Console(config-mst)# name region1
Console(config-mst)# revision 1
```

**instance (MST)** Use **instance** MST Configuration mode command to map VLANs to an MST instance. Use the **no** form of this command to restore default mapping.

#### SYNTAX

**instance** *instance-id* **vlan** *vlan-range*  
**no instance** *instance-id* **vlan** *vlan-range*

#### PARAMETERS

- ◆ **instance-id**—MST instance (Range: 1–15)
- ◆ **vlan-range**—The specified range of VLANs is added to the existing ones. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 1–4094)

#### DEFAULT CONFIGURATION

All VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

#### COMMAND MODE

MST Configuration mode

**USER GUIDELINES**

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

**EXAMPLE**

The following example maps VLANs 10-20 to MST instance 1.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 1 vlan 10-20
```

**name (MST)** Use the **name** MST Configuration mode command to define the MST configuration name. Use the **no** form of this command to restore the default setting.

**SYNTAX**

**name** *string*

**no name**

**PARAMETERS**

**string**—Specifies the MST configuration name. (Length: 1–32 characters)

**DEFAULT CONFIGURATION**

The default name is the bridge address.

**COMMAND MODE**

MST Configuration mode

**EXAMPLE**

The following example defines the configuration name as Region1.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# name region1
```

**revision (MST)** Use the **revision** MST Configuration mode command to define the MST configuration revision number. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**revision** *value*

**no revision**

**PARAMETERS**

**value**—Specifies the MST configuration revision number. (Range: 0–65535)

**DEFAULT CONFIGURATION**

The default configuration revision number is 0.

**COMMAND MODE**

MST Configuration mode

**EXAMPLE**

The following example sets the configuration revision to 1.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # revision 1
```

**show (MST)** Use the **show** MST Configuration mode command to displays the current or pending MST region configuration.

**SYNTAX**

**show** {*current* | *pending*}

**PARAMETERS**

- ◆ **current**—Displays the current MST region configuration.
- ◆ **pending**—Displays the pending MST region configuration.

**COMMAND MODE**

MST Configuration mode

**EXAMPLE**

The following example displays a pending MST region configuration.

```
Console(config-mst)# show pending

Pending MST configuration
Name: Region1
Revision: 1

Instance      Vlans Mapped      State
-----      -
0             1-9,21-4094      Enabled
1             10-20             Enabled
```

**exit (MST)** Use the **exit** MST Configuration mode command to exit the MST region Configuration mode and apply all configuration changes.

#### SYNTAX

**exit**

#### COMMAND MODE

MST Configuration mode

#### EXAMPLE

The following example exits the MST Configuration mode and saves changes.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# exit
Console(config)#
```

**abort (MST)** Use the **abort** MST Configuration mode command to exit the MST Configuration mode without applying the configuration changes.

#### SYNTAX

**abort**

#### COMMAND MODE

MST Configuration mode

#### EXAMPLE

The following example exits the MST Configuration mode without saving changes.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# abort
```

**show spanning-tree** Use the **show spanning-tree** Privileged EXEC mode command to display the spanning-tree configuration.

#### SYNTAX

**show spanning-tree** [*interface-id*] [*instance instance-id*]

**show spanning-tree** [*detail*] [*active | blockedports*] [*instance instance-id*]

**show spanning-tree** *mst-configuration*

**PARAMETERS**

- ◆ **instance instance-id**—Specifies the spanning tree instance ID. (Range: 0–15)
- ◆ **detail**—Displays detailed information.
- ◆ **active**—Displays active ports only.
- ◆ **blockedports**—Displays blocked ports only.
- ◆ **mst-configuration**—Displays the MST configuration identifier.
- ◆ **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following examples display spanning-tree information.

```

Console# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled

Root ID      Priority      32768
            Address      00:01:42:97:e0:00
            Path Cost  20000
            Root Port  te1

            Hello Time 2 sec           Max Age 20 sec   Forward Delay 15 sec

Bridge ID    Priority      36864
            Address      00:02:4b:29:7a:00

            Hello Time 2 sec           Max Age 20 sec   Forward Delay 15 sec

```

## Interfaces

Name	State	Prio. Nbr	Cost	Sts	Role	PortFast	Type
te1	Enabled	128.1	20000	FWD	Root	No	P2p (RSTP)
te2	Enabled	128.2	20000	FWD	Desg	No	Shared (STP)
te3	Disabled	128.3	20000	-	-	-	-
te4	Enabled	128.4	20000	BLK	Altn	No	Shared (STP)
te5	Enabled	128.5	20000	DIS	-	-	-

Console# **show spanning-tree**

Spanning tree enabled mode RSTP  
Default port cost method: long

Root ID    Priority            36864  
          Address            00:02:4b:29:7a:00

          This switch is the Root.

          Hello Time 2 sec                    Max Age 20 sec    Forward Delay 15 sec

## Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
te1	Enabled	-	20000	FWD	Desg	No	P2p (RSTP)
te2	Enabled	128.1	20000	FWD	Desg	No	Shared (STP)
te3	Disabled	128.2	20000	-	-	-	-
te4	Enabled	128.3	20000	FWD	Desg	No	Shared (STP)
te5	Enabled	128.4	20000	DIS	-	-	-
		128.5					

Console# **show spanning-tree**

Spanning tree disabled (BPDU filtering) mode RSTP  
Default port cost method: long

Root ID    Priority            N/A  
          Address            N/A  
          Path Cost        N/A  
          Root Port        N/A  
          Hello Time      N/A            Max Age N/A    Forward Delay N/A

Bridge ID   Priority            36864  
          Address            00:02:4b:29:7a:00  
          Hello Time 2 sec                    Max Age 20 sec    Forward Delay 15 sec

## Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
te1	Enabled	-	20000	-	-	-	-
te2	Enabled	128.1	20000	-	-	-	-
te3	Disabled	128.2	20000	-	-	-	-
te4	Enabled	128.3	20000	-	-	-	-
te5	Enabled	128.4	20000	-	-	-	-
		128.5					

Console# **show spanning-tree active**

Spanning tree enabled mode RSTP  
 Default port cost method: long

```

Root ID    Priority      32768
          Address      00:01:42:97:e0:00
          Path Cost   20000
          Root Port   te1

          Hello Time 2 sec          Max Age 20 sec  Forward Delay 15 sec
    
```

```

Bridge ID  Priority      36864
          Address      00:02:4b:29:7a:00

          Hello Time 2 sec          Max Age 20 sec  Forward Delay 15 sec
    
```

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
te1	Enabled	-	20000	FWD	Root	No	P2p (RSTP)
te2	Enabled	128.1	20000	FWD	Desg	No	Shared (STP)
te4	Enabled	128.2	20000	BLK	Altn	No	Shared (STP)
		128.4					

Console# **show spanning-tree blockedports**

Spanning tree enabled mode RSTP  
 Default port cost method: long

```

Root ID    Priority      32768
          Address      00:01:42:97:e0:00
          Path Cost   20000
          Root Port   te1

          Hello Time 2 sec          Max Age 20 sec  Forward Delay 15 sec
    
```

```

Bridge ID  Priority      36864
          Address      00:02:4b:29:7a:00

          Hello Time 2 sec          Max Age 20 sec  Forward Delay 15 sec
    
```

Interfaces



```

Port 4 (te4) enabled
State: Blocking                               Role: Alternate
Port id: 128.4                               Port cost: 20000
Type: Shared (configured:auto) STP          Port Fast: No (configured:no)
Designated bridge Priority: 28672          Address: 00:30:94:41:62:c8
Designated port id: 128.25                 Designated path cost: 20000
Guard root: Disabled                       BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

```

```

Port 5 (te5) enabled
State: Disabled                               Role: N/A
Port id: 128.5                               Port cost: 20000
Type: N/A (configured: auto)                Port Fast: N/A (configured:no)
Designated bridge Priority: N/A             Address: N/A
Designated port id: N/A                    Designated path cost: N/A
Guard root: Disabled                       BPDU guard: Disabled

Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A

```

Console# **show spanning-tree ethernet** tel

```

Port 1 (tel) enabled
State: Forwarding                             Role: Root
Port id: 128.1                               Port cost: 20000
Type: P2p (configured: auto) RSTP          Port Fast: No (configured:no)
Designated bridge Priority: 32768          Address: 00:01:42:97:e0:00
Designated port id: 128.25                 Designated path cost: 0
Guard root: Disabled                       BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

```

Console# **show spanning-tree mst-configuration**

```

Name: Region1
Revision: 1

Instance          Vlans mapped      State
-----          -
0                  1-9, 21-4094     Enabled
1                  10-20             Enabled

```

Console# **show spanning-tree**

```

Spanning tree enabled mode MSTP
Default port cost method: long

##### MST 0 Vlans Mapped: 1-9

CST Root ID          Priority 32768
Address 00:01:42:97:e0:00
Path 20000
Cost tel
Root
Port

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```

```

IST Master ID      Priority 32768
                  Address 00:02:4b:29:7a:00

                  This switch is the IST master.

                  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
                  Max hops 20

```

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
te1	Enabled	128.1	20000	FWD	Root	No	--
te2	Enabled	128.2	20000	FWD	Desg	No	P2p Bound (RSTP)
te3	Enabled	128.3	20000	FWD	Desg	No	Shared Bound
te4	Enabled	128.4	20000	FWD	Desg	No	(STP) P2p P2p

##### MST 1 Vlans Mapped: 10-20

```

Root ID           Priority 24576
                  Address 00:02:4b:29:89:76
                  Path    20000
                  Cost    te4
                  Root    19
                  Port
                  Rem hops

```

```

Bridge ID         Priority 32768
                  Address 00:02:4b:29:7a:00

```

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
te1	Enabled	128.1	20000	FWD	Boun	No	--
te2	Enabled	128.2	20000	FWD	Boun	No	P2p Bound (RSTP)
te3	Enabled	128.3	20000	BLK	Altn	No	Shared Bound
te4	Enabled	128.4	20000	FWD	Root	No	(STP) P2p P2p

Console# **show spanning-tree detail**

```

Spanning tree enabled mode MSTP
Default port cost method: long

```

##### MST 0 Vlans Mapped: 1-9

```

CST Root ID       Priority 32768
                  Address 00:01:42:97:e0:00
                  Path    20000
                  Cost    te1
                  Root
                  Port

                  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

IST Master ID      Priority 32768
                  Address 00:02:4b:29:7a:00

                  This switch is the IST master.

                  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

                  Max hops 20
                  Number of topology changes 2 last change occurred 2d18h ago
                  Times: hold 1, topology change 35, notification 2
                  hello 2, max age 20, forward delay 15
    
```

```

Port 1 (te1) enabled
State: Forwarding                               Role: Root
Port id: 128.1                                  Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP      Port Fast: No (configured:no)
Designated bridge Priority: 32768              Address: 00:01:42:97:e0:00
Designated port id: 128.25                     Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
    
```

```

Port 2 (te2) enabled
State: Forwarding                               Role: Designated
Port id: 128.2                                  Port cost: 20000
Type: Shared (configured: auto) Boundary STP    Port Fast: No (configured:no)
Designated bridge Priority: 32768              Address: 00:02:4b:29:7a:00
Designated port id: 128.2                     Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
    
```

```

Port 3 (te3) enabled
State: Forwarding                               Role: Designated
Port id: 128.3                                  Port cost: 20000
Type: Shared (configured: auto) Internal        Port Fast: No (configured:no)
Designated bridge Priority: 32768              Address: 00:02:4b:29:7a:00
Designated port id: 128.3                     Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
    
```

```

Port 4 (te4) enabled                               v
State: Forwarding
Port id: 128.4
Type: Shared (configured: auto) Internal
Designated bridge Priority: 32768
Designated port id: 128.2
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
    
```

##### MST 1 Vlans Mapped: 10-20

```

Root ID      Priority 24576
             Address 00:02:4b:29:89:76
             Path    20000
             Cost     te4
             Root
             Port

             Rem hops 19
    
```

```

Bridge ID          Priority 32768
                  Address 00:02:4b:29:7a:00

                  Number of topology changes 2 last change occurred 1d9h ago

                  Times: hold 1, topology change 2, notification 2
                  hello 2, max age 20, forward delay 15

```

```

Port 1 (te1) enabled
State: Forwarding                               Role: Boundary
Port id: 128.1                                  Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP      Port Fast: No (configured:no)
Designated bridge Priority: 32768               Address: 00:02:4b:29:7a:00
Designated port id: 128.1                       Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

```

```

Port 2 (te2) enabled
State: Forwarding                               Role: Designated
Port id: 128.2                                  Port cost: 20000
Type: Shared (configured: auto) Boundary STP    Port Fast: No (configured:no)
Designated bridge Priority: 32768               Address: 00:02:4b:29:7a:00
Designated port id: 128.2                       Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

```

```

Port 3 (te3) disabled
State: Blocking                                 Role: Alternate
Port id: 128.3                                  Port cost: 20000
Type: Shared (configured: auto) Internal        Port Fast: No (configured:no)
Designated bridge Priority: 32768               Address: 00:02:4b:29:1a:19
Designated port id: 128.78                      Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

```

```

Port 4 (te4) enabled
State: Forwarding                               Role: Designated
Port id: 128.4                                  Port cost: 20000
Type: Shared (configured: auto) Internal        Port Fast: No (configured:no)
Designated bridge Priority: 32768               Address: 00:02:4b:29:7a:00
Designated port id: 128.2                       Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

```

```
Console# show spanning-tree
```

```
Spanning tree enabled mode MSTP
Default port cost method: long
```

```
##### MST 0 Vlans Mapped: 1-9
```

```

CST Root ID          Priority 32768
                    Address 00:01:42:97:e0:00
                    Path    20000
                    Cost    te1
                    Root
                    Port

                    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```

```

IST Master ID      Priority 32768
                  Address 00:02:4b:19:7a:00
                  Path    10000
                  Cost    19
                  Rem hops

Bridge ID         Priority 32768
                  Address 00:02:4b:29:7a:00

                  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
                  Max hops 20

Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

##### MST 0 Vlans Mapped: 1-9

CST Root ID      Priority 32768
                  Address 00:01:42:97:e0:00

                  This switch is root for CST and IST master.

                  Root      te1
                  Port

                  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
                  Max hops 20

```

**show spanning-tree bpd** Use the **show spanning-tree bpd** EXEC mode command to display the BPDUs handling when spanning-tree is disabled.

#### SYNTAX

**show spanning-tree bpd** *[interface-id]*

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following examples display spanning-tree information.

```
Console# show spanning-tree bpdu
```

```
Global: Flooding
```

Interface	Admin Mode	Oper Mode
te1	Global	Flooding
te2	Global	STP
te3	Flooding	STP

### spanning-tree loopback-guard

Use the **spanning-tree loopback-guard global configuration** command to shut down any interface when it receives a loopback bridge protocol data unit (BPDU). Use the **no** form of this command to return the default setting.

#### SYNTAX

```
spanning-tree loopback-guard  
no spanning-tree loopback-guard
```

#### COMMAND MODE

Global

#### USER GUIDELINES

This command is used with Spanning Tree configuration.

#### EXAMPLE

```
Switch (config)# spanning-tree loopback-guard
```



# VIRTUAL LOCAL AREA NETWORK (VLAN) COMMANDS

**vlan database** Use the **vlan database** Global Configuration mode command to enter the VLAN Configuration mode.

## SYNTAX

**vlan database**

## COMMAND MODE

Global Configuration mode

## EXAMPLE

The following example enters the VLAN database mode.

```
Console(config)# vlan database
Console(config-vlan)#
```

**vlan** Use the **vlan** VLAN Configuration mode command to create a VLAN. Use the **no** form of this command to restore the default configuration or delete a VLAN.

## SYNTAX

**vlan** *vlan-range* [*name* *vlan-name*]

**no vlan** *vlan-range*

## PARAMETERS

- ◆ **vlan-range**—Specifies a list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- ◆ **name**—Specifies the VLAN name. The option is only valid in cases where only one VLAN is configured by the command (Range: 1–32 characters)

## COMMAND MODE

VLAN Configuration mode

## EXAMPLE

The following example creates VLAN number 1972.

```
Console(config)# vlan database
Console(config-vlan)# vlan 1972
```

**interface vlan** Use the **interface vlan** Global Configuration mode command to enter the Interface Configuration (VLAN) mode and enable configuration of the specified VLAN ID.

#### SYNTAX

```
interface vlan vlan-id
```

#### PARAMETERS

**vlan-id**—Specifies an existing VLAN ID.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

If the VLAN does not exist (ghost VLAN), not all of the commands are available under the interface VLAN context.

The commands that are supported for VLANs that do not exist are:

- ◆ IGMP snooping control commands
- ◆ Bridge multicast configuration commands

#### EXAMPLE

The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console (config)# interface vlan 1
Console (config-if)# ip address 131.108.1.27 255.255.255.0
```

**interface range vlan** Use the **interface range vlan** Global Configuration mode command to enable configuring multiple VLANs simultaneously.

#### SYNTAX

```
interface range vlan vlan-range
```

#### PARAMETERS

**vlan-range**—Specifies a list of VLAN IDs. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of

the interfaces, an error message is displayed and command execution continues on the other interfaces.

#### EXAMPLE

The following example groups VLANs 221 through 228 and 889 to receive the same command.

```
Console(config)# interface range vlan 221-228, vlan 889
Console(config-if)#
```

**name** Use the **name** Interface Configuration (VLAN) mode command to add a name to a VLAN. Use the **no** form of this command to remove the VLAN name.

#### SYNTAX

```
name string
no name
```

#### PARAMETERS

**string**—Specifies a unique name associated with this VLAN. (Length: 1–32 characters)

#### DEFAULT CONFIGURATION

No name is defined.

#### COMMAND MODE

Interface Configuration (VLAN) mode. It cannot be configured for a range of interfaces (range context).

#### USER GUIDELINES

The VLAN name must be unique.

#### EXAMPLE

The following example gives VLAN number 19 the name Marketing.

```
Console(config)# interface vlan 19
Console(config-if)# name Marketing
```

**switchport protected-port** Use the **switchport protected-port** Interface Configuration mode command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. Use the **no** form of this command to disable protection on the port.

#### SYNTAX

**switchport protected-port**  
**no switchport protected-port**

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT CONFIGURATION

Unprotected

#### COMMAND MODE

Interface configuration (Ethernet, port-channel)

#### USER GUIDELINES

Use this command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports (that are not associated with the same community as the ingress interface) on the same switch. Please note that the packet is still subject to FDB decision and to all filtering rules. Use the **switchport community** Interface Configuration command to associate the interface with a community.

#### EXAMPLE

```
console(config)# interface tel
console(config-if)# switchport protected-port
```

**switchport community** Use the **switchport community** Interface Configuration mode command to associate a protected port with a community. Use the **no** form of this command to return to default.

#### SYNTAX

**switchport community** *community*  
**no switchport community**

#### PARAMETERS

**community**—Specifies the community number. (Range:1 - 30)

#### DEFAULT CONFIGURATION

The port is not associated with any community.

#### COMMAND MODE

Interface Configuration (Ethernet, port-channel) mode

**USER GUIDELINES**

The command is relevant only when the port is defined as a protected port. Use the **switchport protected-port** Interface Configuration command to define a port as a protected port.

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# switchport community 1
```

**show interfaces protected-ports**

Use the **show interfaces protected-ports** EXEC mode command to show protected ports configuration.

**SYNTAX**

**show interfaces protected-ports** [*interface-id*]

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

```
console# show interfaces protected-ports
```

Interface	State	Community
te1	Protected	1
te2	Protected	Isolated
te3	Unprotected	20
te4	Unprotected	Isolated



**NOTE:** The Community column for unprotected ports is relevant only when the port state is changed to Protected.

**switchport**

Use the **switchport** Interface Configuration mode command with no keywords to put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration. Use the **no** form of this command to put an interface in Layer 3 mode.

**SYNTAX**

**switchport**

**no switchport**

**DEFAULT CONFIGURATION**

Layer 2 mode

**COMMAND MODE**

Interface Configuration (Ethernet, port-channel) mode

**switchport mode** Use the **switchport mode** Interface Configuration (Ethernet, port-channel) mode command to configure the VLAN membership mode of a port. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
switchport mode { access | trunk | general | private-vlan
                  {promiscuous | host} | customer }
```

```
no switchport mode
```

**PARAMETERS**

- ◆ **access**—Specifies an untagged layer 2 VLAN port.
- ◆ **trunk**—Specifies a trunking layer 2 VLAN port.
- ◆ **general**—Specifies a full 802-1q supported VLAN port.
- ◆ **customer**—Specifies that the port is connected to customer equipment. Used when the switch is in a provider network.
- ◆ **private-vlan promiscuous**—Private-VLAN promiscuous port.
- ◆ **private-vlan host**—Private-VLAN host port.

**DEFAULT CONFIGURATION****COMMAND MODE**

Interface Configuration (Ethernet, port-channel) mode

**USER GUIDELINES**

- ◆ When the port mode is changed, it receives the configuration corresponding to the mode.
- ◆ If the port mode is changed to access and the access VLAN does not exist, then the port will not belong to any VLAN.

**EXAMPLE**

The following example configures tengigabitethernet port 0/1 as an untagged layer 2 VLAN port.

```
Console(config)# interface tengigabitethernet 0/1
Console(config-if)# switchport mode access
```

**switchport access vlan** Use the **switchport access vlan** Interface Configuration (Ethernet, port-channel) mode command to configure the VLAN ID when the interface is in access mode. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
switchport access vlan { vlan-id | none }
no switchport access vlan
```

#### PARAMETERS

**vlan-id**—Specifies the VLAN ID to which the port is configured.

**none**—Specifies the access port cannot belong to any VLAN.

#### DEFAULT CONFIGURATION

If the default VLAN is enabled, the VLAN ID is 1. Otherwise, it is not a member of any VLAN.

#### COMMAND MODE

Interface Configuration (Ethernet, port-channel) mode

#### USER GUIDELINES

The command automatically removes the port from the previous VLAN and adds it to the new VLAN.

#### EXAMPLE

The following example configures a VLAN ID of 23 to the untagged layer 2 VLAN tengigabitethernet port 0/1.

```
Console(config)# interface tengigabitethernet 0/1
Console(config-if)# switchport access vlan 23
```

**switchport trunk allowed vlan** Use the **switchport trunk allowed vlan** Interface Configuration mode command to set the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

#### SYNTAX

```
switchport trunk allowed vlan { all | none | add vlan-list | remove
vlan-list | except vlan-list }
no switchport trunk allowed vlan
```

#### PARAMETERS

**all**—Specifies all VLANs from 1 to 4094. At any time, the port belongs to all VLANs exiting at the time. (Range: 1–4094)

**none**—Specifies an empty VLAN list The port does not belong to any VLAN.

**add vlan-list**—List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

**remove vlan-list**—List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

**except vlan-list**—List of VLAN IDs is calculated by inverting the defined list of VLANs (the calculated list will include all VLANs from interval 1..4094 except VLANs from the defined list).

#### DEFAULT CONFIGURATION

The Default VLAN is its Native VLAN and the port belongs to either all VLANs or only to the Default VLAN depending on a value of parameter Trunk Port Default Configuration.

#### COMMAND MODE

Interface Configuration (Ethernet, port-channel) mode

#### USER GUIDELINES

The RS port model behavior allows only the following options: Add and Remove.

Inside **except vlan-list** is saved as **add ~ vlan-list**, where **~ vlan-list** is a list of all VLANs from 1 to 4094 minus the VLANs from **vlan-list**. Command **show running/startup** always uses the latter format.

The port must be in trunk mode before the command can take effect.

#### EXAMPLE

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan all
```

**switchport trunk native vlan** Use the **switchport trunk native vlan** Interface Configuration (Ethernet, port-channel) mode command to define the native VLAN when the interface is in trunk mode. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
switchport trunk native vlan { vlan-id | none }
no switchport trunk native vlan
```

#### PARAMETERS

- ◆ **vlan-id**—Specifies the native VLAN ID.
- ◆ **none**—Specifies the access port cannot belong to any VLAN.

**DEFAULT CONFIGURATION**

If the default VLAN is enabled, the VLAN ID is 1. Otherwise, the VLAN ID is 4095.

**COMMAND MODE**

Interface Configuration (Ethernet, port-channel) mode

**USER GUIDELINES**

The command adds the port as a member of the VLAN. If the port is already a member of the VLAN (not a native), it must first be removed from the VLAN.

**EXAMPLE**

The following example configures VLAN number 123 as the native VLAN when the port is in trunk mode.

```
Console# interface tel
Console(config-if)# switchport trunk native vlan 123
```

**switchport general  
allowed vlan**

Use the **switchport general allowed vlan** Interface Configuration mode command to set the general characteristics when the interface is in general mode. Use the **no** form of this command to reset a general characteristic to the default.

**SYNTAX**

```
switchport general allowed vlan {add | remove} vlan-list
[tagged|untagged]
```

```
no switchport general allowed vlan
```

**PARAMETERS**

- ◆ **add vlan-list**—List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. (Range: 1–4094)
- ◆ **remove vlan-list**—List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- ◆ **tagged** - Specify that packets would be transmitted tagged for the configured VLANs
- ◆ **untagged** - Specify that packets would be transmitted untagged for the configured VLANs (this is the default)

**DEFAULT CONFIGURATION**

The port's PVID equals to the Default VLAN ID and belongs to the Default VLAN as untagged one.

**COMMAND MODE**

Interface Configuration mode

**EXAMPLE**

```
console(config-if)# interface tengigabitethernet 0/1
console(config-if)# switchport mode general
console(config-if)# switchport general allowed vlan add 2-3 tagged
```

**switchport general pvid** Use the **switchport general pvid** Interface Configuration (Ethernet, Port-channel) mode command to configure the Port VLAN ID (PVID) when the interface is in general mode. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**switchport general pvid** *vlan-id*

**no switchport general pvid**

**PARAMETERS**

**vlan-id**—Specifies the Port VLAN ID (PVID).

**DEFAULT CONFIGURATION**

If the default VLAN is enabled, PVID is 1. Otherwise, PVID is =4095.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**EXAMPLE**

The following example configures PVID 234 for tengigabitethernet port 0/2, when the interface is in general mode.

```
Console(config)# interface tengigabitethernet 0/2
Console(config-if)# switchport mode general
Console(config-if)# switchport general pvid 234
```

**switchport general ingress-filtering disable** Use the **switchport general ingress-filtering disable** Interface Configuration (Ethernet, Port-channel) mode command to disable port ingress filtering. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**switchport general ingress-filtering disable**

**no switchport general ingress-filtering disable**

**DEFAULT CONFIGURATION**

Ingress filtering is enabled.

**COMMAND MODE**

Interface Configuration (Ethernet, port-channel) mode

**EXAMPLE**

The following example disables port ingress filtering on tengigabitethernet port 0/1.

```
Console(config)# interface tengigabitethernet 0/1
Console(config-if)# switchport mode general
Console(config-if)# switchport general ingress-filtering disable
```

### **switchport general acceptable-frame- type**

Use the **switchport general acceptable-frame-type** Interface Configuration mode command to configure ingress filtering based on packet type tagged/untagged. Use the **no** form of this command to return to default.

**SYNTAX**

**switchport general acceptable-frame-type** {*tagged-only* | *untagged-only* | *all*}

**no switchport general acceptable-frame-type**

**PARAMETERS**

- ◆ **tagged-only**—Discard untagged packets and priority tagged packets.
- ◆ **untagged-only**—Discard VLAN tagged packets (not including Priority tagged packets)
- ◆ **all**—Do not discard packets based on whether the packet is VLAN tagged or not.

**DEFAULT CONFIGURATION**

All frame types are accepted at ingress.

**COMMAND MODE**

Interface Configuration (Ethernet, port-channel) mode

**EXAMPLE**

The following example configures tengigabitethernet port 0/3 to discard untagged frames at ingress.

```
Console(config)# interface tengigabitethernet 0/3
Console(config-if)# switchport mode general
Console(config-if)# switchport general acceptable-frame-type tagged-only
```

**map protocol protocols-group** Use the **map protocol protocols-group** VLAN Configuration mode command to map a protocol to a group of protocols. Use the **no** form of this command to delete a protocol from a group.

#### SYNTAX

```
map protocol protocol [encapsulation] protocols-group group
no map protocol protocol [encapsulation]
```

#### PARAMETERS

- ◆ **protocol**—Specifies a 16-bit protocol number or one of the reserved names listed in the User Guidelines. (Range: 0x0600–0xFFFF)
- ◆ **encapsulation**—Specifies one of the following values: Ethernet, rfc1042, llcOther. If no option is indicated, the default is Ethernet.
- ◆ **protocols-group group**—Specifies the group number of the group of protocols associated together. (Range: 1–2147483647)

#### DEFAULT CONFIGURATION

The default encapsulation is Ethernet.

#### COMMAND MODE

VLAN Configuration mode

#### USER GUIDELINES

The value 0x8100 is not valid as the protocol number for Ethernet encapsulation.

The following protocol names are reserved for Ethernet Encapsulation:

- ◆ ip
- ◆ arp
- ◆ ipv6
- ◆ ipx

#### EXAMPLE

The following example maps protocol ip to protocol group number 213.

```
Console(config)# vlan database
Console(config-vlan)# map protocol ip protocols-group 213
```

**switchport general map protocols-group vlan** Use the **switchport general map protocols-group vlan** Interface Configuration (Ethernet, Port-channel) mode command to set a protocol-based classification rule. Use the **no** form of this command to delete a classification.

#### SYNTAX

```
switchport general map protocols-group group vlan vlan-id
no switchport general map protocols-group group
```

#### PARAMETERS

- ◆ **group**—Specifies the group number as defined in the **map protocol protocols-group** command. (Range: 1–65535)
- ◆ **vlan-id**—Defines the VLAN ID in the classifying rule.

#### COMMAND MODE

Interface Configuration (Ethernet, port-channel) mode

#### DEFAULT CONFIGURATION

No classification is defined.

#### USER GUIDELINES

The VLAN classification rule priorities are:

1. MAC-based VLAN (Best match among the rules)
2. Subnet-based VLAN (Best match among the rules)
3. Protocol-based VLAN
4. PVID

#### EXAMPLE

The following example sets a protocol-based classification rule.

```
Console(config-if)# switchport general map protocols-group 1 vlan 8
```

**map mac macs-group** Use the **map mac macs-group** VLAN Configuration mode command to map a MAC address or range of MAC addresses to a group of MAC addresses. Use the **no** form of this command to delete the map.

#### SYNTAX

```
map mac mac-address {prefix-mask | host} macs-group group
no map mac mac-address {prefix-mask | host}
```

**PARAMETERS**

- ◆ **mac-address**—Specifies the MAC address to be mapped to the group.
- ◆ **prefix-mask**—Specifies the number of ones in the mask.
- ◆ **host**—Specifies that the mask is comprised of all 1s.
- ◆ **group**—Specifies the group number. (Range: 1–2147483647)

**COMMAND MODE**

VLAN Configuration mode

**EXAMPLE**

The following example maps a MAC address to a group of MAC addresses.

```
Console(config)# vlan database
Console(config-vlan)# map mac 0011.1111.1111 8 macs-group 1
```

**switchport general  
map macs-group  
vlan**

Use the **switchport general map macs-group vlan** Interface Configuration (Ethernet, Port-channel) mode command to set a mac-based classification rule. Use the no form of this command to delete a classification rule.

**SYNTAX**

```
switchport general map macs-group group vlan vlan-id
no switchport general map macs-group group
```

**PARAMETERS**

- ◆ **group**—Specifies the group number. (Range: 1–2147483647)
- ◆ **vlan-id**—Defines the VLAN ID associated with the rule.

**COMMAND MODE**

Interface Configuration (Ethernet, port-channel) mode

**USER GUIDELINES**

MAC-based VLAN rules cannot contain overlapping ranges on the same interface.

The VLAN classification rule priorities are:

1. MAC-based VLAN (Best match among the rules).
2. Subnet-based VLAN (Best match among the rules).
3. Protocol-based VLAN.
4. PVID.

**EXAMPLE**

The following example sets a mac-based classification rule.

```
Console (config-if)# switchport general map mac-group 1 vlan 8
```

### **map subnet subnets-group**

Use the **map subnet subnets-group** VLAN Configuration mode command to map an IP subnet to a group of IP subnets. Use the **no** form of this command to delete the map.

**SYNTAX**

```
map subnet ip-address prefix-mask subnets-group group  
no map subnet ip-address prefix-mask
```

**PARAMETERS**

- ◆ **ip-address**—Specifies the IP address prefix of the subnet to be mapped to the group.
- ◆ **prefix-mask**—Specifies the number of 1s in the mask.
- ◆ **group**—Specifies the group number. (Range: 1–2147483647)

**COMMAND MODE**

VLAN Configuration mode

**EXAMPLE**

The following example maps an IP subnet to a group of IP subnets.

```
Console (config-vlan)# map subnet 172.16.1.1 24 subnets-group 4
```

### **switchport general map subnets-group vlan**

Use the **switchport general map subnets-group vlan** Interface Configuration (Ethernet, Port-channel) mode command to set a subnet-based classification rule. Use the **no** form of this command to delete a subnet-based classification rule.

**SYNTAX**

```
switchport general map subnets-group group vlan vlan-id  
no switchport general map subnets-group group
```

**PARAMETERS**

- ◆ **group**—Specifies the group number. (Range: 1–2147483647)
- ◆ **vlan-id**—Defines the VLAN ID associated with the rule.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**USER GUIDELINES**

The VLAN classification rule priorities are:

1. MAC-based VLAN (Best match among the rules)
2. Subnet-based VLAN (Best match among the rules)
3. Protocol-based VLAN
4. PVID

**EXAMPLE**

The following example sets a subnet-based classification rule.

```
Console (config-if)# switchport general map subnets-group 1 vlan 8
```

**show vlan** Use the **show vlan** Privileged EXEC mode command to display VLAN information for all VLANs or for a specific VLAN.

**SYNTAX**

**show vlan** [*tag vlan-id* | *name vlan-name*]

**PARAMETERS**

- ◆ **tag vlan-id**—Specifies a VLAN ID.
- ◆ **name vlan-name**—Specifies a VLAN name string. (Length: 1-32 characters)

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays information for all VLANs.

```

Console# show vlan

```

VLAN	Name	Ports	Type	Authorization
1	default	te1-2	Other	Required
10	VLAN0010	te3-4	dynamic	Required
11	VLAN0011	te1-2	static	Required
20	VLAN0020	te3-4	static	Required
21	VLAN0021		static	Required
30	VLAN0030		static	Required
31	VLAN0031		static	Required
91	VLAN0091	te1-2	static	Not Required
3978	Guest VLAN	te17	static	Guest

**show vlan protocols-groups** Use the **show vlan protocols-groups** EXEC mode command to display protocols-groups information.

**SYNTAX**

**show vlan protocols-groups**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays protocols-groups information.

```

Console> show vlan protocols-groups

```

Protocol	Encapsulation	Group
0x800 (IP)	Ethernet	1
0x806 (ARP)	Ethernet	1
0x86dd (IPv6)	Ethernet	2
0x8898	Ethernet	3

**show vlan macs-groups** Use the **show vlan macs-groups** EXEC mode command to display macs-groups information.

**SYNTAX**

**show vlan macs-groups**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays macs-groups information.

```

console# show vlan macs-groups

```

Mac Address	Mask	Group Id
00:12:34:56:78:90	20	22
00:60:70:4c:73:ff	40	1

**show vlan subnets-groups** Use the **show vlan subnets-groups** EXEC mode command to display subnets-groups information.

**SYNTAX****show vlan subnets-groups****COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays subnets-groups information.

```

console# show vlan subnets-groups

```

Ip Subnet Address	Mask	Group Id
1.1.1.1	32	1
172.16.2.0	24	2

**show interfaces switchport** Use the **show interfaces switchport** Privileged EXEC command to display the administrative and operational status of all interfaces or a specific interface.

**SYNTAX****show interfaces switchport** [*interface-id*]**PARAMETERS****Interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.**EXAMPLE**

```

Protected: Enabled, Uplink is gi1/0/1
Classification rules:

```

Classification type	Group ID	VLAN ID
-----	-----	-----
Protocol	1	19
Protocol	1	20
Protocol	2	72
Subnet	1	15
MAC	6	11

---



## VIRTUAL LOCAL AREA NETWORK (VLAN) NON-ISCLI COMMANDS

### **switchport forbidden default-vlan**

Use the **switchport forbidden default-vlan** interface configuration command to forbid a port from being added to the default VLAN. Use the no form of this command to revert to default.

#### SYNTAX

**switchport forbidden default-vlan**  
**no switchport forbidden default-vlan**

#### PARAMETERS

This command has no keywords or arguments.

#### DEFAULT CONFIGURATION

Membership in the Default VLAN is allowed.

#### COMMAND MODE

Interface and Interface range configuration (Ethernet, port-channel)

#### USER GUIDELINES

The command may be used only when the Default VLAN is supported. If the Default VLAN is supported the command may be used at any time regardless of if the port belongs to the Default VLAN.

The 'no' command does not add the port to Default VLAN, it only defines an interface as permitted to be a member of the Default VLAN, and the port will be added only when conditions are met.

### **switchport forbidden vlan**

The **switchport forbidden vlan** Interface Configuration (Ethernet, Port-channel) mode command forbids adding or removing specific VLANs to or from a port. To restore the default configuration, use the **no** form of this command.

#### SYNTAX

**switchport forbidden vlan** {**add** *vlan-list* | **remove** *vlan-list*}  
**no switchport forbidden vlan** {**add** *vlan-list* | **remove** *vlan-list*}

#### PARAMETERS

- ◆ **add** *vlan-list* — Specifies a list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen designate a range of IDs.

- ◆ **remove** *vlan-list* — Specifies a list of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen designate a range of IDs.

#### DEFAULT CONFIGURATION

All VLANs are allowed.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-channel) mode

#### EXAMPLE

The following example forbids adding VLAN IDs 234 to 256 to Ethernet port 1/7.

```
Console(config)# interface ethernet 1/7
Console(config-if)# switchport mode trunk
Console(config-if)# switchport forbidden vlan add 234-256
```

### switchport default-vlan tagged

Use the **switchport default-vlan tagged** interface configuration command to configure the port as a tagged port in the default VLAN as a tagged port. Use the **no** form of the command to return to default.

#### SYNTAX

```
switchport default-vlan tagged
no switchport default-vlan tagged
```

#### PARAMETERS

This command has no keywords or arguments.

#### DEFAULT CONFIGURATION

If the port is a member in the default VLAN, it is a member as an untagged port.

#### COMMAND MODE

Interface configuration (Ethernet, port-channel)

#### USER GUIDELINES

The command adds a port to the default VLAN as a tagged port.

The command is available only if the port mode is trunk or general.

When a trunk port is a member in the default VLAN as a tagged port then:

The native VLAN can't be the default VLAN

The default of the native VLAN is 4095




---

**NOTE:** If the native VLAN of a port is the default VLAN when the port is added to the default VLAN as a tagged, the native VLAN is set by the system to 4095.

---

When a general port is a member in the default VLAN as a tagged port then:

1. The PVID can be the default VLAN.
2. The default of the PVID is the default VLAN




---

**NOTE:** The PVID is not changed when the port is added to the default VLAN as a tagged.

---

If one of the following conditions exists when executing the “switchport default-vlan tagged” command, the port would be added (automatically by the system) to the default VLAN when the condition does not longer exist:

The port is a member in a LAG.

The port is 802.1X unauthorized.

An IP address is defined on the port.

The port is a destination port of port mirroring.

An IP address is defined on the default VLAN and the port is a PVE protected port.

The “no switchport default-vlan tagged” command removes the port from the default VLAN, and return the default VLAN mode to “untagged”.




---

**NOTE:** If the native VLAN of a trunk port is 4095 when the port is removed from the default VLAN (as a tagged), the native VLAN is set by the system to the default VLAN.

**NOTE:** The PVID of a general port is not changed when the port is removed from the default VLAN (as a tagged). If the PVID is the default VLAN, the port is added by the system to the default VLAN as an untagged.

---

## show interfaces switchport

The **show interfaces switchport** EXEC mode command displays the switchport configuration for all interfaces or for a specific interface.

### SYNTAX

```
show interfaces switchport { interface-id }
```

**PARAMETERS**

**interface-id**—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following examples display the switchport configuration.

```

Console> show interfaces switchport ethernet 1/1
Port 1/1:
VLAN Membership mode: General

PVID: 1 (default)
Ingress Filtering: Enabled
Acceptable Frame Type: All
GVRP status: Enabled
Protected: Enabled, Uplink is 1/9.

Port 1/1 is member in:

```

	VLAN Name	Egress rule	Type
	1	default	untaggedSystem
	8	VLAN008	taggedDynamic
11		VLAN0011	taggedStatic
19		IPv6VLAN	untaggedStatic
72		VLAN0072	untaggedStatic

```

Forbidden VLANs:

```

	VLAN Name
	73 Out

```

Classification rules:
Classification type
-----
Protocol based VLANs
Protocol based VLANs

```

	Group	VLAN
		219
		372

```

Console> show interfaces switchport ethernet 1/2
Port 1/2:
VLAN Membership mode: General

Operating parameters:
PVID: 4095 (discard vlan)
Ingress Filtering: Enabled
Acceptable Frame Type: All
GVRP status: Enabled
Protected: Disabled

Port 1/1 is member in:

```

	VLAN Name	Egress rule	Type
	91	IP Telephony	taggedStatic

```

Protected: Disabled

Port 1/2 is statically configured to:

```

	VLAN Name	Egress rule

```

8          VLAN0072untagged
91         IP Telephony  tagged
    
```

Forbidden VLANs:

```

          VLAN Name
-----
          73 Out
    
```

```

Console> show interfaces switchport ethernet 1/2
Port 1/2:
VLAN Membership mode: Access
Access VLAN: Dynamic
    
```

```

PVID: 9
Ingress Filtering: Enabled
Acceptable Frame Type: All
GVRP status: Enabled
VLAN Membership:
    
```

```

          VLAN NameEgress rule
-----
8          VLAN0072untagged
    
```

**ip igmp snooping (Global)** Use the **ip igmp snooping** Global Configuration mode command to enable Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable IGMP snooping.

#### SYNTAX

**ip igmp snooping**  
**no ip igmp snooping**

#### DEFAULT CONFIGURATION

IGMP snooping is disabled.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example enables IGMP snooping.

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

**ip igmp snooping vlan** Use the **ip igmp snooping vlan** Global Configuration mode command to enable Internet Group Management Protocol (IGMP) snooping on a specific VLAN. Use the **no** form of this command to disable IGMP snooping on a VLAN interface.

#### SYNTAX

**ip igmp snooping vlan** *vlan-id*  
**no ip igmp snooping vlan** *vlan-id*

#### PARAMETERS

**vlan-id**—Specifies the VLAN.

#### DEFAULT

Disabled

#### COMMAND MODE

Global Configuration mode

**USER GUIDELINES**

IGMP snooping can be enabled only on static VLANs.

IGMPv1, IGMPv2 and IGMPv3 are supported.

To activate IGMP snooping, the **bridge multicast filtering** should be enabled.

The User Guidelines of the bridge multicast mode Interface VLAN Configuration command describes the configuration that is written into the FDB as a function of the FDB mode and the IGMP version that is used in the network.

**EXAMPLE**

```
console(config)# ip igmp snooping vlan 2
```

**ip igmp snooping  
mrouter**

Use the **ip igmp snooping mrouter** Global Configuration mode command to enable automatic learning of multicast router ports. Use the **no** form of this command to remove the configuration.

**SYNTAX**

```
ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp  
no ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp
```

**PARAMETERS**

**vlan-id**—Specifies the VLAN.

**DEFAULT**

**Learning pim-dvmrp** is enabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Multicast router ports are learned based on:

- ◆ Queries received on the port
- ◆ PIM/PIMv2 received on the port
- ◆ DVMRP received on the port
- ◆ MRDISC received on the port
- ◆ MOSPF received on the port

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

**ip igmp snooping mrouter interface**

Use the **ip igmp snooping mrouter interface** Global Configuration mode command to define a port that is connected to a multicast router port. Use the **no** form of this command to remove the configuration.

**SYNTAX**

**ip igmp snooping** *vlan vlan-id* **mrouter interface** *interface-list*

**no ip igmp snooping** *vlan vlan-id* **mrouter interface** *interface-list*

**PARAMETERS**

- ◆ **vlan-id**—Specifies the VLAN.
- ◆ **interface-list**—Specifies the list of interfaces. The interfaces can be one of the following types: Ethernet port or Port-channel.

**DEFAULT**

No ports defined

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

A port that is defined as a multicast router port receives all IGMP packets (reports and queries) as well as all multicast data.

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# ip igmp snooping vlan 1 mrouter interface tel
```

**ip igmp snooping forbidden mrouter interface**

Use the **ip igmp snooping forbidden mrouter interface** Global Configuration mode command to forbid a port from being defined as a multicast router port by static configuration or by automatic learning. Use the **no** form of this command to remove the configuration.

**SYNTAX**

**ip igmp snooping** *vlan vlan-id* **forbidden mrouter interface** *interface-list*

**no ip igmp snooping** *vlan vlan-id* **forbidden mrouter interface** *interface-list*

**PARAMETERS**

- ◆ **vlan-id**—Specifies the VLAN.
- ◆ **interface-list**—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

**DEFAULT**

No ports defined

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

A port that is a forbidden mrouter port cannot be a multicast router port (i.e. cannot be learned dynamically or assigned statically).

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# ip igmp snooping vlan 1 forbidden mrouter interface tel
```

**ip igmp snooping static**

Use the **ip igmp snooping static** Global Configuration mode command to register an IP-layer multicast address to the bridge table, and to add statically ports to the group. Use the **no** form of this command to remove ports specified as members of a static multicast group.

**SYNTAX**

```
ip igmp snooping vlan vlan-id static ip-address [interface interface-list]
```

```
no ip igmp snooping vlan vlan-id static ip-address [interface interface-list]
```

**PARAMETER**

- ◆ **vlan-id**—Specifies the VLAN.
- ◆ **ip-address**—Specifies the IP multicast address.
- ◆ **interface-list**—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

**DEFAULT CONFIGURATION**

No multicast addresses are defined.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Static multicast addresses can only be defined on static VLANs.

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the **no**. command without a port-list removes the entry.

**EXAMPLE**

```
console(config)# ip igmp snooping vlan 1 static 239.2.2.2 te
```

**ip igmp snooping querier**

Use the **ip igmp snooping querier** Global Configuration mode command to enable the Internet Group Management Protocol (IGMP) querier on a specific VLAN. Use the **no** form of this command to disable the IGMP querier on a VLAN interface.

**SYNTAX**

**ip igmp snooping vlan *vlan-id* querier**

**no ip igmp snooping vlan *vlan-id* querier**

**PARAMETERS**

**vlan-id**—Specifies the VLAN

**DEFAULT**

Disabled

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The IGMP snooping querier can be enabled on a VLAN only if IGMP snooping is enabled for that VLAN.

No more than one switch can be configured as an IGMP Querier for a VLAN.

When the IGMP snooping querier is enabled, it starts after a host-time-out/2 with no IGMP traffic detected from a multicast router.

The IGMP Snooping Querier disables itself if it detects IGMP traffic from a multicast router. It restarts automatically after host-time-out/2.

Following are the IGMP snooping querier parameters as a function of the IGMP snooping parameters:

- ◆ QueryMaxResponseTime: host-time-out/10.
- ◆ QueryInterval: host-time-out/ 3.

**EXAMPLE**

```
console(config)# ip igmp snooping vlan 1 querier
```

**ip igmp snooping querier address**

Use the **ip igmp snooping querier address** Global Configuration mode command to define the source IP address that the IGMP snooping querier would use. Use the **no** form of this command to return to default.

**SYNTAX**

**ip igmp snooping** *vlan vlan-id* **querier address** *ip-address*

**no ip igmp snooping** *vlan vlan-id* **querier address**

**PARAMETERS**

- ◆ **vlan-id**—Specifies the VLAN.
- ◆ **ip-address**—Source IP address.

**DEFAULT**

If an IP address is configured for the VLAN, it is used as the source address of the IGMP snooping querier.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

If an IP address is not configured by this command, and no IP address is configured for the querier's VLAN, the querier is disabled.

**EXAMPLE**

```
console(config)# ip igmp snooping vlan 1 querier address 1.2.3.4
```

**ip igmp snooping querier version**

Use the **ip igmp snooping querier version** Global Configuration mode command to configure the IGMP version of an IGMP querier on a specific VLAN. Use the **no** form of this command to return to default.

**SYNTAX**

**ip igmp snooping** *vlan vlan-id* **querier version** {2 | 3}

**no ip igmp snooping** *vlan vlan-id* **querier version**

**PARAMETERS**

- ◆ **vlan-id**—Specifies the VLAN.
- ◆ **2**—Specifies that the IGMP version would be IGMPv2.

- ◆ **3**—Specifies that the IGMP version would be IGMPv3.

**DEFAULT**  
IGMPv2.

**COMMAND MODE**  
Global Configuration mode

**EXAMPLE**

```
console(config)# ip igmp snooping vlan 1 querier version 3
```

**ip igmp robustness** Use the **ip igmp robustness** Interface Configuration mode command to change a value of the IGMP robustness variable. Use the **no** format of the command to return to default.

**SYNTAX**

**ip igmp robustness** *count*  
**no ip igmp robustness**

**PARAMETERS**

*count*—The number of expected packet loss on a link. Parameter range. (Range: 1–7)

**DEFAULT**  
2

**COMMAND MODE**  
Interface Configuration (VLAN) mode

**USER GUIDELINES**

You can execute the command before the VLAN is created.

```
console(config)# interface vlan 1
console(config-if)# ip igmp robustness 3
```

**ip igmp query-interval** Use the **ip igmp query-interval** Interface Configuration mode command to configure the Query interval. Use the **no** format of the command to return to default.

**SYNTAX**

**ip igmp query-interval** *seconds*  
**no ip igmp query-interval**

**PARAMETERS**

**seconds**—Frequency, in seconds, at which IGMP query messages are sent on the interface. (Range: 30–18000)

**DEFAULT**

125

**COMMAND MODE**

Interface Configuration (VLAN) mode

**USER GUIDELINES**

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# interface vlan 1
console(config-if)# ip igmp query-interval 300
```

**ip igmp query-max-response-time**

Use the **ip igmp query-max-response-time** Interface Configuration mode command to configure the Query Maximum Response time. Use the **no** format of the command to return to default.

**SYNTAX**

```
ip igmp query-max-response-time seconds
no ip igmp query-max-response-time
```

**PARAMETERS**

**seconds**—Maximum response time, in seconds, advertised in IGMP queries. (Range: 5–20)

**DEFAULT**

10

**COMMAND MODE**

Interface Configuration (VLAN) mode

**USER GUIDELINES**

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# interface vlan 1
console(config-if)# ip igmp query-max-response-time 5
```

**ip igmp last-member-query-count** Use the **ip igmp last-member-query-count** Interface Configuration mode command to configure the Last Member Query Counter. Use the **no** format of the command to return to default.

#### SYNTAX

```
ip igmp last-member-query-count count
no ip igmp last-member-query-count
```

#### PARAMETER

**count**—The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

#### DEFAULT

A value of Robustness variable

#### COMMAND MODE

Interface Configuration (VLAN) mode

#### USER GUIDELINES

You can execute the command before the VLAN is created.

#### EXAMPLE

```
console(config)# interface vlan 1
console(config-if)# ip igmp last-member-query-count 3
```

**ip igmp last-member-query-interval** Use the **ip igmp last-member-query-interval** Interface Configuration mode command to configure the Last Member Query interval. Use the **no** format of the command to return to default.

#### SYNTAX

```
ip igmp last-member-query-interval milliseconds
no ip igmp last-member-query-interval
```

#### PARAMETERS

**milliseconds**—Interval, in milliseconds, at which IGMP group-specific host query messages are sent on the interface. (Range: 100–25500)

#### DEFAULT

1000

#### COMMAND MODE

Interface Configuration (VLAN) mode

#### USER GUIDELINES

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# interface vlan 1
console(config-if)# ip igmp last-member-query-interval 3000
```

**ip igmp snooping  
vlan immediate-  
leave**

Use the **ip igmp snooping vlan immediate-leave** Global Configuration mode command to enable the IGMP Snooping Immediate-Leave processing on a VLAN. Use the **no** format of the command to disable IGMP Snooping Immediate-Leave processing.

**SYNTAX**

```
ip igmp snooping vlan vlan-id immediate-leave
no ip igmp snooping vlan vlan-id immediate-leave
```

**PARAMETERS**

**vlan-id**—Specifies the VLAN ID value. (Range: 1–4094)

**DEFAULT**

Disabled

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# ip igmp snooping vlan 1 immediate-leave
```

**show ip igmp  
snooping mrouter**

The **show ip igmp snooping mrouter** EXEC mode command displays information on dynamically learned multicast router interfaces for all VLANs or for a specific VLAN.

**SYNTAX**

```
show ip igmp snooping mrouter [interface vlan-id]
```

**PARAMETERS**

**interface vlan-id**—Specifies the VLAN ID.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays information on dynamically learned multicast router interfaces for VLAN 1000.

```

Console# show ip igmp snooping mrouter interface 1000

VLAN          Static          Dynamic          Forbidden
----          -
1000          te1              te2              te3-te23

```

### show ip igmp snooping interface

The **show ip igmp snooping interface** EXEC mode command displays the IGMP snooping configuration for a specific VLAN.

**SYNTAX**

**show ip igmp snooping interface** *vlan-id*

**PARAMETERS**

**vlan-id**—Specifies the VLAN ID.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the IGMP snooping configuration for VLAN 1000.

```

Console # show ip igmp snooping interface 1000
IGMP Snooping is globally enabled
IGMP Snooping admin: Enabled
IGMP Snooping oper: Enabled
Routers IGMP version: 3
Groups that are in IGMP version 2 compatibility mode:
231.2.2.3, 231.2.2.3
Groups that are in IGMP version 1 compatibility mode:

IGMP snooping querier admin: Enabled
IGMP snooping querier oper: Enabled
IGMP snooping querier address admin:
IGMP snooping querier address oper: 172.16.1.1
IGMP snooping querier version admin: 3

IGMP snooping robustness: admin 2 oper 2
IGMP snooping query interval: admin 125 sec oper 125 sec
IGMP snooping query maximum response: admin 10 sec oper 10 sec
IGMP snooping last member query counter: admin 2 oper 2
IGMP snooping last member query interval: admin 1000 msec oper 500 msec
IGMP snooping last immediate leave: enable

Automatic learning of multicast router ports is enabled

```

**show ip igmp snooping groups** The **show ip igmp snooping groups** EXEC mode command displays the multicast groups learned by the IGMP snooping.

#### SYNTAX

```
show ip igmp snooping groups [vlan vlan-id] [address ip-multicast-address] [source ip-address]
```

#### PARAMETERS

**vlan vlan-id**—Specifies the VLAN ID.

**address ip-multicast-address**—Specifies the IP multicast address.

**source ip-address**—Specifies the IP source address.

#### COMMAND MODE

EXEC mode

#### USER GUIDELINES

To see the full multicast address table (including static addresses), use the **show bridge multicast address-table** command.

The Include list contains the ports which are in forwarding state for this group according to the snooping database. In general, the Exclude list contains the ports that have issued an explicit Exclude for that specific source in a multicast group. The Reporters That Are Forbidden Statically list contains the list of ports which have asked to receive a multicast flow but were defined as forbidden for that multicast group in multicast bridge.



**NOTE:** Under certain circumstances, the Exclude list may not contain accurate information. For example, in the case when two Exclude reports were received on the same port for the same group but for different sources, the port will not be in the Exclude list but rather in the Include list.

#### EXAMPLE

The following example shows the output for IGMP version 2.

```
Console# show ip igmp snooping groups
```

Vlan	IP Address	Querier	Ports
1	231.2.2.2	Yes	te1
1	231.2.2.3	No	te2
19	231.2.2.4	Yes	te9

**ipv6 mld snooping (Global)** The **ipv6 mld snooping** Global Configuration mode command enables IPv6 Multicast Listener Discovery (MLD) snooping. To disable IPv6 MLD snooping, use the **no** form of this command.

**SYNTAX**

**ipv6 mld snooping**  
**no ipv6 mld snooping**

**DEFAULT CONFIGURATION**

IPv6 MLD snooping is disabled.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example enables IPv6 MLD snooping.

```
Console(config)# ip ipv6 mld snooping
```

**ipv6 mld snooping vlan** Use the **ipv6 mld snooping vlan** Global Configuration mode command to enable MLD snooping on a specific VLAN. Use the **no** form of this command to disable MLD snooping on a VLAN interface.

**SYNTAX**

**ipv6 mld snooping vlan** *vlan-id*  
**no ipv6 mld snooping vlan** *vlan-id*

**PARAMETERS**

*vlan-id*—Specifies the VLAN.

**DEFAULT**

Disabled

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

MLD snooping can only be enabled on static VLANs.

MLDv1 and MLDv2 are supported.

To activate MLD snooping, the Bridge Multicast Filtering command should be enabled.

The user guidelines of the bridge multicast IPv6 mode interface VLAN configuration command describe the configuration that can be written into the FDB as a function of the FDB mode, and the MLD version that is used in the network.

#### EXAMPLE

```
console(config)# ipv6 mld snooping vlan 2
```

**ipv6 mld robustness** Use the **ipv6 mld robustness** interface Configuration mode command to change a value of the IGMP robustness variable. Use the **no** format of the command to return to default.

#### SYNTAX

**ipv6 mld robustness** *count*

**no ipv6 mld robustness**

#### PARAMETERS

**count**The number of expected packet losses on a link. (Range: 1-7)

#### DEFAULT

2

#### COMMAND MODE

Interface Configuration (VLAN) mode

#### USER GUIDELINES

You can execute the command before the VLAN is created.

#### EXAMPLE

```
console(config)# interface vlan 1
console(config-if)# ipv6 mld robustness 3
```

**ipv6 mld snooping mrouter** Use the **ipv6 mld snooping mrouter** Global Configuration mode command to enable automatic learning of multicast router ports. Use the **no** form of this command to remove the configuration.

#### SYNTAX

**ipv6 mld snooping** *vlan vlan-id* **mrouter** *learn pim-dvmrp*

**no ipv6 mld snooping** *vlan vlan-id* **mrouter** *learn pim-dvmrp*

**PARAMETERS**

**vlan-id**—Specifies the VLAN.

**DEFAULT**

Learning **pim-dvmrp** is enabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Multicast router ports can be configured statically with the **bridge multicast forward-all** command.

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# ipv6 mld snooping vlan 1 mrouter learn pim-dvmrp
```

**ipv6 mld snooping  
mrouter interface**

Use the **ipv6 mld snooping mrouter interface** Global Configuration mode command to define a port that is connected to a multicast router port. Use the **no** form of this command to remove the configuration.

**SYNTAX**

```
ipv6 mld snooping vlan vlan-id mrouter interface interface-list  
no ipv6 mld snooping vlan vlan-id mrouter interface interface-list
```

**PARAMETERS**

- ◆ **vlan-id**—Specifies the VLAN.
- ◆ **interface-list**—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernetport or Port-channel.

**DEFAULT**

No ports defined

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

This command may be used in conjunction with the **bridge multicast forward-all** command, which is used in older versions to statically configure a port as a multicast router.

A port that is defined as a multicast router port receives all MLD packets (reports and queries) as well as all multicast data.

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# ipv6 mld snooping vlan 1 mrouter interface tel
```

### ipv6 mld snooping forbidden mrouter interface

Use the **ipv6 mld snooping forbidden mrouter interface** Global Configuration mode command to forbid a port from being defined as a multicast router port by static configuration or by automatic learning. Use the **no** form of this command to remove the configuration.

**SYNTAX**

```
ipv6 mld snooping vlan vlan-id forbidden mrouter interface  
interface-list
```

```
no ipv6 mld snooping vlan vlan-id forbidden mrouter interface  
interface-list
```

**PARAMETERS**

- ◆ **vlan-id**—Specifies the VLAN.
- ◆ **interface-list**—Specifies list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

**DEFAULT**

No forbidden ports by default

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

A port that is forbidden mrouter port cannot be a multicast router port (i.e. cannot be learned dynamically or assigned statically).

The command bridge **multicast forbidden forward-all** command was used in older versions to forbid dynamic learning of multicast router ports.

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# ipv6 mld snooping vlan 1 forbidden mrouter interface tel
```

**ipv6 mld snooping static** Use the **ipv6 mld snooping static** Global Configuration mode command to register a IPv6-layer multicast address to the bridge table, and to add statically ports to the group. Use the **no** form of this command to remove ports specified as members of a static multicast group.

#### SYNTAX

```
ipv6 mld snooping vlan vlan-id static ipv6-address interface
[interface-list]
```

```
no ipv6 mld snooping vlan vlan-id static ipv6-address interface
[interface-list]
```

#### PARAMETERS

- ◆ **vlan-id**—Specifies the VLAN.
- ◆ **ipv6-address**—Specifies the IP multicast address
- ◆ **interface-list**—Specifies list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

#### DEFAULT CONFIGURATION

No multicast addresses are defined.

#### COMMAND MODE

Global configuration mode

#### USER GUIDELINES

Static multicast addresses can only be defined on static VLANs.

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the **no** command without a port-list removes the entry.

#### EXAMPLE

```
console(config)# ipv6 mld snooping vlan 1 static 239.2.2.2 te1
```

**ipv6 mld query-interval** Use the **ipv6 mld query-interval** Interface Configuration mode command to configure the Query interval. Use the **no** format of the command to return to default.

#### SYNTAX

```
ipv6 mld query-interval seconds
```

```
ipv6 mld query-interval
```

**PARAMETERS**

**seconds**—Frequency, in seconds, at which MLD query messages are sent on the interface. (Range: 30–18000)

**DEFAULT**

125

**COMMAND MODE**

Interface Configuration (VLAN) mode

**USER GUIDELINES**

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# interface vlan 1
console(config-if)# ipv6 mld query-interval 3000
```

**ipv6 mld query-max-response-time**

Use the **ipv6 mld query-max-response-time** Interface Configuration mode command to configure the Query Maximum Response time. Use the **no** format of the command to return to default.

**SYNTAX**

**ipv6 mld query-max-response-time** *seconds*

**no ipv6 mld query-max-response-time**

**PARAMETER**

**seconds**—Maximum response time, in seconds, advertised in MLD queries. (Range: 5–20)

**DEFAULT**

10

**COMMAND MODE**

Interface Configuration (VLAN) mode

**USER GUIDELINES**

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# interface vlan 1
console(config-if)# ipv6 mld query-max-response-time 5
```

**ipv6 mld last-member-query-count** Use the **ipv6 mld last-member-query-count** Interface Configuration mode command to configure the Last Member Query Counter. Use the **no** format of the command to return to default.

#### SYNTAX

```
ipv6 mld last-member-query-count count
no ipv6 mld last-member-query-count
```

#### PARAMETERS

**count**—The number of times that group- or group-source-specific queries are sent upon receipt of message indicating a leave. (Range: 1–7)

#### DEFAULT

A value of Robustness variable

#### COMMAND MODE

Interface Configuration (VLAN) mode

#### USER GUIDELINES

You can execute the command before the VLAN is created.

#### EXAMPLE

```
console(config)# interface vlan 1
console(config-if)# ipv6 mld last-member-query-count 3
```

**ipv6 mld last-member-query-interval** Use the **ipv6 mld last-member-query-interval** interface configuration command to configure the Last Member Query Interval. Use the **no** format of the command to return to default.

#### SYNTAX

```
ipv6 mld last-member-query-interval milliseconds
no ipv6 mld last-member-query-interval
```

#### PARAMETER

**milliseconds**—Interval, in milliseconds, at which IGMP group-specific host query messages are sent on the interface. (Range: 100–64512).

#### DEFAULT

1000

#### COMMAND MODE

Interface Configuration (VLAN) mode

#### USER GUIDELINES

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# interface vlan 1
console(config-if)# ipv6 mld last-member-query-interval 2000
```

**ipv6 mld snooping  
vlan immediate-  
leave**

Use the **ipv6 mld snooping vlan immediate-leave** Global Configuration mode command to enable MLD Snooping Immediate-Leave processing on a VLAN. Use the **no** format of the command to return to disable MLD Snooping Immediate-Leave processing.

**SYNTAX**

```
ipv6 mld snooping vlan vlan-id immediate-leave
no ipv6 mld snooping vlan vlan-id immediate-leave
```

**PARAMETERS**

**vlan-id**—Specifies the VLAN ID value. (Range: 1–4094)

**DEFAULT**

Disabled

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

You can execute the command before the VLAN is created.

**EXAMPLE**

```
console(config)# ipv6 mld snooping vlan 1 immediate-leave
```

**show ipv6 mld  
snooping mrouter**

The **show ipv6 mld snooping mrouter** EXEC mode command displays information on dynamically learned multicast router interfaces for all VLANs or for a specific VLAN.

**SYNTAX**

```
show ipv6 mld snooping mrouter [interface vlan-id]
```

**PARAMETERS**

**interface vlan-id**—Specifies the VLAN ID.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays information on dynamically learned multicast router interfaces for VLAN 1000

```

Console# show ipv6 mld snooping mrouter interface 1000
VLAN   Static   Dynamic   Forbidden
----   -
1000   te1      te2       te3-23

```

**show ipv6 mld snooping interface**

The **show ipv6 mld snooping interface** EXEC mode command displays the IPv6 MLD snooping configuration for a specific VLAN.

**SYNTAX**

**show ipv6 mld snooping interface** *vlan-id*

**PARAMETERS**

**vlan-id**—Specifies the VLAN ID.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the MLD snooping configuration for VLAN 1000.

```

Console# show ipv6 mld snooping interface 1000

MLD Snooping is globally enabled

MLD Snooping admin: Enabled
MLD snooping oper mode: Enabled
Routers MLD version: 2
Groups that are in MLD version 1 compatibility mode:
FF12::3, FF12::8

MLD snooping robustness:                admin 2 oper 2
MLD snooping query interval: admin 125 sec oper 125 sec
MLD snooping query maximum response: admin 10 sec oper 10 sec
MLD snooping last member query counter: admin 2 oper 2
MLD snooping last member query interval: admin 1000 msec oper 600 msec
MLD snooping last immediate leave: enable
Automatic learning of multicast router ports is enabled

```

**show ipv6 mld snooping groups**

The **show ipv6 mld snooping groups** EXEC mode command displays the multicast groups learned by the MLD snooping.

**SYNTAX**

**show ipv6 mld snooping groups** [*vlan vlan-id*] [*address ipv6-multicast-address*] [*source ipv6-address*]

**PARAMETERS**

- ◆ **vlan vlan-id**—Specifies the VLAN ID.
- ◆ **address ipv6-multicast-address**—Specifies the IPv6 multicast address.
- ◆ **source ipv6-address**—Specifies the IPv6 source address.

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

To see the full multicast address table (including static addresses), use the **show bridge multicast address-table** command.

The Include list contains the ports which are in a forwarding state for this group according to the snooping database. In general, the Exclude list contains the ports which have issued an explicit Exclude for that specific source in a multicast group.

The Reporters That Are Forbidden Statically list contains the list of ports which have asked to receive a multicast flow but were defined as forbidden for that multicast group in a multicast bridge.



**NOTE:** Under certain circumstances, the Exclude list may not contain accurate information; for example, in the case when two Exclude reports were received on the same port for the same group but for different sources, the port will not be in the Exclude list but rather in the Include list.

**EXAMPLE**

The following example shows the output for IPv6 MLD version 2.

```

Console# show ipv6 mld snooping groups

Vlan  Group          Source          Include  Exclude  Compatibility
     Address        Address          Ports    Ports    Mode
-----
 1    FF12::3          FE80::201:C9FF:FE40:8001  te1      te1      1
 1    FF12::3          FE80::201:C9FF:FE40:8002  te2      te2      1
 19   FF12::8          FE80::201:C9FF:FE40:8003  te9      te9      2
 19   FF12::8          FE80::201:C9FF:FE40:8004  te1      te12     2
 19   FF12::8          FE80::201:C9FF:FE40:8005  te0-11   te12     2

MLD Reporters that are forbidden statically:

Vlan  Group          Source address  Ports
     Address
-----
 1    FF12::3          FE80::201:C9FF:FE40:8001  te8
 19   FF12::8          FE80::201:C9FF:FE40:8001  te8

```



## LINK AGGREGATION CONTROL PROTOCOL (LACP) COMMANDS

**lacp system-priority** Use the **lacp system-priority** Global Configuration mode command to set the system priority. Use the **no** form of this command to restore the default configuration.

### SYNTAX

**lacp system-priority** *value*  
**no lacp system-priority**

### PARAMETERS

**value**—Specifies the system priority value. (Range: 1–65535)

### DEFAULT CONFIGURATION

The default system priority is 1.

### COMMAND MODE

Global Configuration mode

### EXAMPLE

The following example sets the system priority to 120.

```
Console(config)# lacp system-priority 120
```

**lacp port-priority** Use the **lacp port-priority** Interface Configuration (Ethernet) mode command to set the physical port priority. Use the **no** form of this command to restore the default configuration.

### SYNTAX

**lacp port-priority** *value*  
**no lacp port-priority**

### PARAMETERS

**value**—Specifies the port priority. (Range: 1–65535) Use the **no** form of this command to restore the default configuration.

### DEFAULT CONFIGURATION

The default port priority is 1.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**EXAMPLE**

The following example sets the priority of tengigabitethernet port 0/6.

```
console(config)# interface te6
console(config-if)# lacp port-priority 247
```

**lacp timeout** Use the **lacp timeout** Interface Configuration (Ethernet) mode command to assign an administrative LACP timeout to an interface. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**lacp timeout** {*long* | *short*}

**no lacp timeout**

**PARAMETERS**

- ◆ **long**—Specifies the long timeout value.
- ◆ **short**—Specifies the short timeout value.

**DEFAULT CONFIGURATION**

The default port timeout value is Long.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**EXAMPLE**

The following example assigns a long administrative LACP timeout to tengigabitethernet port 0/6.

```
Console(config)# interface tengigabitethernet 0/6
Console(config-if)# lacp timeout long
```

**show lacp** Use the **show lacp** EXEC mode command to display LACP information for all Ethernet ports or for a specific Ethernet port.

**SYNTAX**

**show lacp** *interface-id* [ *parameters* | *statistics* | *protocol-state* ]

**PARAMETERS**

- ◆ **parameters**—Displays parameters only.
- ◆ **statistics**—Displays statistics only.

- ◆ **protocol-state**—Displays protocol state only.

### COMMAND MODE

EXEC mode

### EXAMPLE

The following example displays LACP information for tengigabitethernet port 0/1.

```
Console> show lacp ethernet tel
```

Port tel LACP parameters:

Actor

```

system priority:          1
system mac addr:         00:00:12:34:56:78
port Admin key:          30
port Oper key:           30
port Oper number:        21
port Admin priority:     1
port Oper priority:      1
port Admin timeout:      LONG
port Oper timeout:       LONG
LACP Activity:           ACTIVE
Aggregation:             AGGREGATABLE
synchronization:        FALSE
collecting:              FALSE
distributing:            FALSE
expired:                 FALSE

```

Partner

```

system priority:          0
system mac addr:         00:00:00:00:00:00
port Admin key:          0
port Oper key:           0
port Oper number:        0
port Admin priority:     0
port Oper priority:      0
port Admin timeout:      LONG
port Oper timeout:       LONG
LACP Activity:           PASSIVE
Aggregation:             AGGREGATABLE
synchronization:        FALSE
collecting:              FALSE
distributing:            FALSE
expired:                 FALSE

```

Port tel LACP Statistics:

```

LACP PDUs sent:          2
LACP PDUs received:     2

```

Port tel LACP Protocol State:

LACP State Machines:

```

Receive FSM:             Port Disabled State
Mux FSM:                 Detached State

```

Control Variables:

```

BEGIN:                                FALSE
LACP_Enabled:                          TRUE
Ready_N:                                FALSE
Selected:                               UNSELECTED
Port_moved:                             FALSE
NNT:                                    FALSE
Port_enabled:                           FALSE

Timer counters:

periodic tx timer:                      0
current while timer:                    0
wait while timer:                       0

```

**show lacp port-channel** Use the **show lacp port-channel** EXEC mode command to display LACP information for a port-channel.

#### SYNTAX

```
show lacp port-channel [ port_channel_number ]
```

#### PARAMETERS

**port\_channel\_number**—Specifies the port-channel number.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays LACP information about port-channel 1.

```

Console> show lacp port-channel 1

Port-Channel 1:Port Type 1000 Ethernet

Actor

System                1
  Priority:            000285:0E1C00
MAC Address:          29
Admin Key:            29
Oper Key:

Partner

System                0
  Priority:            00:00:00:00:00:00
MAC Address:          14
Oper Key:

```

# GARP VLAN REGISTRATION PROTOCOL (GVRP) COMMANDS

**gvrp enable (Global)** Use the **gvrp enable** Global Configuration mode command to enable the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) globally. Use the **no** form of this command to disable GVRP on the device.

## SYNTAX

**gvrp enable**  
**no gvrp enable**

## DEFAULT CONFIGURATION

GVRP is globally disabled.

## COMMAND MODE

Global Configuration mode

## EXAMPLE

The following example enables GVRP globally on the device.

```
Console(config)# gvrp enable
```

**gvrp enable (Interface)** Use the **gvrp enable** Interface Configuration (Ethernet, Port-channel) mode command to enable GVRP on an interface. Use the **no** form of this command to disable GVRP on an interface.

## SYNTAX

**gvrp enable**  
**no gvrp enable**

## DEFAULT CONFIGURATION

GVRP is disabled on all interfaces.

## COMMAND MODE

Interface Configuration (Ethernet, Port-channel) mode

## USER GUIDELINES

An access port does not dynamically join a VLAN because it is always a member of one VLAN only. Membership in an untagged VLAN is propagated

in the same way as in a tagged VLAN. That is, the PVID must be manually defined as the untagged VLAN VID.

#### EXAMPLE

The following example enables GVRP on tengigabitethernet port 0/6.

```
Console(config)# interface tengigabitethernet 0/6
Console(config-if)# gvrp enable
```

**garp timer** Use the **garp timer** Interface Configuration (Ethernet, port channel) mode command to adjust the values of the join, leave and leaveall timers of GARP applications, such as GVRP. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
garp timer {join | leave | leaveall} timer-value
no garp timer
```

#### PARAMETERS

- ◆ **join** | **leave** | **leaveall**—Specifies the type of timer for which the timer value is specified. The possible values are:
  - **join**—Specifies the GARP join timer. The GARP join timer value specifies the time interval between the two join messages sent by the GARP application.
  - **leave**—Specifies the GARP leave timer. The GARP leave timer value specifies the time interval for a GARP application to wait for a join message after receiving a leave message for a GARP attribute, before it de-registers the GARP attribute.
  - **leaveall**—Specifies the GARP leaveall timer. The GARP leaveall timer value specifies the time interval between leaveall messages for a GARP entity, which prompt other GARP entities to re-reregister all attribute information on this entity.
- ◆ **timer-value**—Specifies the timer value in milliseconds in multiples of 10. (Range: 10–2147483640)

#### DEFAULT CONFIGURATION

The following are the default timer values:

- ◆ **Join timer**—200 milliseconds
- ◆ **Leave timer**—600 milliseconds
- ◆ **Leaveall timer**—10000 milliseconds

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**USER GUIDELINES**

The **timer-value** value must be a multiple of 10.

The following relationship must be maintained between the timers:

- ◆ The leave time must be greater than or equal to three times the join time.
- ◆ The leave-all time must be greater than the leave time.

Set the same GARP timer values on all Layer 2-connected devices to ensure proper operation of the GARP application.

**EXAMPLE**

The following example sets the leave timer for tengigabitethernet port 0/6 to 900 milliseconds.

```
Console(config)# interface tengigabitethernet 0/6
Console(config-if)# garp timer leave 900
```

**gvrp vlan-creation-forbid**

Use the **gvrp vlan-creation-forbid** Interface Configuration (Ethernet, Port-channel) mode command to disable dynamic VLAN creation or modification. Use the **no** form of this command to enable dynamic VLAN creation or modification.

**SYNTAX**

```
gvrp vlan-creation-forbid
no gvrp vlan-creation-forbid
```

**DEFAULT CONFIGURATION**

Dynamic VLAN creation or modification is enabled.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**EXAMPLE**

The following example disables dynamic VLAN creation on tengigabitethernet port 0/3.

```
Console(config)# interface tengigabitethernet 0/3
Console(config-if)# gvrp vlan-creation-forbid
```

**gvrp registration-forbid** Use the **gvrp registration-forbid** Interface Configuration (Ethernet, Port-channel) mode command to deregister all dynamic VLANs on a port and prevent VLAN creation or registration on the port. Use the **no** form of this command to allow dynamic registration of VLANs on a port.

#### SYNTAX

```
gvrp registration-forbid
no gvrp registration-forbid
```

#### DEFAULT CONFIGURATION

Dynamic registration of VLANs on the port is allowed.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-channel) mode

#### EXAMPLE

The following example forbids dynamic registration of VLANs on tengigabitethernet port 0/2.

```
Console(config)# interface tengigabitethernet 0/2
Console(config-if)# gvrp registration-forbid
```

**clear gvrp statistics** Use the **clear gvrp statistics** Privileged EXEC mode command to clear GVRP statistical information for all interfaces or for a specific interface.

#### SYNTAX

```
clear gvrp statistics [interface-id]
```

#### PARAMETERS

**Interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example clears all GVRP statistical information on tengigabitethernet port 0/5.

```
Console# clear gvrp statistics ethernet 5
```

**show gvrp configuration** Use the **show gvrp configuration** EXEC mode command to display GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation are enabled, and which ports are running GVRP.

#### SYNTAX

**show gvrp configuration** [*interface-id*]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays GVRP configuration information.

```

console# show gvrp configuration

GVRP Feature is currently Enabled on the device.
Maximum VLANs: 4094

Port(s) GVRP-Status Regist- Dynamic Timers(ms)
          ration   VLAN   Creation Join   Leave All
-----
te1  Enabled   Forbidden Disabled 200   600 10000
te2  Enabled   Normal   Enabled 400  1200 20000

```

**show gvrp statistics** Use the **show gvrp statistics** EXEC mode command to display GVRP statistics for all interfaces or for a specific interface.

#### SYNTAX

**show gvrp statistics** [*interface-id*]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

#### COMMAND MODE

EXEC mode

**EXAMPLE**

The following example displays GVRP statistical information.

```

Console# show gvrp statistics

GVRP statistics:
-----
Legend:
rJE : Join Empty Received      rJIn: Join In Received
rEmp: Empty Received          rLIn: Leave In Received
rLE : Leave Empty Received    rLA : Leave All Received
sJE : Join Empty Sent         sJIn: Join In Sent
sEmp: Empty Sent              sLIn: Leave In Sent
sLE : Leave Empty Sent        sLA : Leave All Sent

Port  rJE  rJIn  rEmp  rLIn  rLE  rLA  sJE  sJIn  sEmp  sLIn  sLE  sLA
----  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---
1      0    0    0    0    0    0    0    0    0    0    0    0
2      0    0    0    0    0    0    0    0    0    0    0    0
3      0    0    0    0    0    0    0    0    0    0    0    0
4      0    0    0    0    0    0    0    0    0    0    0    0
5      0    0    0    0    0    0    0    0    0    0    0    0
6      0    0    0    0    0    0    0    0    0    0    0    0
7      0    0    0    0    0    0    0    0    0    0    0    0
8      0    0    0    0    0    0    0    0    0    0    0    0

```

**show gvrp error-statistics** Use the **show gvrp error-statistics** EXEC mode command to display GVRP error statistics for all interfaces or for a specific interface.

**SYNTAX**

**show gvrp error-statistics** [*interface-id*]

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays GVRP error statistics.

```

console# show gvrp error-statistics

GVRP Error Statistics:
-----
Legend:
INVPROT : Invalid Protocol Id
INVATYP : Invalid Attribute Type  INVALEN : Invalid Attribute Length
INVAVAL : Invalid Attribute Value INVEVENT: Invalid Event

```

Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT
te1	0	0	0	0	0
te2	0	0	0	0	0
te3	0	0	0	0	0
te4	0	0	0	0	0
te5	0	0	0	0	0
te6	0	0	0	0	0
te0/7	0	0	0	0	0
te0/8	0	0	0	0	0

---

# DHCP SNOOPING AND ARP INSPECTION COMMANDS

**ip dhcp snooping** Use the **ip dhcp snooping** Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) Snooping globally. Use the **no** form of this command to restore the default configuration.

## SYNTAX

**ip dhcp snooping**  
**no ip dhcp snooping**

## DEFAULT CONFIGURATION

DHCP snooping is disabled.

## COMMAND MODE

Global Configuration mode

## USER GUIDELINES

For any DHCP Snooping configuration to take effect, DHCP Snooping must be enabled globally. DHCP Snooping on a VLAN is not active until DHCP Snooping on a VLAN is enabled by using the **ip dhcp snooping vlan** Global Configuration mode command.

## EXAMPLE

The following example enables DHCP Snooping on the device.

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

**ip dhcp snooping vlan** Use the **ip dhcp snooping vlan** Global Configuration mode command to enable DHCP Snooping on a VLAN. Use the **no** form of this command to disable DHCP Snooping on a VLAN.

## SYNTAX

**ip dhcp snooping vlan** *vlan-id*  
**no ip dhcp snooping** *vlan-id*

## PARAMETERS

**vlan-id**—Specifies the VLAN ID.

## DEFAULT CONFIGURATION

DHCP Snooping on a VLAN is disabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

DHCP Snooping must be enabled globally before enabling DHCP Snooping on a VLAN.

**EXAMPLE**

The following example enables DHCP Snooping on VLAN 21.

```
Console(config)# ip dhcp snooping vlan 21
```

**ip dhcp snooping trust**

Use the **ip dhcp snooping trust** Interface Configuration (Ethernet, Port-channel) mode command to configure a port as trusted for DHCP snooping purposes. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

**DEFAULT CONFIGURATION**

The interface is untrusted.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**USER GUIDELINES**

Configure as trusted the ports that are connected to a DHCP server or to other switches or routers. Configure the ports that are connected to DHCP clients as untrusted.

**EXAMPLE**

The following example configures tengigabitethernet port 0/5 as trusted for DHCP Snooping.

```
Console(config)# interface tengigabitethernet 0/5
Console(config-if)# ip dhcp snooping trust
```

**ip dhcp snooping information option allowed-untrusted**

Use the **ip dhcp snooping information option allowed-untrusted** Global Configuration mode command to allow a device to accept DHCP packets with option-82 information from an untrusted port. Use the **no** form of this command to drop these packets from an untrusted port.

**SYNTAX**

**ip dhcp snooping information option allowed-untrusted**  
**no ip dhcp snooping information option allowed-untrusted**

**DEFAULT CONFIGURATION**

DHCP packets with option-82 information from an untrusted port are discarded.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example allows a device to accept DHCP packets with option-82 information from an untrusted port.

```
Console(config)# ip dhcp snooping information option allowed-untrusted
```

**ip dhcp snooping verify**

Use the **ip dhcp snooping verify** Global Configuration mode command to configure a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address. Use the **no** form of this command to disable MAC address verification in a DHCP packet received on an untrusted port.

**SYNTAX**

**ip dhcp snooping verify**  
**no ip dhcp snooping verify**

**DEFAULT CONFIGURATION**

The switch verifies that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address in the packet.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example configures a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address.

```
Console(config)# ip dhcp snooping verify
```

**ip dhcp snooping database**

Use the **ip dhcp snooping database** Global Configuration mode command to enable the DHCP Snooping binding database file. Use the **no** form of this command to delete the DHCP Snooping binding database file.

**SYNTAX**

**ip dhcp snooping database**  
**no ip dhcp snooping database**

**DEFAULT CONFIGURATION**

The DHCP Snooping binding database file is not defined.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The DHCP Snooping binding database file resides on Flash.

To ensure that the lease time in the database is accurate, the Simple Network Time Protocol (SNTP) must be enabled and configured.

The device writes binding changes to the binding database file only if the device system clock is synchronized with SNTP.

**EXAMPLE**

The following example enables the DHCP Snooping binding database file.

```
Console(config)# ip dhcp snooping database
```

**ip dhcp snooping database update-freq**

Use the **ip dhcp snooping database update-freq** Global Configuration mode command to set the update frequency of the DHCP Snooping binding database file. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**ip dhcp snooping database update-freq** *seconds*  
**no ip dhcp snooping database update-freq**

**PARAMETERS**

**seconds**—Specifies the update frequency in seconds. (Range: 600–86400)

**DEFAULT CONFIGURATION**

The default update frequency value is 1200 seconds.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example sets the DHCP Snooping binding database file update frequency to 1 hour.

```
Console(config)# ip dhcp snooping database update-freq 3600
```

**ip dhcp snooping binding**

Use the **ip dhcp snooping binding** Privileged EXEC mode command to configure the DHCP Snooping binding database and add binding entries to the database. Use the **no** form of this command to delete entries from the binding database.

**SYNTAX**

```
ip dhcp snooping binding mac-address vlan-id ip-address interface-id expiry {seconds | infinite}
no ip dhcp snooping binding mac-address vlan-id
```

**PARAMETERS**

- ◆ **mac-address**— Specifies a MAC address.
- ◆ **vlan-id**— Specifies a VLAN number.
- ◆ **ip-address**— Specifies an IP address.
- ◆ **interface-id**— Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- ◆ **expiry seconds**— Specifies the time interval, in seconds, after which the binding entry is no longer valid. (Range: 10–4294967295)
- ◆ **expiry infinite**— Specifies infinite lease time.

**DEFAULT CONFIGURATION**

No static binding exists.

**COMMAND MODE**

Privileged EXEC mode

**USER GUIDELINES**

After entering this command, an entry is added to the DHCP Snooping database. If the DHCP Snooping binding file exists, the entry is also added to that file.

The entry is displayed in the show commands as a DHCP Snooping entry.

The user cannot delete dynamic temporary entries for which the IP address is 0.0.0.0.

**EXAMPLE**

The following example adds a binding entry to the DHCP Snooping binding database.

```
Console# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1 ethernet 5
        expiry 900
```

**clear ip dhcp snooping database**

Use the **clear ip dhcp snooping database** Privileged EXEC mode command to clear the DHCP Snooping binding database.

**SYNTAX**

**clear ip dhcp snooping database**

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example clears the DHCP Snooping binding database.

```
Console# clear ip dhcp snooping database
```

**show ip dhcp snooping**

Use the **show ip dhcp snooping** EXEC mode command to display the DHCP snooping configuration for all interfaces or for a specific interface.

**SYNTAX**

**show ip dhcp snooping** [*interface-id*]

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the DHCP snooping configuration.

```

console# show ip dhcp snooping
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 21
DHCP snooping database is Enabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 6666 seconds

  Interface      Trusted
  -----
te1              Yes
te2              Yes

```

### **show ip dhcp snooping binding**

Use the **show ip dhcp snooping binding** User EXEC mode command to display the DHCP Snooping binding database and configuration information for all interfaces or for a specific interface.

**SYNTAX**

```
show ip dhcp snooping binding [mac-address mac-address] [ip-address ip-address] [vlan vlan-id] [interface-id]
```

**PARAMETERS**

- ◆ **mac-address mac-address**—Specifies a MAC address.
- ◆ **ip-address ip-address**—Specifies an IP address.
- ◆ **vlan vlan-id**—Specifies a VLAN ID.
- ◆ **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

User EXEC mode

**EXAMPLE**

The following examples displays the DHCP snooping binding database and configuration information for all interfaces on a device.

```

Console# show ip dhcp snooping binding

Update frequency: 1200
Total number of binding: 2

Mac Address      IP Address      Lease      Type      VLAN      Interface
-----
0060.704C.73FF  10.1.8.1        -----   snooping   3         21
0060.704C.7BC1  10.1.8.2        7983      snooping   3         22
                                   92332      (s)

```

**ip source-guard** Use the **ip source-guard** Interface Configuration (Ethernet, Port-channel) mode command to enable IP Source Guard on an interface. Use the **no** form of this command to disable IP Source Guard on an interface.

**SYNTAX**

```

ip source-guard
no ip source-guard

```

**DEFAULT CONFIGURATION**

IP source guard is disabled.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**USER GUIDELINES**

IP Source Guard must be enabled globally before enabling IP Source Guard on an interface.

IP Source Guard is active only on DHCP snooping untrusted interfaces, and if at least one of the interface VLANs are DHCP snooping enabled.

**EXAMPLE**

The following example enables IP Source Guard on tengigabitethernet port 0/5.

```

Console(config)# interface tengigabitethernet 0/5
Console(config-if)# ip source-guard

```

**ip arp inspection** Use the **ip arp inspection** Global Configuration mode command globally to enable Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to disable ARP inspection.

#### SYNTAX

```
ip arp inspection
no ip arp inspection
```

#### DEFAULT CONFIGURATION

ARP inspection is disabled.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Note that if a port is configured as an untrusted port, then it should also be configured as an untrusted port for DHCP Snooping, or the IP-address-MAC-address binding for this port should be configured statically. Otherwise, hosts that are attached to this port cannot respond to ARPs.

#### EXAMPLE

The following example enables ARP inspection on the device.

```
Console(config)# ip arp inspection
```

**ip arp inspection vlan** Use the **ip arp inspection vlan** Global Configuration mode command to enable ARP inspection on a VLAN, based on the DHCP Snooping database. Use the **no** form of this command to disable ARP inspection on a VLAN.

#### SYNTAX

```
ip arp inspection vlan vlan-id
no ip arp inspection vlan vlan-id
```

#### PARAMETERS

**vlan-id**—Specifies the VLAN ID.

#### DEFAULT CONFIGURATION

DHCP Snooping based ARP inspection on a VLAN is disabled.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

This command enables ARP inspection on a VLAN based on the DHCP snooping database. Use the **ip arp inspection list assign** Global Configuration mode command to enable static ARP inspection.

**EXAMPLE**

The following example enables DHCP Snooping based ARP inspection on VLAN 23.

```
Console(config)# ip arp inspection vlan 23
```

**ip arp inspection trust**

Use the **ip arp inspection trust** Interface Configuration (Ethernet, Port-channel) mode command to configure an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
ip arp inspection trust
no ip arp inspection trust
```

**DEFAULT CONFIGURATION**

The interface is untrusted.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**USER GUIDELINES**

The device does not check ARP packets that are received on the trusted interface; it only forwards the packets.

For untrusted interfaces, the device intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The device drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection log-buffer vlan** Global Configuration mode command.

**EXAMPLE**

The following example configures tengigabitethernet port 0/3 as a trusted interface.

```
Console(config)# interface tengigabitethernet 0/3
Console(config-if)# ip arp inspection trust
```

**ip arp inspection validate** Use the **ip arp inspection validate** Global Configuration mode command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**ip arp inspection validate**  
**no ip arp inspection validate**

#### DEFAULT CONFIGURATION

ARP inspection validation is disabled.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The following checks are performed:

- ◆ **Source MAC address:** Compares 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.
- ◆ **Destination MAC address:** Compares the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses.
- ◆ **IP addresses:** Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

#### EXAMPLE

The following example executes ARP inspection validation.

```
Console(config)# ip arp inspection validate
```

**ip arp inspection list create** Use the **ip arp inspection list create** Global Configuration mode command to create a static ARP binding list and enters the ARP list configuration mode. Use the **no** form of this command to delete the list.

#### SYNTAX

**ip arp inspection list create** *name*  
**no ip arp inspection list create** *name*

#### PARAMETERS

**name**—Specifies the static ARP binding list name. (Length: 1–32 characters)

**DEFAULT CONFIGURATION**

No static ARP binding list exists.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Use the **ip arp inspection list assign** command to assign the list to a VLAN.

**EXAMPLE**

The following example creates the static ARP binding list 'servers' and enters the ARP list configuration mode.

```
Console(config)# ip arp inspection list create servers
Console(config-ARP-list)#
```

**ip mac** Use the **ip mac** ARP-list Configuration mode command to create a static ARP binding. Use the **no** form of this command to delete a static ARP binding.

**SYNTAX**

```
ip ip-address mac mac-address
no ip ip-address mac mac-address
```

**PARAMETERS**

- ◆ **ip-address**—Specifies the IP address to be entered to the list.
- ◆ **mac-address**—Specifies the MAC address associated with the IP address.

**DEFAULT CONFIGURATION**

No static ARP binding is defined.

**COMMAND MODE**

ARP-list Configuration mode

**EXAMPLE**

The following example creates a static ARP binding.

```
Console(config)# ip arp inspection list create servers
Console(config-ARP-list)# ip 172.16.1.1 mac 0060.704C.7321
Console(config-ARP-list)# ip 172.16.1.2 mac 0060.704C.7322
```

**ip arp inspection list assign** Use the **ip arp inspection list assign** Global Configuration mode command to assign a static ARP binding list to a VLAN. Use the **no** form of this command to delete the assignment.

#### SYNTAX

```
ip arp inspection list assign vlan-id name
no ip arp inspection list assign vlan
```

#### PARAMETERS

- ◆ **vlan-id**—Specifies the VLAN ID.
- ◆ **name**—Specifies the static ARP binding list name.

#### DEFAULT CONFIGURATION

No static ARP binding list assignment exists.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example assigns the static ARP binding list Servers to VLAN 37.

```
Console(config)# ip arp inspection list assign 37 servers
```

**ip arp inspection logging interval** Use the **ip arp inspection logging interval** Global Configuration mode command to set the minimum time interval between successive ARP SYSLOG messages. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
ip arp inspection logging interval {seconds | infinite}
no ip arp inspection logging interval
```

#### PARAMETERS

- ◆ **seconds**—Specifies the minimum time interval between successive ARP SYSLOG messages. A 0 value means that a system message is immediately generated. (Range: 0–86400)
- ◆ **infinite**—Specifies that SYSLOG messages are not generated.

#### DEFAULT CONFIGURATION

The default minimum ARP SYSLOG message logging time interval is 5 seconds.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example sets the minimum ARP SYSLOG message logging time interval to 60 seconds.

```
Console(config)# ip arp inspection logging interval 60
```

**show ip arp inspection** Use the **show ip arp inspection** EXEC mode command to display the ARP inspection configuration for all interfaces or for a specific interface.

**SYNTAX**

```
show ip arp inspection [interface-id]
```

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the ARP inspection configuration.

```
console# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 222 seconds

  Interface      Trusted
  -----
te1              Yes
te2              Yes
```

**show ip arp inspection list** Use the **show ip arp inspection list** Privileged EXEC mode command to display the static ARP binding list.

**SYNTAX**

```
show ip arp inspection list
```

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the static ARP binding list.

```

Console# show ip arp inspection list

List name: servers
Assigned to VLANs: 1,2

IP                ARP
-----
172.16.1.1        0060.704C.7322
172.16.1.2        0060.704C.7322

```

### show ip arp inspection statistics

Use the **show ip arp inspection statistics** EXEC command to display Statistics For The Following Types Of Packets That Have Been Processed By This Feature: Forwarded, Dropped, IP/MAC Validation Failure.

**SYNTAX**

**show ip arp inspection statistics** [*vlan vlan-id*]

**PARAMETERS**

**vlan-id**—Specifies VLAN ID.

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

To clear ARP Inspection counters use the **clear ip arp inspection statistics** CLI command. Counters values are kept when disabling the ARP Inspection feature.

**EXAMPLE**

```

console# show ip arp inspection statistics

Vlan  Forwarded Packets  Dropped Packets  IP/MAC Failures
----  -
2     1500                100              80

```

### clear ip arp inspection statistics

Use the **clear ip arp inspection statistics** Privileged EXEC mode command to clear statistics ARP Inspection statistics globally.

**SYNTAX**

**clear ip arp inspection statistics** [*vlan vlan-id*]

**PARAMETERS****vlan-id**—Specifies VLAN ID**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

```
console# clear ip arp inspection statistics
```

**ip dhcp information option**

Use the **ip dhcp information option** Global Configuration command to enable DHCP option-82 data insertion. Use the **no** form of this command to disable DHCP option-82 data insertion.

**SYNTAX****ip dhcp information option****no ip dhcp information option****PARAMETERS**

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

DHCP option-82 data insertion is disabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

DHCP option 82 would be enabled only if DHCP snooping or DHCP relay are enabled.

**EXAMPLE**

```
console(config)# ip dhcp information option
```

**show ip dhcp information option**

The **show ip dhcp information option** EXEC mode command displays the DHCP Option 82 configuration.

**SYNTAX****show ip dhcp information option****COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the DHCP Option 82 configuration.

```
console# show ip dhcp information option
Relay agent Information option is Enabled
```

**ip address** Use the **ip address** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to define an IP address for an interface. Use the **no** form of this command to remove an IP address definition.

#### SYNTAX

If the product is a switch router.

```
ip address ip-address {mask | prefix-length}
```

```
no ip address [ip-address]
```

If the product is a switch only.

```
ip address ip-address {mask | prefix-length} [default-gateway ip-address]
```

```
no ip address [ip-address]
```

If the product is switch only and supports a single IP address:

```
ip address ip-address {mask | prefix-length} [default-gateway ip-address]
```

```
no ip address
```

#### PARAMETERS

- ◆ **ip-address**—Specifies the IP address.
- ◆ **mask**—Specifies the network mask of the IP address.
- ◆ **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 8–30)
- ◆ **default-gateway ip-address**—Specifies the default gateway IP address.

#### DEFAULT CONFIGURATION

No IP address is defined for interfaces.

#### COMMAND MODE

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

#### USER GUIDELINES

Defining a static IP address on an interface implicitly removes the DHCP client configuration on the interface.

If the product supports multiple IP addresses:

The product supports up to x IP addresses. The IP addresses should be from different IP subnets. When adding an IP address from a subnet that already exists in the list, the new IP address replaces the existing IP address from that subnet.

If the product is switch only and supports a single IP address.

If the IP address configured in global context then it would be bound to the currently defined management interface. If the management interface is Default VLAN and the VID of the default VLAN is changed then when new setting is applied, the IP address will be automatically redefined on the new Default VLAN.

If the IP address is configured in Interface context then the IP address is bound to the interface in context.

If a static IP address is already defined, the user must do **no IP address** in the relevant interface context before changing the IP address.

If a dynamic IP address is already defined, the user must do **no ip address** in the relevant interface context before configuring another dynamic IP address.

The Interface context could be a port, LAG or VLAN, depending on support that is defined for the product.

#### EXAMPLE

The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console(config)# interface vlan 1
Console(config-if)# ip address 131.108.1.27 255.255.255.0
```

**ip address dhcp** Use the **ip address dhcp** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to acquire an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. Use the **no** form of this command to release an acquired IP address.

#### SYNTAX

```
ip address dhcp
no ip address dhcp
```

#### PARAMETERS

No parameters

**COMMAND MODE**

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

**USER GUIDELINES**

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol.

DHCP client configuration on an interface implicitly removes the static IP address configuration on the interface.

If the device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If the **ip address dhcp** command is used with or without the optional keyword, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the host name specified in the option 12 field is the globally configured device host name.

The **no ip address dhcp** command releases any IP address that was acquired, and sends a DHCPRELEASE message.

**EXAMPLE**

The following example acquires an IP address for tengigabitethernet port 0/16 from DHCP.

```
Console(config)# interface tengigabitethernet 0/16
Console(config-if)# ip address dhcp
```

**renew dhcp** Use the **renew dhcp** Privileged EXEC mode command to renew an IP address that was acquired from a DHCP server for a specific interface.

**SYNTAX**

```
renew dhcp { interface-id } [force-autoconfig]
```

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

**force-autoconfig** - In the case the DHCP server holds a DHCP option 67 record for the assigned IP address, the file would overwrite the existing device configuration

**COMMAND MODE**

Privileged EXEC mode

**USER GUIDELINES**

Note that this command does not enable DHCP on an interface. If DHCP is not enabled on the requested interface, the command returns an error message.

If DHCP is enabled on the interface and an IP address was already acquired, the command tries to renew that IP address.

If DHCP is enabled on the interface and an IP address has not yet been acquired, the command initiates a DHCP request.

**EXAMPLE**

The following example renews an IP address that was acquired from a DHCP server for VLAN 19.

```
Console# renew dhcp vlan 19
```

**ip default-gateway** The **ip default-gateway** Global Configuration mode command defines a default gateway (device). Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
ip default-gateway ip-address  
no ip default-gateway
```

**PARAMETERS**

**ip-address**—Specifies the default gateway IP address.

**COMMAND MODE**

Global Configuration mode

**DEFAULT CONFIGURATION**

No default gateway is defined.

**EXAMPLE**

The following example defines default gateway 192.168.1.1.

```
Console(config)# ip default-gateway 192.168.1.1
```

**show ip interface** Use the **show ip interface** EXEC mode command to display the usability status of configured IP interfaces.

#### SYNTAX

**show ip interface** [*interface-id* ]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the configured IP interfaces and their types.

The information on the default gateway is not shown when the device is in router mode

```

console# show ip interface

Gateway IP Address      Activity status      Type
-----
1.1.1.254                Inactive             static

IP Address              I/F                 Type                 Status
-----
1.1.1.1/8                vlan 1              Static                Valid
2.2.2.2/24               te1                  Static                Valid

```

**arp** Use the **arp** Global Configuration mode command to add a permanent entry to the Address Resolution Protocol (ARP) cache. Use the **no** form of this command to remove an entry from the ARP cache.

#### SYNTAX

**arp** *ip-address mac-address* [*interface-id*]

**no arp** *ip-address*

#### PARAMETERS

- ◆ **ip-address**—IP address or IP alias to map to the specified MAC address.
- ◆ **mac-address**—MAC address to map to the specified IP address or IP alias.

- ◆ **interface-id**—interface ID. Can be Ethernet port, Port-channel or VLAN.

#### COMMAND MODE

Global Configuration mode

#### DEFAULT CONFIGURATION

No permanent entry is defined.

#### USER GUIDELINES

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware (MAC) addresses. Because most hosts support dynamic address resolution, static ARP cache entries generally do not need to be specified.

#### Example

The following example adds IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
Console(config)# arp 198.133.219.232 00:00:0c:40:0f:bc ethernet 6
```

**arp timeout (Global)** Use the **arp timeout** Global Configuration mode command to set the time interval during which an entry remains in the ARP cache. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**arp timeout** *seconds*

**no arp timeout**

#### PARAMETERS

**seconds**—Specifies the time interval (in seconds) during which an entry remains in the ARP cache.  
(Range: 1–40000000)

#### DEFAULT CONFIGURATION

The default ARP timeout is 60000 seconds in Router mode, and 300 seconds in Switch mode.

#### COMMAND MODE

Global Configuration mode

#### EXAMPLE

The following example configures the ARP timeout to 12000 seconds.

```
Console(config)# arp timeout 12000
```

**arp timeout** Use the **arp timeout** inTeface Configuration command to configure how long an entry remains in the ARP cache for specific interface. Use the **no** form of this command restore the default value.

#### SYNTAX

```
arp timeout seconds
no arp timeout
```

#### PARAMETERS

**seconds**—Time (in seconds) that an entry remains in the ARP cache. It is recommended not to set it to less than 3600. (Range: 1–40000000)

#### DEFAULT

Defined by the **arp timeout** Global Configuration command

#### COMMAND MODE

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

#### USER GUIDELINES

This configuration can be applied only if at least one IP address defined on specific interface.

#### EXAMPLE

```
Console (config)# interface vlan 1
Console(config-if)# arp timeout 12000
```

**clear arp-cache** Use the **clear arp-cache** Privileged EXEC mode command to delete all dynamic entries from the ARP cache.

#### SYNTAX

```
clear arp-cache
```

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

The following example deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```

**show arp** Use the **show arp** Privileged EXEC mode command to display entries in the ARP table.

#### SYNTAX

```
show arp [ip-address ip-address] [mac-address mac-address]
           [interface-id]
```

#### PARAMETERS

- ◆ **ip-address ip-address**—Specifies the IP address.
- ◆ **mac-address mac-address**—Specifies the MAC address.
- ◆ **interface-id** Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

#### COMMAND MODE

Privileged EXEC mode

#### USER GUIDELINES

Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

If an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.

#### EXAMPLE

The following example displays entries in the ARP table.

```
Console# show arp

ARP timeout: 80000 Seconds

VLAN      Interface      IP Address      HW Address      Status
-----
VLAN 1    1              10.7.1.102     00:10:B5:04:DB:4B  Dynamic
VLAN 1    2              10.7.1.135     00:50:22:00:2A:A4  Static
```

**show arp configuration** Use the **show arp configuration** privileged EXEC command to display the global and interface configuration of the ARP protocol.

#### SYNTAX

```
show arp configuration
```

#### PARAMETERS

This command has no arguments or key words.

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

```

Console# show arp configuration

Global configuration:
ARP timeout:      80000 Seconds
ARP Proxy: enabled

Interface configuration:
g2:
ARP timeout:60000 Seconds
VLAN 1:
ARP Proxy: enabled
ARP timeout:      70000 Seconds
VLAN 2:
ARP Proxy: enabled
ARP timeout:80000 Second (Global)

```

**ip helper-address** Use the **ip helper-address** Global Configuration mode command to enable the forwarding of User Datagram Protocol (UDP) broadcast packets received on an interface to a specific (helper) address. Use the **no** form of this command to disable the forwarding of broadcast packets to a specific (helper) address.

**SYNTAX**

```

ip helper-address {ip-interface | all} address [udp-port-list]
no ip helper-address {ip-interface | all} address

```

**PARAMETERS**

- ◆ **ip-interface**—Specifies the IP interface.
- ◆ **all**—Specifies all IP interfaces.
- ◆ **address**—Specifies the destination broadcast or host address to which to forward UDP broadcast packets. A value of 0.0.0.0 specifies that UDP broadcast packets are not forwarded to any host.
- ◆ **udp-port-list**—Specifies the destination UDP port number to which to forward broadcast packets. (Range: 1–65535)

**DEFAULT CONFIGURATION**

Forwarding of User Datagram Protocol (UDP) broadcast packets received on an interface to a specific (helper) address is disabled.

If **udp-port-list** is not specified, packets for the default services are forwarded to the helper address.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The **ip helper-address** command forwards specific UDP broadcast packets from one interface to another.

Many helper addresses may be defined. However, the total number of address-port pairs is limited to 128 for the device.

The setting of a helper address for a specific interface has precedence over the setting of a helper address for all the interfaces.

Forwarding of BOOTP/DHCP (ports 67, 68) cannot be enabled with this command. Use the DHCP relay commands to relay BOOTP/DHCP packets.

The **ip helper-address** command specifies a UDP port number to which UDP broadcast packets with that destination port number are forwarded. By default, if no UDP port number is specified, the device forwards UDP broadcast packets for the following six services:

- ◆ IEN-116 Name Service (port 42)
- ◆ DNS (port 53)
- ◆ NetBIOS Name Server (port 137)
- ◆ NetBIOS Datagram Server (port 138)
- ◆ TACACS Server (port 49)
- ◆ Time Service (port 37)

**EXAMPLE**

The following example enables the forwarding of User Datagram Protocol (UDP) broadcasts received on all interfaces to specific UDP ports of a destination IP address.

```
Console (config)# ip helper-address all 172.16.9.9 49 53
```

**show ip helper-address** Use the **show ip helper-address** Privileged EXEC mode command to display the IP helper addresses configuration on the system.

**SYNTAX**

**show ip helper-address**

**PARAMETERS**

This command has no arguments or key words.

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example displays the IP helper addresses configuration on the system.

```

Console# show ip helper-address

Interface          Helper Address      Udp ports
-----
192.168.1.1        172.16.8.8         37, 42, 49, 53, 137, 138
192.168.2.1        172.16.9.9         37, 49

```

**ip domain lookup** Use the **ip domain lookup** Global Configuration mode command to enable the IP Domain Name System (DNS)-based host name-to-address translation. Use the **no** form of this command to disable DNS-based host name-to-address translation.

**SYNTAX**

**ip domain lookup**

**no ip domain lookup**

**DEFAULT CONFIGURATION**

IP Domain Name System (DNS)-based host name-to-address translation is enabled.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example enables IP Domain Name System (DNS)-based host name-to-address translation.

```

Console(config)# ip domain lookup

```

**ip domain name** Use the **ip domain name** Global Configuration mode command to define a default domain name used by the software to complete unqualified host names (names without a dotted-decimal domain name). Use the **no** form of this command to remove the default domain name.

**SYNTAX**

**ip domain name** *name*

**no ip domain name**

**PARAMETERS**

**name**—Specifies the default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Length: 1–158 characters. Maximum label length: 63 characters)

**DEFAULT CONFIGURATION**

A default domain name is not defined.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Domain names and host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

The maximum size of a label is 63 characters. The maximum name size is 158 bytes.

**EXAMPLE**

The following example defines the default domain name as 'www.website.com'.

```
Console(config)# ip domain name www.website.com
```

**ip name-server** Use the **ip name-server** Global Configuration mode command to define the available name servers. Use the **no** form of this command to remove a name server.

**SYNTAX**

```
ip name-server { server1-ipv4-address | server1-ipv6-address }  
[server-address2 ... server-address8]
```

```
no ip name-server [server-address ... server-address8]
```

**PARAMETERS**

**server-address**—IP addresses of the name server. Up to 8 servers can be defined in one command or by using multiple commands. The IP address can be IPv4 address or IPv6 address. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.

**DEFAULT CONFIGURATION**

No name server IP addresses are defined.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The preference of the servers is determined by the order in which they were entered.

Up to 8 servers can be defined using one command or using multiple commands.

The format of an **IPv6Z address** is: <ipv6-link-local-address>%<interface-name>

**interface-name** = vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name> | 0

**integer** = <decimal-number> | <integer><decimal-number>

**decimal-number** = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

physical-port-name= Designated port number, for example 0/16.

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

**EXAMPLE**

The following example defines the available name server.

```
Console(config)# ip name-server 176.16.1.18
```

**ip host** Use the **ip host** Global Configuration mode command to define the static host name-to-address mapping in the host cache. Use the **no** form of this command to remove the static host name-to-address mapping.

**SYNTAX**

**ip host** *name* *address* [*address2* *address3* *address4*]

**no ip host** *name*

**PARAMETERS**

- ◆ **name**—Specifies the host name. (Length: 1–158 characters. Maximum label length: 63 characters)
- ◆ **address**—Specifies the associated IP address. Up to 4 addresses can be defined.

**DEFAULT CONFIGURATION**

No host is defined.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

**EXAMPLE**

The following example defines a static host name-to-address mapping in the host cache.

```
Console(config)# ip host accounting.website.com 176.10.23.1
```

**clear host** Use the **clear host** Privileged EXEC mode command to delete entries from the host name-to-address cache.

**SYNTAX**

```
clear host {name | *}
```

**PARAMETERS**

- ◆ **name**—Specifies the host entry to remove. (Length: 1–158 characters. Maximum label length: 63 characters)
- ◆ **\*** —Removes all entries.

**COMMAND MODE**

Privileged EXEC mode

**EXAMPLE**

The following example deletes all entries from the host name-to-address cache.

```
Console# clear host *
```

**clear host dhcp** Use the **clear host dhcp** Privileged EXEC mode command to delete entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).

**SYNTAX**

```
clear host dhcp {name | *}
```

**PARAMETERS**

- ◆ **name** —Specifies the host entry to remove. (Length: 1–158 characters. Maximum label length: 63 characters)

- ◆ \*—Removes all entries.

#### COMMAND MODE

Privileged EXEC mode

#### USER GUIDELINES

This command deletes the host name-to-address mapping temporarily until the next refresh of the IP addresses.

#### EXAMPLE

The following example deletes all entries from the host name-to-address mapping received from DHCP.

```
Console# clear host dhcp *
```

**show hosts** Use the **show hosts** EXEC mode command to display the default domain name, the list of name server hosts, the static and the cached list of host names and addresses.

#### SYNTAX

```
show hosts [name]
```

#### PARAMETERS

**name**—Specifies the host name. (Length: 1–158 characters. Maximum label length: 63 characters)

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays host information.

```
Console> show hosts
```

```
System name: Device
Default domain is gm.com, sales.gm.com, usa.sales.gm.com(DHCP)
Name/address lookup is enabled
Name servers (Preference order): 176.16.1.18 176.16.1.19

Configured host name-to-address mapping:

Host                               Addresses
-----
accounting.gm.com                  176.16.8.8 176.16.8.9 (DHCP)
                                     2002:0:130F::0A0:1504:0BB4
```

Host	Total	Elapsed	Type	Addresses
-----	-----	-----	----	-----
www.stanford.edu	72	3	IP	171.64.14.203

---

**ipv6 enable** Use the **ipv6 enable** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to enable the IPv6 addressing mode on an interface. Use the **no** form of this command to disable the IPv6 addressing mode on an interface.

#### SYNTAX

**ipv6 enable** [*no-autoconfig*]

**no ipv6 enable**

#### PARAMETERS

**no-autoconfig**—EnableS processing of IPv6 on an interface without stateless address autoconfiguration procedure

#### DEFAULT CONFIGURATION

IPv6 addressing is disabled.

Unless you are using the no-autoconfig parameter, when the interface is enabled stateless address autoconfiguration procedure is enabled.

#### COMMAND MODE

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

#### USER GUIDELINES

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface, while also enabling the interface for IPv6 processing. The **no ipv6 enable** command removes the entire IPv6 interface configuration.

To enable stateless address autoconfiguration on an enabled IPv6 interface, use the IPv6 address autoconfig command.

#### EXAMPLE

The following example enables VLAN 1 for the IPv6 addressing mode.

```
Console(config)# interface vlan 1  
Console(config-if)# ipv6 enable
```

**ipv6 address autoconfig** Use the **ipv6 address autoconfig** Interface Configuration mode command to enable automatic configuration of IPv6 addresses, using stateless autoconfiguration on an interface. Addresses are configured depending on the prefixes received in Router Advertisement messages. Use the **no** form of this command to disable address autoconfiguration on the interface.

#### SYNTAX

```
ipv6 address autoconfig
no ipv6 address autoconfig
```

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT CONFIGURATION

Address autoconfiguration is enabled on the interface, no addresses are assigned by default.

#### COMMAND MODE

Interface Configuration (Ethernet, VLAN, Port-channel) mode.

#### USER GUIDELINES

When **address autoconfig** is enabled, router solicitation ND procedure is initiated to discover a router and assign IP addresses to the interface, based on the advertised on-link prefixes.

When disabling address autoconfig, automatically generated addresses that are assigned to the interface are removed.

The default state of the address autoconfig is enabled. Use the **enable ipv6 no-autoconfig** command to enable an IPv6 interface without address autoconfig.

#### EXAMPLE

```
console(config)# interface vlan 1
console(config-if)# ipv6 address autoconfig
```

**ipv6 icmp error-interval** Use the **ipv6 icmp error-interval** Global Configuration mode command to configure the rate limit interval and bucket size parameters for IPv6 Internet Control Message Protocol (ICMP) error messages. Use the **no** form of this command to return the interval to its default setting.

#### SYNTAX

```
ipv6 icmp error-interval milliseconds [bucketsize]
no ipv6 icmp error-interval
```

**PARAMETERS**

- ◆ **milliseconds**—The time interval between tokens being placed in the bucket. Each token represents a single ICMP error message. The acceptable range is from 0–2147483647 with a default of 100 milliseconds. Setting milliseconds to 0 disables rate limiting. (Range: 0– 2147483647)
- ◆ **bucketsize**—(Optional) The maximum number of tokens stored in the bucket. The acceptable range is from 1–200 with a default of 10 tokens.

**DEFAULT CONFIGURATION**

The default interval is 100ms and the default bucketsize is 10 i.e. 100 ICMP error messages per second

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

To set the average ICMP error rate limit, calculate the interval with the following formula:

Average Packets Per Second = (1/ interval) \* bucket size

**EXAMPLE**

```
console(config)# ipv6 icmp error-interval 123 45
```

**show ipv6 icmp error-interval** Use the **show ipv6 error-interval** command in the EXEC mode to display the IPv6 ICMP error interval.

**SYNTAX**

**show ipv6 icmp error-interval**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

```
Console> show ipv6 icmp error-interval
Rate limit interval: 100 ms
Bucket size: 10 tokens
```

**ipv6 address** Use the **ipv6 address** Interface Configuration mode command to configure an IPv6 address for an interface. Use the **no** form of this command To remove the address from the interface.

#### SYNTAX

```
ipv6 address ipv6-address/prefix-length [eui-64] [anycast]  
no ipv6 address [ipv6-address/prefix-length] [eui-64]
```

#### PARAMETERS

- ◆ **ipv6-address**—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
- ◆ **prefix-length**—Specifies the length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark (/) must precede the decimal.
- ◆ **eui-64**—(Optional) Builds an interface ID in the low order 64 bits of the IPv6 address based on the interface MAC address.
- ◆ **anycast**—(Optional) Indicates that this address is an anycast address.
- ◆ **prefix-length**—3–128 (64 when the **eui-64** parameter is used).

#### DEFAULT CONFIGURATION

No IP address is defined for the interface.

#### COMMAND MODE

Interface configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

#### USER GUIDELINES

If the value specified for the /prefix-length argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

Using the no IPv6 address command without arguments removes all manually configured IPv6 addresses from an interface, including link local manually configured addresses.

#### EXAMPLE

```
console(config)# interface vlan 1  
console(config-if)# ipv6 address 3000::123/64 eui-64 anycast
```

**ipv6 address link-local** Use the **ipv6 address link-local** command to configure an IPv6 link-local address for an interface. Use the **no** form of this command to return to the default link local address on the interface.

#### SYNTAX

```
ipv6 address ipv6-address/prefix-length link-local
no ipv6 address [ipv6-address/prefix-length link-local]
```

#### PARAMETERS

- ◆ **ipv6-address**—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
- ◆ **prefix-length**—Specifies the length of the IPv6 prefix. A decimal value indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark (/) must precede the decimal. Only 64-bit length is supported, according to IPv6 over Ethernet's well-known practice

#### DEFAULT CONFIGURATION

IPv6 is enabled on the interface, link local address of the interface is FE80::EUI64 (interface MAC address).

#### COMMAND MODE

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

#### USER GUIDELINES

Using the **no ipv6 link-local address** command removes the manually configured link local IPv6 address from an interface. Multiple IPv6 addresses can be configured per interface, but only one link-local address. When the **no ipv6 link-local address** command is used, the interface is reconfigured with the standard link local address (the same IPv6 link-local address that is set automatically when the **enable ipv6** command is used). The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface. To manually specify a link-local address to be used by an interface, use the **ipv6 link-local address** command. The system supports only 64 bits prefix length for link-local addresses.

#### EXAMPLE

```
console(config)# interface vlan 1
console(config-if)# ipv6 address fe80::123/64 link-local
```

**ipv6 unreachable** Use the **ipv6 unreachable** Interface Configuration mode command to enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface. Use the **no** form of this command To prevent the generation of unreachable messages.

#### SYNTAX

**ipv6 unreachable**  
**no ipv6 unreachable**

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT CONFIGURATION

ICMP unreachable messages are sent by default.

#### COMMAND MODE

Interface Configuration (Ethernet, VLAN, Port-channel) mode.

#### USER GUIDELINES

When ICMP unreachable messages are enabled, when receiving a packet addressed to one of the interface's IP address with TCP/UDP port not assigned, the device sends ICMP unreachable messages. Use the **no ipv6 unreachable** command to disable sending ICMP unreachable messages on the interface.

#### EXAMPLE

```
console(config)# interface tel
console(config-if)# ipv6 unreachable
```

**ipv6 default-gateway** Use the **ipv6 default-gateway** Global Configuration mode command to define an IPv6 default gateway. Use the **no** form of this command To remove the default gateway.

#### SYNTAX

**ipv6 default-gateway** *ipv6-address*  
**no ipv6 default-gateway**

#### PARAMETERS

**ipv6-address**—Specifies the IPv6 address of the next hop that can be used to reach that network. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the user guidelines for the interface name syntax.

#### DEFAULT CONFIGURATION

No default gateway is defined.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The format of an IPv6Z address is: <ipv6-link-local-address>%<interface-name>

**interface-name** = vlan<integer> | ch<integer> | <physical-port-name> | 0

**integer** = <decimal-number> | <integer><decimal-number>

**decimal-number** = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

**physical-port-name** = Designated port number, for example 0/16.

Configuring a new default GW without deleting the previous configured information overwrites the previous configuration. A configured default GW has a higher precedence over automatically advertised (via router advertisement message). Precedence takes effect once the configured default GW is reachable. Reachability state is not verified automatically by the neighbor discovery protocol. Router reachability can be confirmed by either receiving Router Advertisement message containing router's MAC address or manually configured by user using the IPv6 neighbor CLI command. Another option to force reachability confirmation is to ping the router link-local address (this will initiate the neighbor discovery process).

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

**EXAMPLE**

```
console(config)# ipv6 default-gateway fe80::abcd
```

**show ipv6 interface** Use the **show ipv6 interface** EXEC command mode to display the usability status of interfaces configured for IPv6.

**SYNTAX**

**show ipv6 interface** [*interface-id*]

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

**DEFAULT CONFIGURATION**

Displays all IPv6 interfaces.

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

Use the **show ipv6 neighbors** command in the privileged EXEC mode to display IPv6 neighbor discovery cache information.

**EXAMPLE**

```

Console# show ipv6 interface
Interface      IP addresses                                     Type
-----
VLAN 1         4004::55/64 [ANY]                               manual
VLAN 1         fe80::200:b0ff:fe00:0                          linklayer
VLAN 1         ff02::1                                         linklayer
VLAN 1         ff02::77                                        manual
VLAN 1         ff02::1:ff00:0                                 manual
VLAN 1         ff02::1:ff00:1                                 manual
VLAN 1         ff02::1:ff00:55                               manual

Default Gateway IP address      Type      Interface  State
-----
fe80::77                        Static    VLAN 1     unreachable
fe80::200:cff:fe4a:dfa8         Dynamic  VLAN 1     stale

Console# show ipv6 interface Vlan 15
IPv6 is disabled

Console# show ipv6 interface Vlan 1
Number of ND DAD attempts: 1
MTU size: 1500
Stateless Address Autoconfiguration state: enabled
ICMP unreachable message state: enabled
MLD version: 2

IP addresses                                     Type      DAD State
-----
4004::55/64 [ANY]                               manual    Active
fe80::200:b0ff:fe00:0                          linklayer Active
ff02::1                                         linklayer -----
ff02::77                                        manual    -----
ff02::1:ff00:0                                 manual    -----
ff02::1:ff00:1                                 manual    -----
ff02::1:ff00:55                               manual    -----

```

**show IPv6 route** Use the **show ipv6 route** command to display the current state of the IPv6 routing table.

**SYNTAX**

**show ipv6 route**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

```

Console> show ipv6 route
Codes: L - Local, S - Static, I - ICMP, ND - Router Advertisement
The number in the brackets is the metric.

```

```

S  ::/0 via fe80::77 [0] VLAN 1 Lifetime Infinite
ND  ::/0 via fe80::200:cff:fe4a:dfa8 [0] VLAN 1 Lifetime 1784 sec
L  2001::/64 is directly connected, g2 Lifetime Infinite
L  2002:1:1:1::/64 is directly connected, VLAN 1 Lifetime 2147467 sec
L  3001::/64 is directly connected, VLAN 1 Lifetime Infinite
L  4004::/64 is directly connected, VLAN 1 Lifetime Infinite
L  6001::/64 is directly connected, g2 Lifetime Infinite

```

## ipv6 nd dad attempts

Use the **ipv6 nd dad attempts** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to configure the number of consecutive neighbor solicitation messages that are sent on an interface while Duplicate Address Detection (DAD) is performed on the unicast IPv6 addresses of the interface. Use the **no** form of this command to restore the number of messages to the default value.

### SYNTAX

**ipv6 nd dad attempts** *attempts*

### PARAMETERS

**attempts**—Specifies the number of neighbor solicitation messages. A value of 0 disables DAD processing on the specified interface. A value of 1 configures a single transmission without follow-up transmissions. (Range: 0–600)

### DEFAULT CONFIGURATION

Duplicate Address Detection on unicast IPv6 addresses with the sending of one neighbor solicitation message is enabled.

### COMMAND MODE

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

### USER GUIDELINES

Duplicate Address Detection (DAD) verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while DAD is performed). DAD uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

An interface returning to the administrative Up state restarts DAD for all of the unicast IPv6 addresses on the interface. While DAD is performed on the Link Local address of an interface, the state of the other IPv6 addresses is still set to TENTATIVE. When DAD is completed on the Link Local address, DAD is performed on the remaining IPv6 addresses.

When DAD identifies a duplicate address, the address state is set to DUPLICATE and the address is not used. If the duplicate address is the Link Local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message is displayed.

All configuration commands associated with the duplicate address remain as configured while the address state is set to DUPLICATE.

If the Link Local address for an interface changes, DAD is performed on the new Link Local address and all of the other IPv6 address associated with the interface are regenerated (DAD is performed only on the new Link Local address).

Configuring a value of 0 with the **ipv6 nd dad attempts** Interface Configuration mode command disables duplicate address detection processing on the specified interface. A value of 1 configures a single transmission without follow-up transmissions. The default is 1 message.

Until the DAD process is completed, an IPv6 address is in the tentative state and cannot be used for data transfer. It is recommended to limit the configured value.

#### EXAMPLE

The following example configures the number of consecutive neighbor solicitation messages sent during DAD processing to 2 on tengigabitethernet port 0/9.

```
Console (config)# interface tengigabitethernet 0/9
Console (config-if)# ipv6 nd dad attempts 2
```

**ipv6 host** Use the **ipv6 host** Global Configuration mode command to define a static host name-to-address mapping in the host name cache. Use the **no** form of this command to remove the host name-to-address mapping.

#### SYNTAX

```
ipv6 host name ipv6-address1 [ipv6-address2...ipv6-address4]
no ipv6 host name
```

#### PARAMETERS

nameName of the host. (Range: 1–158 characters)

- ◆ **ipv6-address1**—Associated IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the user guidelines for the interface name syntax.
- ◆ **ipv6-address2-4**—(Optional) Additional IPv6 addresses that may be associated with the host's name

#### DEFAULT CONFIGURATION

No host is defined.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The format of an IPv6Z address is: <ipv6-link-local-address>%<interface-name>

**interface-name** = vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name>

**integer** = <decimal-number> | <integer><decimal-number>

**decimal-number** = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

**physical-port-name** = Designated port number, for example 0/16.

**EXAMPLE**

```
console(config)# ipv6 host server 3000::a31b
```

**ipv6 neighbor** Use the **ipv6 neighbor** command to configure a static entry in the IPv6 neighbor discovery cache. Use the **no** form of this command to remove a static IPv6 entry from the IPv6 neighbor discovery cache.

**SYNTAX**

**ipv6 neighbor** *ipv6\_addr interface-id hw\_addr*

**no ipv6 neighbor** *ipv6\_addr interface-id*

**PARAMETERS**

- ◆ **Ipv6\_addr**—Specifies the Pv6 address to map to the specified MAC address.
- ◆ **interface-id**—Specifies the interface that is associated with the IPv6 address
- ◆ **hw\_addr**—Specifies the MAC address to map to the specified IPv6 address.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The **IPv6 neighbor** command is similar to the **ARP** (global) command.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.

A new static neighbor entry with a global address can be configured only if a manually configured subnet already exists in the device.

Use the show **IPv6 neighbors** command to view static entries in the IPv6 neighbor discovery cache.

#### EXAMPLE

```
console(config)# ipv6 neighbor 3000::a31b vlan 1 001b.3f9c.84ea
```

**ipv6 set mtu** Use the **ipv6 mtu** Interface Configuration mode command to set the maximum transmission unit (MTU) size of IPv6 packets sent on an interface. Use the default parameter to restore the default MTU size.

#### SYNTAX

```
ipv6 set mtu { interface-id } { bytes | default }
```

#### PARAMETERS

- ◆ **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- ◆ **bytes**—Specifies the MTU in bytes.
- ◆ **default**—Sets the default MTU size 1500 bytes. Minimum is 1280 bytes

#### DEFAULT CONFIGURATION

1500 bytes

#### COMMAND MODE

Privileged EXEC mode

#### USER GUIDELINES

This command is intended for debugging and testing purposes and should be used only by technical support personnel.

#### EXAMPLE

```
console# ipv6 set mtu tel default
```

**ipv6 mld version** Use the **ipv6 mld version** Interface Configuration mode command to change the version of the Multicast Listener Discovery Protocol (MLD). Use the **no** form of this command to change to the default version.

#### SYNTAX

```
ipv6 mld version {1 | 2}
no ipv6 mld version
```

#### PARAMETERS

**1**—Specifies MLD version 1.

**2**—Specifies MLD version 2.

#### DEFAULT CONFIGURATION

MLD version 1.

#### COMMAND MODE

Interface Configuration (Ethernet, VLAN, Port-channel) mode

```
console(config)# interface vlan 1
console(config-if)# ipv6 mld version 2
```

**ipv6 mld join-group** Use the **ipv6 mld join-group** Interface Configuration mode command to configure Multicast Listener Discovery (MLD) reporting for a specified group. Use the **no** form of this command to cancel reporting and leave the group.

#### SYNTAX

```
ipv6 mld join-group group-address
no ipv6 mld join-group group-address
```

#### PARAMETERS

**group-address**—Specifies the IPv6 address of the multicast group.

#### DEFAULT CONFIGURATION

#### COMMAND MODE

Interface Configuration (Ethernet, VLAN, Port-channel) mode

#### USER GUIDELINES

The **ipv6 mld join-group** command configures MLD reporting for a specified group. The packets that are addressed to a specified group address will be passed up to the client process in the device.

**EXAMPLE**

The following example configures MLD reporting for specific groups:

```
console(config)# interface vlan 1
console(config-if)# ipv6 mld join-group ff02::10
```

**show ipv6 neighbors** Use the **show ipv6 neighbors** Privileged EXEC mode command to display IPv6 neighbor discovery cache information.

**SYNTAX**

```
show ipv6 neighbors {static | dynamic}[ipv6-address ipv6-address]
[mac-address mac-address] [interface-id]
```

**PARAMETERS**

- ◆ **static**—Shows static neighbor discovery cache entries.
- ◆ **dynamic**—Shows dynamic neighbor discovery cache entries.
- ◆ **ipv6-address**—Shows the neighbor discovery cache information entry of a specific IPv6 address.
- ◆ **mac-address**—Shows the neighbor discovery cache information entry of a specific MAC address.
- ◆ **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

**COMMAND MODE**

Privileged EXEC mode

**USER GUIDELINES**

Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

When an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.

The possible neighbor cache states are:

- ◆ **INCMP (Incomplete)**—Address resolution is being performed on the entry. Specifically, a Neighbor Solicitation has been sent to the solicited-node multicast address of the target, but the corresponding Neighbor Advertisement has not yet been received.
- ◆ **REACH (Reachable)**—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While REACHABLE, no special action takes place as packets are sent.

- ◆ STALE—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While stale, no action takes place until a packet is sent.
- ◆ DELAY—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly, and a packet was sent within the last DELAY\_FIRST\_PROBE\_TIME seconds. If no reachability confirmation is received within DELAY\_FIRST\_PROBE\_TIME seconds of entering the DELAY state, send a Neighbor Solicitation and change the state to PROBE.
- ◆ PROBE—A reachability confirmation is actively sought by retransmitting Neighbor Solicitations every RetransTimer milliseconds until a reachability confirmation is received.

#### EXAMPLE

```

Console# show ipv6 neighbors dynamic

Interface      IPv6 address          HW address           State Router
-----
VLAN 1         fe80::200:cff:fe4a:dfa8 00:00:0c:4a:df:a8   stale yes
VLAN 1         fe80::2d0:b7ff:fea1:264d 00:d0:b7:a1:26:4d   stale no

```

**clear ipv6 neighbors** Use the **clear ipv6 neighbors** Privileged EXEC mode command to delete all entries in the IPv6 neighbor discovery cache, except for static entries.

#### SYNTAX

**clear ipv6 neighbors**

#### PARAMETERS

This command has no keywords or arguments.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

```

console# clear ipv6 neighbors

```



## IP ROUTING PROTOCOL- INDEPENDENT COMMANDS

**ip route** Use the **ip route** Global Configuration mode command to configure static routes. Use the **no** form of this command to remove static routes.

### SYNTAX

```
ip route prefix {mask | prefix-length} ip-address [metric distance]  
[reject-route]
```

```
no ip route prefix {mask | prefix-length} [ip-address]
```

### PARAMETERS

- ◆ **prefix**—Specifies the IP address that is the IP route prefix for the destination IP.
- ◆ **mask**—Specifies the network subnet mask of the IP address prefix.
- ◆ **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- ◆ **ip-address**—Specifies the IP address or IP alias of the next hop that can be used to reach the network.
- ◆ **metric distance**—Specifies an administrative distance. (Range: 1–255)
- ◆ **reject-route**—Stops routing to the destination network via all gateways.

### DEFAULT CONFIGURATION

The default administrative distance is 1.

### COMMAND MODE

Global Configuration mode

### EXAMPLE

The following example configures a static route with prefix 172.16.0.0, prefix length 16, and gateway 131.16.1.1.

```
Console(config)# ip route 172.16.0.0 /16 131.16.1.1
```

**ip routing** Use the **ip routing** Global Configuration mode command to enable IPv4 Routing. Use the **no** format of the command to disable IPv4 Routing.

#### SYNTAX

**ip routing**  
**no ip routing**

#### DEFAULT CONFIGURATION

Enabled by default.

#### COMMAND MODE

Global Configuration mode

#### DEFAULT CONFIGURATION

No routing is defined

**show ip route** Use the **show ip route** EXEC mode command to display the current routing table state.

#### SYNTAX

**show ip route** [*connected* | *static* | {*address address* [*mask* | *prefix-length*] [*longer-prefixes*]}]

#### PARAMETERS

- ◆ **connected**—Displays connected routing entries only.
- ◆ **static**—Displays static routing entries only.
- ◆ **address address**—Specifies the address for which routing information is displayed.
- ◆ **mask**—Specifies the network subnet mask of the IP address.
- ◆ **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 1–32)
- ◆ **longer-prefixes**—Specifies that the **address** and **mask** pair becomes a prefix and any routes that match that prefix are displayed.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the current routing table state.

---

```

Console> show ip route
console# show ip route
Maximum Parallel Paths: 1 (1 after reset)

```

```

IP Forwarding:          enabled

Codes: C - connected, S - static, D - DHCP

S 0.0.0.0/0             [1/1] via 10.5.234.254 119:9:27  vlan 1
C 10.5.234.0/24        is directly connected          vlan 1
Console> show ip route address 172.1.1.0 255.255.255.0

Codes: C - connected, S - static, E - OSPF external, * - candidate default

S 172.1.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet1

Console> show ip route address 172.1.1.0 255.255.255.0 longer-prefixes
Codes: C - connected, S - static, E - OSPF external

S 172.1.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet1
S 172.1.1.1/32 [5/3] via 10.0.3.1, 19:51:18, Ethernet1

```

The following table describes the significant fields shown in the display:

Field	Description
<b>O</b>	The protocol that derived the route.
<b>10.8.1.0/24</b>	The remote network address.
<b>[30/2000]</b>	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
<b>via 10.0.1.2</b>	The address of the next router to the remote network.
<b>00:39:08</b>	The last time the route was updated, in hours:minutes:seconds.
<b>Ethernet 1</b>	The interface through which the specified network can be reached.

**interface tunnel** Use the **interface tunnel** Global Configuration mode command to enter the Interface Configuration (Tunnel) mode.

**SYNTAX**

**interface tunnel** *number*

**PARAMETERS**

**number**—Specifies the tunnel index.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example enters the Interface Configuration (Tunnel) mode.

```
Console(config)# interface tunnel 1
Console(config-tunnel)#
```

**tunnel mode ipv6ip** Use the **tunnel mode ipv6ip** Interface Configuration (Tunnel) mode command to configure an IPv6 transition-mechanism global support mode. Use the **no** form of this command to remove an IPv6 transition mechanism.

**SYNTAX**

**tunnel mode ipv6ip** *{isatap}*  
**no tunnel mode** *ipv6ip*

**PARAMETERS**

**isatap**—Enables an automatic IPv6 over IPv4 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnel.

**DEFAULT CONFIGURATION**

The IPv6 transition-mechanism global support mode is disabled.

**COMMAND MODE**

Interface Configuration (Tunnel) mode

**USER GUIDELINES**

The system can be enabled to ISATAP tunnel. When enabled, an automatic tunnel interface is created on each interface that is assigned an IPv4 address.

Note that on a specific interface (for example, port or VLAN), both native IPV6 and transition-mechanisms can coexist. The host implementation chooses the egress interface according to the scope of the destination IP address (such as ISATAP or native IPv6).

**EXAMPLE**

The following example configures an IPv6 transition mechanism global support mode.

```
Console(config)# interface tunnel 1
Console(config-tunnel)# tunnel mode ipv6ip isatap
```

**tunnel isatap router** Use the **tunnel isatap router** Interface Configuration (Tunnel) mode command to configure a global string that represents a specific automatic tunnel router domain name. Use the **no** form of this command to remove the string associated with the router domain name and restore the default configuration.

**SYNTAX**

```
tunnel isatap router router-name
no tunnel isatap router
```

**PARAMETERS**

**router-name**—Specifies the router's domain name.

**DEFAULT CONFIGURATION**

The automatic tunnel router's default domain name is ISATAP.

**COMMAND MODE**

Interface Configuration (Tunnel) mode

**USER GUIDELINES**

The **ipv6 tunnel routers-dns** command determines the string that the host uses for automatic tunnel router lookup in the IPv4 DNS procedure. By default, the string ISATAP is used for the corresponding automatic tunnel types.

Only one string can represent the automatic tunnel router name per tunnel. Using this command, therefore, overwrites the existing entry.

**EXAMPLE**

The following example configures the global string ISATAP2 as the automatic tunnel router domain name.

```
Console(config)# tunnel 1
Console(config-tunnel)# tunnel isatap router ISATAP2
```

**tunnel source** Use the **tunnel source** Interface Configuration (Tunnel) mode command to set the local (source) IPv4 address of a tunnel interface. The **no** form deletes the tunnel local address.

**SYNTAX**

```
tunnel source { auto | ipv4-address }
no tunnel source
```

**PARAMETERS**

- ◆ **auto**—The system minimum IPv4 address is used as the source address for packets sent on the tunnel interface. If the IPv4 address is changed, then the local address of the tunnel interface is changed too.
- ◆ **ip4-address**—Specifies the IPv4 address to use as the source address for packets sent on the tunnel interface. The local address of the tunnel interface is not changed when the IPv4 address is moved to another interface (only if StackTable is changed).

**DEFAULT**

No source address is defined.

**COMMAND MODE**

Interface Configuration (Tunnel) mode

**USER GUIDELINES**

The configured source IPv4 address is used for forming the tunnel interface identifier. The interface identifier is set to the 8 least significant bytes of the SIP field of the encapsulated IPv6 tunneled packets.

**EXAMPLE**

```
console(config)# interface tunnel 1
console(config-tunnel)# tunnel source auto
```

**tunnel isatap query-interval** Use the **tunnel isatap query-interval** Global Configuration mode command to set the time interval between Domain Name System (DNS) queries (before the ISATAP router IP address is known) for the automatic tunnel router domain name. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**tunnel isatap query-interval** *seconds*  
**no tunnel isatap query-interval**

#### PARAMETERS

**seconds**—Specifies the time interval in seconds between DNS queries. (Range: 10–3600)

#### DEFAULT CONFIGURATION

The default time interval between DNS queries is 10 seconds.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

This command determines the time interval between DNS queries before the ISATAP router IP address is known. If the IP address is known, the robustness level that is set by the **tunnel isatap robustness** Global Configuration mode command determines the refresh rate.

#### EXAMPLE

The following example sets the time interval between DNS queries to 30 seconds.

```
Console(config)# tunnel isatap query-interval 30
```

**tunnel isatap solicitation-interval** Use the **tunnel isatap solicitation-interval** Global Configuration mode command to set the time interval between ISATAP router solicitation messages. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**tunnel isatap solicitation-interval** *seconds*  
**no tunnel isatap solicitation-interval**

#### PARAMETERS

**seconds**—Specifies the time interval in seconds between ISATAP router solicitation messages. (Range: 10–3600)

**DEFAULT CONFIGURATION**

The default time interval between ISATAP router solicitation messages is 10 seconds.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

This command determines the interval between router solicitation messages when there is no active ISATAP router. If there is an active ISATAP router, the robustness level set by the **tunnel isatap robustness** Global Configuration mode command determines the refresh rate.

**EXAMPLE**

The following example sets the time interval between ISATAP router solicitation messages to 30 seconds.

```
Console(config)# tunnel isatap solicitation-interval 30
```

**tunnel isatap robustness**

Use the **tunnel isatap robustness** Global Configuration mode command to configure the number of DNS query/router solicitation refresh messages that the device sends. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

**tunnel isatap robustness** *number*

**no tunnel isatap robustness**

**PARAMETERS**

**number**—Specifies the number of DNS query/router solicitation refresh messages that the device sends. (Range: 1–20)

**DEFAULT CONFIGURATION**

The default number of DNS query/router solicitation refresh messages that the device sends is 3.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

The DNS query interval (after the ISATAP router IP address is known) is the Time-To-Live (TTL) that is received from the DNS, divided by (Robustness + 1).

The router solicitation interval (when there is an active ISATAP router) is the minimum-router-lifetime that is received from the ISATAP router, divided by (Robustness + 1).

**EXAMPLE**

The following example sets the number of DNS query/router solicitation refresh messages that the device sends to 5.

```
Console(config)# tunnel isatap robustness 5
```

**show ipv6 tunnel** Use the **show ipv6 tunnel** EXEC mode command to display information on the ISATAP tunnel.

**SYNTAX**

**show ipv6 tunnel**

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays information on the ISATAP tunnel.

```
Console> show ipv6 tunnel
Tunnel 1
-----

Tunnel status                : DOWN
Tunnel protocol              : NONE
Tunnel Local address type    : auto
Tunnel Local Ipv4 address    : 0.0.0.0
Router DNS name              : ISATAP
Router IPv4 address          : 0.0.0.0
DNS Query interval          : 300 seconds
Min DNS Query interval       : 0 seconds
Router Solicitation interval : 10 seconds
Min Router Solicitation interval : 0 seconds
Robustness                   : 2
```

**ip access-list extended** Use the **ip access-list** global configuration mode command to define an IPv4 access list and to place the device in IPv4 access list configuration mode. Use the **no** form of this command to remove the access list.

#### SYNTAX

```
ip access-list extended access-list-name
no ip access-list extended access-list-name
```

#### PARAMETERS

- ◆ **access-list-name**—Name of the IPv4 access list.
- ◆ **access-list-name**—0–32 characters. (Use "" for empty string)

#### DEFAULT

No IPv4 access list is defined.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

IPv4 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or Policy Map cannot have the same name.

#### EXAMPLE

```
console(config)# ip access-list extended server
```

**permit ( IP )** Use the **permit** IP Access-list Configuration mode command to set permit conditions for IPv4 access list.

#### SYNTAX

```
permit protocol {any | source source-wildcard} {any | destination
destination-wildcard} [dscp number | precedence number] [time-range
time-range-name]
permit icmp {any | source source-wildcard} {any | destination
destination-wildcard} [any | icmp-type] [any | icmp-code] [dscp
number | precedence number] [time-range time-range-name]
```

**permit igmp** *{any | source source-wildcard} {any | destination destination-wildcard} [igmp-type] [dscp number | precedence number] [time-range time-range-name]*

**permit tcp** *{any | source source-wildcard} {any|source-port/port-range}{any | destination destination-wildcard} {any|destination-port/port-range } [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name]*

**permit udp** *{any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range } [dscp number | precedence number] [match-all time-range-name] [time-range time-range-name]*

#### PARAMETERS

- ◆ **protocol**—The name or the number of an IP protocol. Available protocol names icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol use the ip keyword.(Range: 0–255)
- ◆ **source**—Source IP address of the packet.
- ◆ **source-wildcard**—Wildcard bits to be applied to the source IP address. Use ones in the bit position that you want to be ignored.
- ◆ **destination**—Destination IP address of the packet.
- ◆ **destination-wildcard**—Wildcard bits to be applied to the destination IP address. Use ones in the bit position that you want to be ignored.
- ◆ **dscp number**—Specifies the DSCP value.
- ◆ **precedence number**—Specifies the IP precedence value.
- ◆ **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- ◆ **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- ◆ **igmp-type**—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)

- ◆ **destination-port**—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177).(Range: 0-65535).
- ◆ **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0-65535)
- ◆ **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set, it is prefixed by "+". If a flag should be unset, it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- ◆ **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1-32)

**DEFAULT**

No IPv4 access list is defined.

**COMMAND MODE**

IP Access-list Configuration mode

**USER GUIDELINES**

You enter IP-access list configuration mode by using the IP Access-list Global Configuration command.

After an access control entry (ACE) is added to an access control list, an implied deny any any condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for source port in ACE it would be not be counted again if it is also used for source port in another ACE. If a range of ports is used for destination port in ACE it would be not be counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it would be counted again if it is also used for destination port.

**EXAMPLE**

```
console(config)# ip access-list extended server
console(config-ip-al)# permit ip 1.1.1.0 0.0.0.255 1.1.2.0 0.0.0.0
```

**deny ( IP )** Use the **deny** IP Access-list Configuration mode command to set deny conditions for IPv4 access list.

**SYNTAX**

**deny** *protocol* {*any* | *source source-wildcard*} {*any* | *destination destination-wildcard*} [*dscp number* | *precedence number*] [*time-range time-range-name*] [*disable-port* | *log-input*]

**deny** *icmp* {*any* | *source source-wildcard*} {*any* | *destination destination-wildcard*} {*any|icmp-type*} {*any|icmp-code*} [*dscp number* | *precedence number*] [*time-range time-range-name*] [*disable-port* | *log-input*]

**deny** *igmp* {*any* | *source source-wildcard*} {*any* | *destination destination-wildcard*} [*igmp-type*] [*dscp number* | *precedence number*] [*time-range time-range-name*] [*disable-port* | *log-input*]

**deny** *tcp* {*any* | *source source-wildcard*} {*any|source-port/port-range*} {*any* | *destination destination-wildcard*} {*any|destination-port/port-range*} [*dscp number* | *precedence number*] [*match-all list-of-flags*] [*time-range time-range-name*] [*disable-port* | *log-input*]

**deny** *udp* {*any* | *source source-wildcard*} {*any|source-port/port-range*} {*any* | *destination destination-wildcard*} {*any|destination-port/port-range*} [*dscp number* | *precedence number*] [*match-all time-range-name*] [*time-range time-range-name*] [*disable-port* | *log-input*]

**PARAMETERS**

- ◆ **protocol**—The name or the number of an IP protocol. Available protocol names: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol use the Ip keyword. (Range: 0–255)
- ◆ **source**—Source IP address of the packet.
- ◆ **source-wildcard**—Wildcard bits to be applied to the source IP address. Use 1s in the bit position that you want to be ignored.
- ◆ **destination**—Destination IP address of the packet.
- ◆ **destination-wildcard**—Wildcard bits to be applied to the destination IP address. Use 1s in the bit position that you want to be ignored.
- ◆ **dscp number**—Specifies the DSCP value.
- ◆ **precedence number**—Specifies the IP precedence value.

- ◆ **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- ◆ **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- ◆ **igmp-type**—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- ◆ **destination-port**—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp 161, snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- ◆ **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- ◆ **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set it is prefixed by "+". If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- ◆ **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- ◆ **disable-port**—The Ethernet interface is disabled if the condition is matched.
- ◆ **log-input**—Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding is done in hardware and logging is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might

not be able to match the hardware processing rate, and not all packets will be logged.

#### DEFAULT

No IPv4 access list is defined.

#### COMMAND MODE

IP Access-list Configuration mode

#### USER GUIDELINES

You enter IP-access list configuration mode by using the IP Access-list Global Configuration command.

After an access control entry (ACE) is added to an access control list, an implied deny any any condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for source port in ACE it would be not be counted again if it is also used for source port in another ACE. If a range of ports is used for destination port in ACE it would be not be counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port, it would be counted again if it is also used for destination port.

#### EXAMPLE

```
console(config)# ip access-list extended server
console(config-ip-al)# deny ip 1.1.1.0 0.0.0.255 1.1.2.0 0.0.0.0
```

**ipv6 access-list** Use the **ipv6 access-list** global configuration mode command to define an IPv6 access list and to place the device in IPv6 access list configuration mode. Use the **no** form of this command to remove the access list.

#### SYNTAX

```
ipv6 access-list [access-list-name]
no ipv6 access-list [access-list-name]
```

#### PARAMETERS

- ◆ **access-list-name**—Name of the IPv6 access list.
- ◆ **access-list-name**—0–32 characters (use "" for empty string)

#### DEFAULT

No IPv6 access list is defined.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

IPv6 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or Policy Map cannot have the same name.

Every IPv6 ACL has implicit permit icmp any any nd-ns any, permit icmp any any nd-na any, and deny ipv6 any any statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.)

The IPv6 neighbor discovery process makes use of the IPv6 network layer service, therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

**EXAMPLE**

```
Switch (config)# ipv6 access-list acl1
Switch(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/64 any any 80
```

**permit ( IPv6 )** Use the **permit** command in IPv6 Access-list Configuration mode to set permit conditions for IPv6 access list.

**SYNTAX**

**permit** *protocol* {*any* | {*source-prefix/length* } {*any* | *destination-prefix/length* } [*dscp number* | *precedence number*] [*time-range* *time-range-name*]

**permit** *icmp* {*any* | {*source-prefix/length* } {*any* | *destination-prefix/length* } {*any|icmp-type*} {*any|icmp-code*} [*dscp number* | *precedence number*] [*time-range* *time-range-name*]

**permit** *tcp* {*any* | {*source-prefix/length* } {*any* | *source-port/port-range* } } {*any* | *destination-prefix/length* } {*any* | *destination-port/port-range* } [*dscp number* | *precedence number*] [*match-all list-of-flags*] [*time-range* *time-range-name*]

**permit** *udp* {*any* | {*source-prefix/length* } } {*any* | *source-port/port-range* } } {*any* | *destination-prefix/length* } {*any* | *destination-port/port-range* } [*dscp number* | *precedence number*] [*time-range* *time-range-name*]

**PARAMETERS**

- ◆ **protocol**—The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol, use the ipv6 keyword. (Range: 0–255)

- ◆ **source-prefix/length**—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- ◆ **destination-prefix/length**—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- ◆ **dscp number**—Specifies the DSCP value. (Range: 0–63)
- ◆ **precedence number**—Specifies the IP precedence value.
- ◆ **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)
- ◆ **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- ◆ **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- ◆ **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- ◆ **match-all list-of-flag**—List of TCP flags that should occur. If a flag should be set it is prefixed by "+". If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- ◆ **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

**DEFAULT**

No IPv6 access list is defined.

**COMMAND MODE**

IPv6 Access-list Configuration mode

**USER GUIDELINES**

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for a source port in ACE it would be not be counted again if it is also used for a source port in another ACE. If a range of ports is used for destination port in ACE it would be not be counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it would be counted again if it is also used for destination port.

**EXAMPLE**

```
console(config)# ipv6 access-list server
console(config-ipv6-al)# permit tcp 3001::2/64 any any 80
```

**deny ( IPv6 )** Use the **deny** command in IPv6 access list configuration mode to set permit conditions for IPv6 access list.

**SYNTAX**

**deny** *protocol* {*any* | {*source-prefix/length* } {*any* | *destination- prefix/length* } [*dscp number* | *precedence number*] [*time-range time-range-name*] [*disable-port* | *log-input*]

**deny** *icmp* {*any* | {*source-prefix/length* } {*any* | *destination- prefix/length* } {*any|icmp-type*} {*any|icmp-code*} [*dscp number* | *precedence number*] [*time-range time-range-name*] [*disable-port* | *log-input*]

**deny** *tcp* {*any* | {*source-prefix/length* } {*any* | *source-port/port-range* } } {*any* | *destination- prefix/length* } {*any* | *destination-port/port-range*} [*dscp number* | *precedence number*] [*match-all list-of-flags*] [*time-range time-range-name*] [*disable-port* | *log-input*]

**deny** *udp* {*any* | {*source-prefix/length* } } {*any* | *source-port/port-range* } } {*any* | *destination- prefix/length* } {*any* | *destination-port/port-range*} [*dscp number* | *precedence number*] [*time-range time-range-name*] [*disable-port* | *log-input*]

**PARAMETERS**

- ◆ **protocol**—The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol use the ipv6 keyword. (Range: 0–255)
- ◆ **source-prefix/length**—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the

form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.

- ◆ **destination-prefix/length**—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- ◆ **dscp number**—Specifies the DSCP value. (Range: 0–63)
- ◆ **precedence number**—Specifies the IP precedence value.
- ◆ **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)
- ◆ **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- ◆ **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- ◆ **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- ◆ **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set it is prefixed by "+". If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- ◆ **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- ◆ **disable-port**—The Ethernet interface would be disabled if the condition is matched.

- ◆ **log-input**—Specifies to send an informational syslog message about the packet that matches the entry. Because forwarding is done in hardware and logging is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

**DEFAULT**

No IPv6 access list is defined.

**COMMAND MODE**

IPv6 Access-list Configuration mode

**USER GUIDELINES**

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for source port in ACE it would be not be counted again if it is also used for source port in another ACE. If a range of ports is used for a destination port in ACE it would be not be counted again if it is also used for a destination port in another ACE.

If a range of ports is used for source port it would be counted again if it is also used for destination port.

**EXAMPLE**

```
console(config)# ipv6 access-list server
console(config-ipv6-al)# deny tcp 3001::2/64 any any 80
```

**mac access-list** Use the **mac access-list** Global Configuration mode command to define a Layer 2 access list and to place the device in MAC access list configuration mode. Use the **no** form of this command to remove the access list.

**SYNTAX**

```
mac access-list extended access-list-name
no mac access-list extended access-list-name
```

**PARAMETERS**

**access-list-name**—Specifies the name of the MAC access list. (Range: access-list-name0–32 characters - use "" for empty string)

**DEFAULT**

No MAC access list is defined.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or Policy Map cannot have the same name.

**EXAMPLE**

```
console(config)# mac access-list extended server1
```

**permit ( MAC )** Use the **permit** command in MAC Access List Configuration mode to set permit conditions for an MAC access list,.

**SYNTAX**

```
permit {any | source source-wildcard} {any | destination
destination-wildcard} [eth-type 0| aarp | amber | dec-spanning |
decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos
cos-wildcard] [time-range time-range-name]
```

**PARAMETERS**

- ◆ **source**—Source MAC address of the packet.
- ◆ **source-wildcard**—Wildcard bits to be applied to the source MAC address. Use 1s in the bit position that you want to be ignored.
- ◆ **destination**—Destination MAC address of the packet.
- ◆ **destination-wildcard**—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- ◆ **eth-type**—The Ethernet type in hexadecimal format of the packet.
- ◆ **vlan-id**—The VLAN ID of the packet. (Range: 1-4094)
- ◆ **cos**—The Class of Service of the packet. (Range: 0-7)
- ◆ **cos-wildcard**—Wildcard bits to be applied to the CoS.
- ◆ **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1-32)

**DEFAULT**

No MAC access list is defined.

**COMMAND MODE**

MAC Access-list Configuration mode

**USER GUIDELINES**

You enter MAC-access list configuration mode by using the MAC Access-list Global Configuration command.

After an access control entry (ACE) is added to an access control list, an implied deny-any-any condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

#### EXAMPLE

```
console(config)# mac access-list extended server1
console(config-mac-acl)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

**service-acl** use the **service-acl** command in interface configuration mode to control access to an interface. Use the **no** form of this command to remove the access control.

#### SYNTAX

```
service-acl input acl-name1 [acl-name2]
no service-acl input
```

#### PARAMETERS

**acl-name**—Specifies an ACL to apply to the interface. See the usage guidelines. (Range: acl-name0–32 characters. Use "" for empty string)

#### DEFAULT

No ACL is assigned.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-Channel) mode.

Interface Configuration (Ethernet, VLAN, Port-Channel) mode.

#### USER GUIDELINES

IPv4 ACL and IPv6 ACL can be bound together to an interface.

MAC ACL cannot be bound on an interface with IPv4 ACL or IPv6 ACL.

Two ACLs of the same type can't be added to a port.

An ACL can't be added to a port that is already bounded to an ACL, without first removing the current ACL and binding the two ACLs together.

#### EXAMPLE

```
console(config)# mac access-list extended server
console(config-mac-acl)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
console(config-mac-acl)# exit
console(config)# interface tengigabitethernet 0/1
console(config-if)# service-acl input server
```

**show access-lists** Use the **show access-lists** Privileged EXEC mode command to display access control lists (ACLs) configured on the switch.

#### SYNTAX

```
show access-lists [name | access-list-number]
show access-lists time-range-active [name]
```

#### PARAMETERS

- ◆ **name**—Specifies the name of the ACL.
- ◆ **access-list-number**—Specifies the number of the IP standard ACL list.
- ◆ **time-range-active**—Shows only the Access Control Entries (ACEs) that their time-range is currently active (including those that are not associated with time-range).

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

```
Switch# show access-lists
Router# show access-lists

Standard IP access list 1
deny any
Standard IP access list 2
deny 192.168.0.0, wildcard bits 0.0.0.255
permit any
Standard IP access list 3
deny 0.0.0.0
deny 192.168.0.1, wildcard bits 0.0.0.255
permit any
Standard IP access list 4
permit 0.0.0.0
permit 192.168.0.2, wildcard bits 0.0.0.255

Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8 0.0.0.0 any

Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any time-range weekdays
permit 234 172.30.23.8 0.0.0.255 any time-range weekends

Switch# show access-lists time-range-active
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8 0.0.0.0 any

Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any time-range weekdays

Switch# show access-lists
```

**show interfaces access-lists** Use the **show interfaces access-lists** Privileged EXEC mode command to display access lists applied on interfaces.

#### SYNTAX

**show interfaces access-lists** [*interface-id* ]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

```

Console# show interfaces access-lists
Interface      Input ACL
-----
te1            ACL1
te2            ACL3
te3            blockcdp, blockvtp

```

**clear access-lists counters** Use The **Clear Access-lists Counters** Privileged EXEC mode command to clear access-lists counters.

#### SYNTAX

**clear access-lists counters** [*interface-id*]

#### PARAMETERS

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

#### COMMAND MODE

Privileged EXEC mode

#### EXAMPLE

```

console# clear access-lists counters tengigabitethernet 0/1

```

**show interfaces access-lists counters** Use the **show interfaces access-lists counters** Privileged EXEC mode command to display Access List counters.

#### SYNTAX

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

**PARAMETERS**

**interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

**COMMAND MODE**

Privileged EXEC mode

**USER GUIDELINES**

The counter of deny ACE hits counts only ACEs with the log-input keyword.

Because forwarding is done in hardware and counting is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets are counted.

**EXAMPLE**

```
console# show interfaces access-lists counters
```

Interface	deny ACE hits
-----	-----
te1	79
te2	9
te3	0

```
Number of hits that were counted in global counter (due to lack of resources)  
=19
```

## QUALITY OF SERVICE (QoS) COMMANDS

**qos** Use the **qos** Global Configuration mode command to enable Quality of Service (QoS) on the device. Use the **no** form of this command to disable QoS on the device.

### SYNTAX

```
qos [basic | advanced [ports-not-trusted | ports-trusted]]  
no qos
```

### PARAMETERS

- ◆ **basic**—QoS basic mode. If no option is specified, the QoS mode defaults to the basic mode.
- ◆ **advanced**—Specifies the QoS advanced mode, which enables the full range of QoS configuration.

*ports-not-trusted*—Relevant for advanced mode only. Indicates that packets not classified by Policy map rules to a QoS action are mapped to egress queue 0. This is the default setting in advanced mode.

*ports-trusted*—Relevant for advanced mode only. Indicates that packets not classified by Policy map rules to a QoS action are mapped to an egress queue based on the packet's fields. Use the **qos advanced-mode trust global** configuration command to specify the trust mode.

### DEFAULT CONFIGURATION

If the **qos** command is entered without any parameters, the QoS **basic** mode is enabled.

### COMMAND MODE

Global Configuration mode

### EXAMPLE

The following example enables the QoS basic mode on the device.

```
Console(config)# qos basic
```

**qos advanced-mode trust** Use the **qos advanced-mode trust** global configuration command to configure the trust mode when the default action is trust in advanced mode. Use the **no** form of this command to return to default.

#### SYNTAX

```
qos advanced-mode trust {cos | dscp | cos-dscp}
no qos advanced-mode trust
```

#### PARAMETERS

*cos*—Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.

*dscp*—Classifies ingress packets with the packet DSCP values.

*cos-dscp*—Classifies ingress packets with the packet DSCP values for IP packets. For other packet types, use the packet CoS values.

#### DEFAULT CONFIGURATION

*cos-dscp*

#### COMMAND MODE

Global configuration

#### USER GUIDELINES

The configuration is relevant for advanced mode in the following cases:

- ◆ ports-not-trusted mode: For packets that are classified to the QoS action trust.
- ◆ ports-trusted mode: For packets that are not classified by to any QoS action or classified to the QoS action trust.

#### EXAMPLE



**show qos** Use the **show qos** EXEC mode command to display the Quality of Service (QoS) mode for the device. The trust mode is displayed for the QoS basic mode.

#### SYNTAX

```
show qos
```

#### PARAMETERS

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

Disabled Command Mode

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

Trust mode is displayed if QoS is enabled in basic mode.

**EXAMPLE**

The following example displays QoS attributes when QoS is enabled in basic mode on the device and the advanced mode is supported.

```
Console> show qos
Qos: basic
Basic trust: dscp
```

```
console>show qos
Qos: Disabled
```

```
console>show qos
Qos: Basic mode
Basic trust: dscp
```

```
console>show qos
Qos: Advanced mode
Advanced mode ports state: Trusted
Advanced mode trust type: cos
```

The following example displays QoS attributes when QoS is enabled in basic mode on the device and the advanced mode is not supported.

```
Console> show qos
Qos: disable
Trust: dscp
```

**class-map** Use the **class-map** Global Configuration mode command to create or modify a class map and enters the Class-map Configuration mode. Use the **no** form of this command to delete a class map.

**SYNTAX**

```
class-map class-map-name [match-all | match-any]
```

```
no class-map class-map-name
```

**PARAMETERS**

◆ **class-map-name**—Specifies the class map name.

- ◆ **match-all**—Performs a logical AND of all the matching statements under this class map. All match criteria in this class map must be matched.
- ◆ **match-any**—Performs a logical OR of all the matching statements under this class map. One or more match criteria in this class map must be matched.

#### DEFAULT CONFIGURATION

If neither **match-all** nor **match-any** is specified, the **match-all** parameter is selected by default.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The **class-map** Global Configuration mode command specifies the name of the class map for which class-map match criteria are to be created or modified and enters class-map configuration mode. In this mode, up to two match commands can be entered to configure the match criteria for this class. When using two match commands, each has to point to a different type of ACL (one IP and one MAC). The classification is by first match, therefore, the order is important. The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-interface basis. If there is more than one match statement in a match-all class map and if there is a repetitive classification field in the participating ACLs, an error message is generated.

After entering the Quality of Service (QoS) Class-map Configuration mode, the following configuration commands are available:

**exit**: Exits the QoS Class-map Configuration mode.

**match**: Configures classification criteria.

**no**: Removes a match statement from a class map.

#### EXAMPLE

The following example creates a class map called Class1 and configures it to check that packets match all classification criteria in the class map match statement.

```
Console(config)# class-map class1 match-all
Console(config-cmap)#
```

**show class-map** The **show class-map** EXEC mode command displays all class maps.

#### SYNTAX

```
show class-map [class-map-name]
```

**PARAMETERS**

**class-map-name**—Specifies the name of the class map to be displayed.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the class map for Class1.

```
Console> show class-map class1

Class Map match-any class1 (id4)
Match Ip dscp 11 21
```

**match** Use the **match** Class-map Configuration mode command to define the match criteria for classifying traffic. Use the **no** form of this command to delete the match criteria.

**SYNTAX**

```
match access-group acl-name
no match access-group acl-name
```

**PARAMETERS**

**acl-name**—Specifies the MAC or IP Access Control List (ACL) name.

**DEFAULT CONFIGURATION**

No match criterion is supported.

**COMMAND MODE**

Class-map Configuration mode.

**EXAMPLE**

The following example defines the match criterion for classifying traffic as an access group called Enterprise in a class map called Class1.

```
Console(config)# class-map class1
Console(config-cmap)# match access-group enterprise
```

**policy-map** Use the **policy-map** Global Configuration mode command to creates a policy map and enter the Policy-map Configuration mode. Use the **no** form of this command to delete a policy map.

**SYNTAX**

```
policy-map policy-map-name
no policy-map policy-map-name
```

**PARAMETERS**

**policy-map-name**—Specifies the policy map name.

**DEFAULT CONFIGURATION**

The default behavior of the policy map is to set the DSCP value to 0 if the packet is an IP packet, and to set the CoS value to 0 if the packet is tagged.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Use the **policy-map** Global Configuration mode command to specify the name of the policy map to be created, added to, or modified before configuring policies for classes whose match criteria are defined in a class map.

Entering the **policy-map** Global Configuration mode command also enables configuring or modifying the class policies for that policy map. Class policies in a policy map can be configured only if the classes have match criteria defined for them. Use the **class-map** Global Configuration mode and **match** Class-map Configuration mode commands to configure the match criteria for a class.

The match criteria is for a class. Only one policy map per interface per direction is supported. The same policy map can be applied to multiple interfaces and directions.

**EXAMPLE**

The following example creates a policy map called Policy1 and enters the Policy-map Configuration mode.

```
Console(config)# policy-map policy1
Console(config-pmap)#
```

**class** The **class** Policy-map Configuration mode command defines a traffic classification and enters the Policy-map Class Configuration mode. Use the **no** form of this command to detach a class map from the policy map.

**SYNTAX**

```
class class-map-name [access-group acl-name]
no class class-map-name
```

**PARAMETERS**

◆ **class-map-name**—Specifies the name of an existing class map. If the class map does not exist, a new class map is created under the specified name.

- ◆ **acl-name**—Specifies the name of an IP or MAC Access Control List (ACL).

#### DEFAULT CONFIGURATION

No class map is defined for the policy map.

#### COMMAND MODE

Policy-map Configuration mode

#### USER GUIDELINES

Use the **policy-map** Global Configuration mode command to identify the policy map and to enter the Policy-map Configuration mode before using the **class** command. After specifying a policy map, a policy for new classes can be configured or a policy for any existing classes in that policy map can be modified.

Use the **service-policy** Interface Configuration (Ethernet, Port-channel) mode command to attach a policy map to an interface. Use an existing class map to attach classification criteria to the specified policy map and use the **access-group** parameter to modify the classification criteria of the class map.

If this command is used to create a new class map, the name of an IP or MAC ACL must also be specified with the **access-group** parameter.

#### EXAMPLE

The following example defines a traffic classification called Class1 with an access-group called Enterprise. The class is in a policy map called policy1.

```
Console(config)# policy-map policy1
Console(config-pmap)# class class1 access-group enterprise
```

**show policy-map** Use the **show policy-map** EXEC mode command to display all policy maps or a specific policy map.

#### SYNTAX

```
show policy-map [policy-map-name]
```

#### PARAMETERS

**policy-map-name**—Specifies the policy map name.

#### COMMAND MODE

EXEC mode

**EXAMPLE**

The following example displays all policy maps.

```

Console> show policy-map
Policy Map policy1
class class1
set Ip dscp 7
Policy Map policy2
class class 2
police 96000 4800 exceed-action drop
class class3
police 124000 96000 exceed-action policed-dscp-transmit

```

**trust** Use the **trust** Policy-map Class Configuration mode command to configure the trust state, which selects the value that QoS uses as the source of the internal DSCP value. Use the **no** form of this command to return to the default trust state.

**SYNTAX**

**trust** *cos-dscp*

**no trust**

**PARAMETERS**

**cos-dscp**—Specifies that if the packet is IP, then QoS acts as for **dscp**; otherwise QoS acts as for **cos**.

**DEFAULT CONFIGURATION**

The default state is untrusted.

If the **trust** command is specified with no parameters, the default mode is **dscp**.

**COMMAND MODE**

Policy-map Class Configuration mode

**USER GUIDELINES**

Use this command to distinguish the Quality of Service (QoS) trust behavior for certain traffic from others. For example, incoming traffic with certain DSCP values can be trusted. A class map can be configured to match and trust the DSCP values in the incoming traffic.

Trust values set with this command supersede trust values set on specific interfaces with the **qos trust** Interface Configuration mode command.

The **trust** command and the **set** Policy-map Class Configuration mode command are mutually exclusive within the same policy map.

Policy maps that contain **set** or **trust** Policy-map Class Configuration mode commands cannot be attached, or that have Access Control List (ACL)

classification to an egress interface by using the **service-policy** Interface Configuration mode command.

If specifying **trust cos**, QoS maps a packet to a queue, the received or default port CoS value, and the CoS-to-queue map.

If specifying **trust dscp**, QoS maps the packet using the DSCP value from the ingress packet.

If specifying **tcp-udp-port**, QoS maps the packet to a queue using the TCP\UDP port value from the ingress packet and the tcp-udp-port-to-queue map.

#### EXAMPLE

The following example creates an ACL, places it into a class map, places the class map into a policy map and configures the trust state using the DSCP value in the ingress packet.

```
console(config)# mac access-list extended m1
console(config-mac-acl)# permit any any
console(config-mac-acl)# exit
console(config)# class-map c1
console(config-cmap)# match access-group m1
console(config-cmap)# exit
console(config)# policy-map p1
console(config-pmap)# class c1
console(config-pmap-c)# trust cos-dscp
```

**set** Use the **set** Policy-map Class Configuration mode command to set new values in the IP packet.

#### SYNTAX

```
set {dscp new-dscp | queue queue-id | cos new-cos}
```

**no set**

#### PARAMETERS

- ◆ **dscp new-dscp**—Specifies the new DSCP value for the classified traffic. (Range: 0–63)
- ◆ **queue queue-id**—Specifies the explicit queue id to set the egress queue.
- ◆ **cos new-cos**—Specifies the new User priority to be marked in the packet. (Range: 0–7)

#### COMMAND MODE

Policy-map Class Configuration mode

**USER GUIDELINES**

This command and the **trust** Policy-map Class Configuration mode command are mutually exclusive within the same policy map.

Policy maps that contain **set** or **trust** Policy-map Class Configuration mode commands or that have ACL classifications cannot be attached to an egress interface using the Service-policy Interface Configuration mode command.

To return to the Policy-map Configuration mode, use the **exit** command. To return to the Privileged EXEC mode, use the **end** command.

**EXAMPLE**

The following example creates an ACL, places it into a class map, places the class map into a policy map and sets the DSCP value in the packet to 56 for classes in policy map called p1.

```
console(config)# mac access-list extended m1
console(config-mac-acl)# permit any any
console(config-mac-acl)# exit
console(config)# class-map c1
console(config-cmap)# match access-group m1
console(config-cmap)# exit
console(config)# policy-map p1
console(config-pmap)# class c1
console(config-pmap-c)# set dscp 56
```

**police** Use the **police** Policy-map Class Configuration mode command to define the policer for classified traffic. Use the **no** form of this command to remove a policer.

**SYNTAX**

**police** *committed-rate-kbps committed-burst-byte [exceed-action {drop | policed-dscp-transmit}]*

**no police**

**PARAMETERS**

- ◆ **committed-rate-kbps**—Specifies the average traffic rate (CIR) in kbits per second (bps). (Range: 3–12582912)
- ◆ **committed-burst-byte**—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- ◆ **exceed-action {drop | policed-dscp-transmit}**—Specifies the action taken when the rate is exceeded. The possible values are:
  - **drop**—Drops the packet.
  - **policed-dscp-transmit**—Remarks the packet DSCP, according to the policed-DSCP map as configured by the **qos map policed-dscp** Global Configuration mode command.

**COMMAND MODE**

Policy-map Class Configuration mode

**USER GUIDELINES**

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

**EXAMPLE**

The following example defines a policer for classified traffic. When the traffic rate exceeds 124,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped. The class is called Class1 and is in a policy map called Policy1.

```
Console(config)# policy-map policy1
Console(config-pmap)# class class1
Console(config-pmap-c)# police 124000 9600 exceed-action drop
```

**service-policy** Use the **service-policy** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to apply a policy map to the input of a particular interface. Use the **no** form of this command to detach a policy map from an interface.

**SYNTAX**

**service-policy input** *policy-map-name*

**no service-policy input**

**PARAMETERS**

**policy-map-name**—Specifies the policy map name to apply to the input interface. (Length: 1–32 characters)

**COMMAND MODE**

Interface Configuration (Ethernet, VLAN, Port-channel) mode

**USER GUIDELINES**

Only one policy map per interface per direction is supported.

**EXAMPLE**

The following example attaches a policy map called Policy1 to the input interface.

```
Console(config-if)# service-policy input policy1
```

**qos aggregate-policer** Use the **qos aggregate-policer** Global Configuration mode command to define the policer parameters that can be applied to multiple traffic classes. Use the **no** form of this command to remove an existing aggregate policer.

#### SYNTAX

```
qos aggregate-policer aggregate-policer-name committed-rate-kbps
excess-burst-byte [exceed-action {drop | policed-dscp-transmit}]
no qos aggregate-policer aggregate-policer-name
```

#### PARAMETERS

- ◆ **aggregate-policer-name**—Specifies the aggregate policer name.
- ◆ **committed-rate-kbps**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3–57982058)
- ◆ **excess-burst-byte**—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- ◆ **exceed-action** {**drop** | **policed-dscp-transmit**}—Specifies the action taken when the rate is exceeded. The possible values are:
  - **drop**—Drops the packet.
  - **policed-dscp-transmit**—Remarks the packet DSCP.

#### DEFAULT CONFIGURATION

No aggregate policer is defined.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Define an aggregate policer if the policer is shared with multiple classes.

Policers in one port cannot be shared with other policers in another device. Traffic from two different ports can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map. An aggregate policer cannot be applied across multiple policy maps.

An aggregate policer cannot be deleted if it is being used in a policy map. The **no police aggregate** Policy-map Class Configuration mode command must first be used to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer** command.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

#### EXAMPLE

The following example defines the parameters of a policer called Policer1 that can be applied to multiple classes in the same policy map. When the

average traffic rate exceeds 124,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped.

```
Console(config)# qos aggregate-policer policer1 124000 9600 exceed-action
drop
```

**show qos aggregate-policer** Use the **show qos aggregate-policer** EXEC mode command to display the aggregate policer parameter.

#### SYNTAX

**show qos aggregate-policer** [*aggregate-policer-name*]

#### PARAMETERS

**aggregate-policer-name**—Specifies the aggregate policer name.

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example displays the parameters of the aggregate policer called Policer1.

```
Console> show qos aggregate-policer policer1
aggregate-policer policer1 96000 4800 exceed-action drop
not used by any policy map
```

**police aggregate** Use the **police aggregate** Policy-map Class Configuration mode command to apply an aggregate policer to multiple classes within the same policy map. Use the **no** form of this command to remove an existing aggregate policer from a policy map.

#### SYNTAX

**police aggregate** *aggregate-policer-name*

**no police aggregate** *aggregate-policer-name*

#### PARAMETERS

**aggregate-policer-name**—Specifies the aggregate policer name.

#### COMMAND MODE

Policy-map Class Configuration mode

**USER GUIDELINES**

An aggregate policer can be applied to multiple classes in the same policy map. An aggregate policer cannot be applied across multiple policy maps or interfaces.

Use the **exit** command to return to the Policy-map Configuration mode. Use the **end** command to return to the Privileged EXEC mode.

**EXAMPLE**

The following example applies the aggregate policer called Policer1 to a class called Class1 in a policy map called Policy1.

```
Console(config)# policy-map policy1
Console(config-pmap)# class class1
Console(config-pmap-c)# police aggregate policer1
```

**wrr-queue cos-map** Use the **wrr-queue cos-map** Global Configuration mode command maps Class of Service (CoS) values to a specific egress queue. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
wrr-queue cos-map queue-id cos0 ... cos7
no wrr-queue cos-map [queue-id]
```

**PARAMETERS**

- ◆ **queue-id**—Specifies the queue number to which the CoS values are mapped.
- ◆ **cos0 ... cos7**—Specifies up to 7 CoS values to map to the specified queue number. (Range: 1–7)

**DEFAULT CONFIGURATION**

The default CoS value mapping to 8 queues is as follows:

CoS value 0 is mapped to queue 3.  
 CoS value 1 is mapped to queue 1.  
 CoS value 2 is mapped to queue 2.  
 CoS value 3 is mapped to queue 4.  
 CoS value 4 is mapped to queue 5.  
 CoS value 5 is mapped to queue 6.  
 CoS value 6 is mapped to queue 7.  
 CoS value 7 is mapped to queue 8.

The default CoS value mapping to 3 queues is as follows:

CoS value 0 is mapped to queue 2.  
 CoS value 1 is mapped to queue 1.  
 CoS value 2 is mapped to queue 1.  
 CoS value 3 is mapped to queue 2.

CoS value 4 is mapped to queue 2.  
 CoS value 5 is mapped to queue 3.  
 CoS value 6 is mapped to queue 3.  
 CoS value 7 is mapped to queue 3.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

Use this command to distribute traffic to different queues, where each queue is configured with different weighted round robin (WRR) and Weighted Random Early Detection (WRED) parameters.

The expedite queues are enabled using the **priority-queue out** Interface Configuration mode commands

#### EXAMPLE

The following example maps CoS value 4 to queue 2.

```
Console(config)# wrr-queue cos-map 2 7
```

### wrr-queue bandwidth

Use the **wrr-queue bandwidth** global Configuration command to assign Weighted Round Robin (WRR) weights to egress queues. The weight ratio determines the frequency at which the packet scheduler removes packets from each queue. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
wrr-queue bandwidth weight1 weight2 ... weight_n  

no wrr-queue bandwidth
```

#### PARAMETERS

**weight1 weight2 ... weight\_n**—Specifies the ratio of the bandwidth assigned by the WRR packet scheduler to the packet queues. Separate values by a space. (Range: 0–255)

#### DEFAULT CONFIGURATION

wrr is disabled by default. The default wrr weight is '1' for all queues.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The ratio for each queue is defined as the queue weight divided by the sum of all queue weights (the normalized weight). This sets the bandwidth allocation of each queue.

A weight of 0 indicates that no bandwidth is allocated for the same queue, and the shared bandwidth is divided among the remaining queues. It is not recommended to set the weight of a queue to a 0 as it might stop transmission of control-protocols packets generated by the device.

All eight queues participate in the WRR, excluding the expedite queues, in which case the corresponding weight is ignored (not used in the ratio calculation). The expedite queue is a priority queue; it is serviced until empty before the other queues are serviced. The expedite queues are enabled by using the **priority-queue out** Interface Configuration mode command.

#### EXAMPLE

The following 7 WRR queues.

```
Console(config)# wrr-queue bandwidth 6 6 6 6 6 6 6 6
```

#### priority-queue out num-of-queues

Use the **priority-queue out num-of-queues** Global Configuration mode command to configure the number of expedite queues. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
priority-queue out num-of-queues number-of-queues
no priority-queue out num-of-queues
```

#### PARAMETERS

**number-of-queues**—Specifies the number of expedite queues. Expedite queues have higher indexes. (Range: 0–8). If **number-of-queues** = 0, all queues are assured forwarding. If **number-of-queues** = 8, all queues are expedited.

#### DEFAULT CONFIGURATION

All queues are expedite queues.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

While configuring the **priority-queue num-of-queues** command, the weighted round robin (WRR) weight ratios are affected because there are fewer queues participating in WRR. This indicates that the corresponding weight in the **wrr-queue bandwidth** Interface Configuration mode command is ignored (not used in the ratio calculation).

**EXAMPLE**

The following example configures the number of expedite queues as 2.

```
Console(config)# priority-queue out num-of-queues 2
```

**traffic-shape** Use the **traffic-shape** Interface Configuration (Ethernet, Port-channel) mode command to configure the egress port shaper. Use the **no** form of this command to disable the shaper.

**SYNTAX**

**traffic-shape** *committed-rate* [*committed-burst*]

**no traffic-shape**

**PARAMETERS**

- ◆ **committed-rate**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: FE, GE: 64kbps–maximum port speed; 10GE: 64Kbps–maximum port speed)
- ◆ **committed-burst**—Specifies the excess burst size (CBS) in bytes. (Range: 4KB –16MB)

**DEFAULT CONFIGURATION**

The shaper is disabled.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**EXAMPLE**

The following example sets a shaper on tengigabitethernet port 0/5 on queue 1 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
Console(config)# interface te5
Console(config-if)# traffic-shape 1 124000 9600
```

**traffic-shape queue** Use the **traffic-shape queue** Interface Configuration (Ethernet, Port-channel) mode command to configure the egress queue shaper. Use the **no** form of this command to disable the shaper.

**SYNTAX**

**traffic-shape queue** *queue-id* *committed-rate* [*committed-burst*]

**no traffic-shape queue** *queue-id*

**PARAMETERS**

- ◆ **queue-id**—Specifies the queue number to which the shaper is assigned.
- ◆ **committed-rate**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 64 kbps–maximum port speed)
- ◆ **committed-burst**—Specifies the excess burst size (CBS) in bytes. (Range: 4 KB - 16 MB)

**DEFAULT CONFIGURATION**

The shaper is disabled.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**EXAMPLE**

The following example sets a shaper on tengigabitethernet port 0/5 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
Console(config)# interface te5
Console(config-if)# traffic-shape 124000 9600
```

**rate-limit (Ethernet)** Use the **rate-limit** Interface Configuration (Ethernet) mode command to limit the incoming traffic rate on a port. Use the **no** form of this command to disable the rate limit.

**SYNTAX**

**rate-limit** *committed-rate-kbps [burst committed-burst-byte]*  
**no rate-limit**

**PARAMETERS**

- ◆ **rate**—Specifies the maximum number of kilobits per second of ingress traffic on a port. The range is 3–10000000.
- ◆ **burst bytes**—The burst size in bytes (3000–19173960). If unspecified, defaults to 128K.

**DEFAULT CONFIGURATION**

Rate limiting is disabled.

**COMMAND MODE**

Interface Configuration (Ethernet) mode

**USER GUIDELINES**

- ◆ Storm control and rate-limit (of unicast packets) can't be enabled simultaneously on the same port.

**EXAMPLE**

The following example limits the incoming traffic rate on tengigabitethernet port 0/5 to 150,000 kbps.

```
Console(config)# interface te5
Console(config-if)# rate-limit 150000
```

**rate-limit (VLAN)** Use the **rate-limit** (VLAN) Global Configuration mode command to limit the incoming traffic rate for a VLAN. Use the **no** form of this command to disable the rate limit.

**SYNTAX**

```
rate-limit vlan-id committed-rate committed-burst
no rate-limit vlan
```

**PARAMETERS**

- ◆ **vlan-id**—Specifies the VLAN ID.
- ◆ **committed-rate**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3–8000000)
- ◆ **committed-burst**—Specifies the maximum burst size (CBS) in bytes. (Range: 3000–19173960)

**DEFAULT CONFIGURATION**

Rate limiting is disabled.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

Traffic policing in a policy map takes precedence over VLAN rate limiting. If a packet is subject to traffic policing in a policy map and is associated with a VLAN that is rate limited, the packet is counted only in the traffic policing of the policy map.

**EXAMPLE**

The following example limits the rate on VLAN 11 to 150000 kbps or the normal burst size to 9600 bytes.

```
Console(config)# rate-limit 11 150000 9600
```

**qos wrr-queue wrtd** Use the **qos wrr-queue wrtd** Global Configuration mode command to enable Weighted Random Tail Drop (WRTD). Use the **no** form of this command to disable WRTD.

#### SYNTAX

```
qos wrr-queue wrtd
no qos wrr-queue wrtd
```

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT

Disabled

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

The command is effective after reset.

**show qos interface** Use the **show qos interface** EXEC mode command to display Quality of Service (QoS) information on the interface.

#### SYNTAX

```
show qos interface [buffers | queueing | policers | shapers | rate-limit] [interface-id]
```

#### PARAMETERS

- ◆ **buffers**—Displays the buffer settings for the interface's queues. For GE ports, displays the queue depth for each of the 8 queues. For FE ports, displays the minimum reserved setting.
- ◆ **queueing**—Displays the queue's strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.
- ◆ **policers**—Displays all the policers configured for this interface, their settings, and the number of policers currently unused.
- ◆ **shapers**—Displays the shaper of the specified interface and the shaper for the queue on the specified interface.
- ◆ **rate-limit**—Displays the rate-limit configuration.
- ◆ **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, or Port-channel.

#### DEFAULT CONFIGURATION

There is no default configuration for this command.

**COMMAND MODE**

EXEC mode

**USER GUIDELINES**

The **policers** option is relevant for a VLAN interface only.

If no parameter is specified with the **show qos interface** command, the port QoS mode (DSCP trusted, CoS trusted, untrusted, and so on), default CoS value, DSCP-to-DSCP- map (if any) attached to the port, and policy map (if any) attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

**EXAMPLE**

This is an example of the output from the **show qos interface buffers** command for 8 queues.

```

Console> show qos interface buffers tel
tel
Notify Q depth:
buffers gi2/0/1
Ethernet gi2/0/1

qid  thresh0  thresh1  thresh2
1    100      100      80
2    100      100      80
3    100      100      80
4    100      100      80
5    100      100      80
6    100      100      80
7    100      100      80
8    100      100      80

```

This is an example of the output from the **show qos interface shapers** command for 8 queues.

```

Console> show qos interface shapers tel
tengigabitethernet 0/1
Port shaper: enable
Committed rate: 192000 bps
Committed burst: 9600 bytes

      QID      Status      Target
              Committed
              Rate [bps]
      Target
      Committed
      Burst [bytes]
1      Enable      100000
2      Disable     N/A
3      Enable      200000
4      Disable     N/A
5      Disable     N/A
6      Disable     N/A
7      Enable      178000
8      Enable      23000

```

This is an example of the output from the **show qos interface policer** command.

```

Console> show qos interface policer te1
Ethernet te1
Class map: A
Policer type: aggregate
Committed rate: 192000 bps
Committed burst: 9600 bytes
Exceed-action: policed-dscp-transmit

Class map: B
Policer type: single
Committed rate: 192000 bps
Committed burst: 9600 bytes
Exceed-action: drop

Class map: C
Policer type: none
Committed rate: N/A
Committed burst: N/A
Exceed-action: N/A

```

This is an example of the output from the **show qos interface rate-limit** command.

```

Console> show qos interface rate-limit te1

Port          rate-limit [kbps]          Burst [KBytes]
-----          -
te1           1000                      512K

```

**wrr-queue** Use the **wrr-queue** Global Configuration mode command to enable the tail-drop mechanism on an egress queue. Use the **no** form of this command to disable the tail-drop mechanism on an egress queue.

#### SYNTAX

**wrr-queue** *tail-drop*

**no wrr-queue**

#### PARAMETERS

**tail-drop**— Specifies the tail-drop mechanism.

#### DEFAULT CONFIGURATION

The tail-drop mechanism on an egress queue is disabled.

#### COMMAND MODE

Global Configuration mode

**USER GUIDELINES**

This command can only be used if Advanced mode is enabled.

**EXAMPLE**

The following example enables the tail-drop mechanism on an egress queue.

```
Console(config)# wrr-queue tail-drop
```

**qos wrr-queue threshold**

Use the **qos wrr-queue threshold** Global Configuration mode command to assign queue thresholds globally. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
qos wrr-queue threshold tengigabitethernet queue-id threshold-percentage
```

```
no qos wrr-queue threshold tengigabitethernet queue-id
```

**PARAMETERS**

- ◆ **queue-id**—Specifies the queue number to which the tail-drop threshold is assigned.
- ◆ **threshold-percentage**—Specifies the queue threshold percentage value.

**DEFAULT CONFIGURATION**

The default threshold is 80 percent.

**COMMAND MODE**

Global Configuration mode

**USER GUIDELINES**

If the threshold is exceeded, packets with the corresponding DP are dropped until the threshold is no longer exceeded.

**EXAMPLE**

The following example assigns a threshold of 80 percent to WRR queue 1.

```
Console(config)# qos wrr-queue threshold tengigabitethernet 1 80
```

**qos map policed-dscp** Use the **qos map policed-dscp** Global Configuration mode command to configure the policed-DSCP map for remarking purposes. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
qos map policed-dscp dscp-list to dscp-mark-down
no qos map policed-dscp [dscp-list]
```

#### PARAMETERS

- ◆ **dscp- list**—Specifies up to 8 DSCP values, separated by spaces. (Range: 0–63)
- ◆ **dscp-mark-down**—Specifies the DSCP value to mark down. (Range: 0–63)

#### DEFAULT CONFIGURATION

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

#### COMMAND MODE

Global Configuration mode.

#### EXAMPLE

The following example marks incoming DSCP value 3 as DSCP value 43 on the policed-DSCP map.

```
Console(config)# qos map policed-dscp 3 to 43
Reserved DSCP. DSCP 3 was not configured.
```

**qos map dscp-queue** Use the **qos map dscp-queue** Global Configuration mode command to configure the DSCP to CoS map. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

```
qos map dscp-queue dscp-list to queue-id
no qos map dscp-queue [dscp-list]
```

#### PARAMETERS

- ◆ **dscp-list**—Specifies up to 8 DSCP values, separated by spaces. (Range: 0– 63)
- ◆ **queue-id**—Specifies the queue number to which the DSCP values are mapped.

**DEFAULT CONFIGURATION**

The default map for 8 queues is as follows.

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-56	57-63
Queue-ID	1	2	3	4	5	6	7	8

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
Console(config)# qos map dscp-queue 33 40 41 to 1
```

**qos map dscp-dp** Use the **qos map dscp-dp** Global Configuration mode command to map the DSCP to Drop Precedence. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
qos map dscp-dp dscp-list to dp
no qos map dscp-dp [dscp-list]
```

**PARAMETERS**

- ◆ **dscp-list**—Specifies up to 8 DSCP values, with values separated by a space. (Range: 0–63)
- ◆ **dp**—Specifies the Drop Precedence value to which the DSCP values are mapped. (values: 0,2) where 2 is the highest Drop Precedence)

**DEFAULT CONFIGURATION**

All the DSCPs are mapped to Drop Precedence 0.

**COMMAND MODE**

Global Configuration mode.

**EXAMPLE**

The following example maps DSCP values 25, 27 and 29 to Drop Precedence 2.

```
Console(config)# qos map dscp-dp 25 27 29 to 2
```

**qos trust (Global)** Use the **qos trust** Global Configuration mode command to configure the system to the basic mode and trust state. Use the **no** form of this command to return to the default configuration.

#### SYNTAX

```
qos trust {cos | dscp}
no qos trust
```

#### PARAMETERS

- ◆ **cos**— Specifies that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- ◆ **dscp**— Specifies that ingress packets are classified with packet DSCP values.

#### DEFAULT CONFIGURATION

CoS is the default trust mode.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

This command can be used only in QoS basic mode.

Packets entering a quality of service (QoS) domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When the system is configured with trust DSCP, the traffic is mapped to the queue by the DSCP-queue map.

When the system is configured with trust CoS, the traffic is mapped to the queue by the CoS-queue map.

#### EXAMPLE

The following example configures the system to the DSCP trust state.

```
Console(config)# qos trust dscp
```

**qos trust (Interface)** Use the **qos trust** Interface Configuration (Ethernet, Port-channel) mode command to enable each port trust state while the system is in the basic QoS mode. Use the **no** form of this command to disable the trust state on each port.

#### SYNTAX

**qos trust**  
**no qos trust**

#### DEFAULT CONFIGURATION

Each port is enabled while the system is in basic mode.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-channel) mode

#### EXAMPLE

The following example configures tengigabitethernet port 0/15 to the default trust state.

```
Console(config)# interface te15
Console(config-if)# qos trust
```

**qos cos** Use the **qos cos** Interface Configuration (Ethernet, Port-channel) mode command to define the default CoS value of a port. Use the **no** form of this command to restore the default configuration.

#### SYNTAX

**qos cos** *default-cos*  
**no qos cos**

#### PARAMETERS

**default-cos**—Specifies the default CoS value of the port. If the port is trusted and the packet is untagged, then the default CoS value become the CoS value. (Range: 0–7)

#### DEFAULT CONFIGURATION

The default CoS value of a port is 0.

#### COMMAND MODE

Interface Configuration (Ethernet, Port-channel) mode

#### USER GUIDELINES

Use the default CoS value to assign a CoS value to all untagged packets entering the port. Use the **qos cos override** command to assign this default CoS value to tagged packets.

**EXAMPLE**

The following example defines the port `te15` default CoS value as 3 .

```
Console(config)# interface te15
Console(config-if)# qos cos 3
```

**qos dscp-mutation** Use the **qos dscp-mutation** Global Configuration mode command to apply the DSCP Mutation map to system DSCP trusted ports. Use the **no** form of this command to restore the trusted port with no DSCP mutation.

**SYNTAX**

```
qos dscp-mutation
no qos dscp-mutation
```

**COMMAND MODE**

Global Configuration mode.

**USER GUIDELINES**

Apply the DSCP-to-DSCP-mutation map to a port at the boundary of a Quality of Service (QoS) administrative domain. If two QoS domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition of another domain. Apply the map to ingress and to DSCP-trusted ports only. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports. If applying the DSCP mutation map to an untrusted port, to class of service (CoS), or to an IP-precedence trusted port, the command has no immediate effect until the port becomes DSCP-trusted.

**EXAMPLE**

The following example applies the DSCP Mutation map to system DSCP trusted ports.

```
Console(config)# qos dscp-mutation
```

**qos map dscp-mutation** Use the **qos map dscp-mutation** Global Configuration mode command to configure the DSCP to DSCP Mutation table. Use the **no** form of this command to restore the default configuration.

**SYNTAX**

```
qos map dscp-mutation in-dscp to out-dscp
no qos map dscp-mutation [in-dscp]
```

**PARAMETERS**

- ◆ **in-dscp**—Specifies up to 8 DSCP values to map, separated by spaces. (Range: 0–63)
- ◆ **out-dscp**—Specifies up to 8 DSCP mapped values, separated by spaces. (Range: 0–63)

**DEFAULT CONFIGURATION**

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

**COMMAND MODE**

Global Configuration mode.

**USER GUIDELINES**

This is the only map that is not globally configured. It is possible to have several maps and assign each one to a different port.

**EXAMPLE**

The following example changes DSCP values 1, 2, 4, 5 and 6 to DSCP Mutation Map value 63.

```
Console(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

**show qos map** Use the **show qos map** EXEC mode command to display the QoS mapping information.

**SYNTAX**

```
show qos map [dscp-queue | dscp-dp | policed-dscp | dscp-  
mutation]
```

**PARAMETERS**

- ◆ **dscp-queue**—Displays the DSCP to queue map.
- ◆ **dscp-dp**—Displays the DSCP to Drop Precedence map.
- ◆ **policed-dscp**—Displays the DSCP to DSCP remark table.
- ◆ **dscp-mutation**—Displays the DSCP-DSCP mutation table.

**COMMAND MODE**

EXEC mode

**EXAMPLE**

The following example displays the QoS mapping information.

```
Console> show qos map
```

```
Dscp-queue map:
```

d1	:	d2	0	1	2	3	4	5	6	7	8	9
0	:		01	01	01	01	01	01	01	01	02	02
1	:		02	02	02	02	02	02	03	03	03	03
2	:		03	03	03	03	04	04	04	04	04	04
3	:		04	04	05	05	05	05	05	05	05	05
4	:		06	06	06	06	06	06	06	06	07	07
5	:		07	07	07	07	07	07	08	08	08	08
6	:		08	08	08	08						

The following table appears:

```
Dscp-DP map:
```

d1	:	d2	0	1	2	3	4	5	6	7	8	9
0	:		00	00	00	00	00	00	00	00	00	00
1	:		00	00	00	00	00	00	00	00	00	00
2	:		00	00	00	00	00	00	00	00	00	00
3	:		00	00	00	00	00	00	00	00	00	00
4	:		00	00	00	00	00	00	00	00	00	00
5	:		00	00	00	00	00	00	00	00	00	00
6	:		00	00	00	00						

The following table appears:

```
Policed-dscp map:
```

d1	:	d2	0	1	2	3	4	5	6	7	8	9
0	:		00	01	02	03	04	05	06	07	08	09
1	:		10	11	12	13	14	15	16	17	18	19
2	:		20	21	22	23	24	25	26	27	28	29
3	:		30	31	32	33	34	35	36	37	38	39
4	:		40	41	42	43	44	45	46	47	48	49
5	:		50	51	52	53	54	55	56	57	58	59
6	:		60	61	62	63						

The following table appears:

Dscp-dscp mutation map:												
d1	:	d2	0	1	2	3	4	5	6	7	8	9
--	--	--	--	--	--	--	--	--	--	--	--	--
0	:		00	01	02	03	04	05	06	07	08	09
1	:		10	11	12	13	14	15	16	17	18	19
2	:		20	21	22	23	24	25	26	27	28	29
3	:		30	31	32	33	34	35	36	37	38	39
4	:		40	41	42	43	44	45	46	47	48	49
5	:		50	51	52	53	54	55	56	57	58	59
6	:		60	61	62	63						

**clear qos statistics** Use the **clear qos statistics** EXEC mode command to clear the QoS statistics counters.

#### SYNTAX

**clear qos statistics**

#### COMMAND MODE

EXEC mode

#### EXAMPLE

The following example clears the QoS statistics counters.

```
Console# clear qos statistics
```

**qos statistics policer** Use the **qos statistics policer** Interface Configuration (Ethernet, Port-channel) mode command to enable counting in-profile and out-of-profile. Use the **no** form of this command to disable counting.

#### SYNTAX

**qos statistics policer** *policy-map-name class-map-name*

**no qos statistics policer** *policy-map-name class-map-name*

#### PARAMETERS

◆ **policy-map-name**—Specifies the policy map name.

◆ **class-map-name**—Specifies the class map name.

#### DEFAULT CONFIGURATION

Counting in-profile and out-of-profile is disabled.

**COMMAND MODE**

Interface Configuration (Ethernet, Port-channel) mode

**EXAMPLE**

The following example enables counting in-profile and out-of-profile on the interface.

```
Console(config-if)# qos statistics policer policy1 class1
```

**qos statistics aggregate-policer**

Use the **qos statistics aggregate-policer** Global Configuration mode command to enable counting in-profile and out-of-profile. Use the **no** form of this command to disable counting.

**SYNTAX**

```
qos statistics aggregate-policer aggregate-policer-name
no qos statistics aggregate-policer aggregate-policer-name
```

**PARAMETERS**

**aggregate-policer-name**—Specifies the aggregate policer name.

**DEFAULT CONFIGURATION**

Counting in-profile and out-of-profile is disabled.

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

The following example enables counting in-profile and out-of-profile on the interface.

```
Console(config)# qos statistics aggregate-policer policer1
```

**qos statistics queues**

Use the **qos statistics queues** Global Configuration mode command to enable QoS statistics for output queues. Use the **no** form of this command to disable QoS statistics for output queues.

**SYNTAX**

```
qos statistics queues set {queue | all} {dp | all} {interface | all}
no qos statistics queues set
```

**PARAMETERS**

◆ **set**—Specifies the counter set number.

- ◆ **interface**—Specifies the Ethernet port.
- ◆ **queue**—Specifies the output queue number.
- ◆ **dp**—Specifies the drop precedence. The available values are: **high**, **low**.

#### DEFAULT CONFIGURATION

Set 1: All interfaces, all queues, high DP.

Set 2: All interfaces, all queues, low DP.

#### COMMAND MODE

Global Configuration mode

#### USER GUIDELINES

There are no user guidelines for this command.

#### EXAMPLE

The following example enables QoS statistics for output queues for counter set 1.

```
Console(config)# qos statistics queues 1 all all all
```

**show qos statistics** Use the **show qos statistics** EXEC mode command to display Quality of Service statistical information.

#### SYNTAX

**show qos statistics**

#### COMMAND MODE

EXEC mode

#### USER GUIDELINES

Up to 16 sets of counters can be enabled for policers. The counters can be enabled in the creation of the policers.

Use the **qos statistics queues** Global Configuration mode command to enable QoS statistics for output queues.

**EXAMPLE**

The following example displays Quality of Service statistical information.

```
Console# show qos statistics
```

```
Policers
```

```
-----
```

Interface	Policy map	Class Map	In-profile bytes	Out-of-profile bytes
-----	-----	-----	-----	-----
te1	Policy1	Class1	7564575	5433
te1	Policy1	Class2	8759	52
te2	Policy1	Class1	746587458	3214
te2	Policy1	Class2	5326	23

```
Aggregate Policers
```

```
-----
```

Name	In-profile bytes	Out-of-profile bytes
-----	-----	-----
Policer1	7985687	121322

```
Output Queues
```

```
-----
```

Interface	Queue	DP	Total packets	%TD packets
-----	-----	--	-----	-----
te1	2	High	799921	1.2%
te2	All	High	5387326	0.2%



# DATA CENTER ETHERNET COMMANDS

## **dce priority-flow-control enable** (Global)

Use the **dce priority-flow-control enable** global configuration command to globally enable the Priority Flow Control feature. Use the **no** form of this command to disable Priority Flow Control.

### SYNTAX

**dce priority-flow-control enable**  
**no dce priority-flow-control enable**

### DEFAULT CONFIGURATION

Disabled.

### COMMAND MODE

Global Configuration mode.

### DEFAULT CONFIGURATION

Disabled

### USER GUIDELINES

When priority-flow-control (PFC) is disabled on the switch, all interfaces use IEEE 802.3x flow control.

### EXAMPLE

```
console(config)# dce priority-flow-control enable
```

## **dce priority-flow-control priority enable**

Use the **dce priority-flow-control priority enable** global configuration command to enable priority flow control for a priority. Use the **no** form of this command to disable priority flow control.

### SYNTAX

**dce priority-flow-control priority *priority* enable**  
**no dce priority-flow-control priority *priority* enable**

### PARAMETERS

*priority*—802.1Q Priority, range 0–7

### COMMAND MODE

Global configuration mode

**DEFAULT CONFIGURATION**

Disabled

**USER GUIDELINES**

Priority-Flow-Control can be enabled for a priority, only if that priority is mapped (by the priority2queue mapping table) to a dedicated queue (I.e. no other priority is mapped to that queue). If Priority-Flow-Control Priority is enabled for a priority, then that priority cannot be mapped to a queue that is already shared by other priorities.

**EXAMPLE**

```
console(config)# dce priority-flow-control priority 7 enable
```

**dce priority-flow-control enable (interface)**

Use the **dce priority-flow-control enable** interface configuration command to enable the Priority Flow Control feature for an interface. Use the **no** form of this command to disable Priority Flow Control.

**SYNTAX**

```
dce priority-flow-control enable
no dce priority-flow-control enable
```

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

Disabled Command Mode

Interface configuration (Etherment) mode

**USER GUIDELINES**

Use the **dce priority-flow-control enable** global configuration command to globally enable PFC.

Use the **dce priority-flow-control priority enable** global configuration command to determine on which priorities to enable PFC.

**EXAMPLE**

```
console(config-if)# dce priority-flow-control enable
```

**show dce priority-flow-control** To display the information on Priority Flow Control, use the **show dce priority-flow-control** command in EXEC mode.

#### SYNTAX

```
show dce priority-flow-control [interface-id]
```

#### PARAMETERS

*interface-id*—Specifies an interface ID. The interface ID must be an Ethernet port.

#### COMMAND MODE

Privileged EXEC

#### EXAMPLE

```
console# show dce priority-flow-control
```

```
PFC is globally enabled
```

Priority	PFC Admin	PFC Oper
0	Disabled	Disabled
1	Disabled	Disabled
2	Disabled	Disabled
3	Disabled	Disabled
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Enabled	Enabled

Interface	PFC Admin	PFC Oper
te0/1	Enabled	Disabled
te0/2	Disabled	Disabled
te0/3	Disabled	Disabled
te0/4	Disabled	Disabled
te0/5	Disabled	Disabled
.		
.		
.		
te0/47	Disabled	Disabled
te0/48	Disabled	Disabled

**dce qcn enable (global)** Use the **dce qcn enable** global configuration command to enable Quantized Congestion Notification (QCN) feature. Use the **no** form of this command to disable QCN.

#### SYNTAX

```
dce qcn enable
```

```
no dce qcn enable
```

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

Disabled

**COMMAND MODE**

Global configuration

**USER GUIDELINES**

Enable the QCN feature to throttle traffic at the edge of the network when there is congestion.

**EXAMPLE**

```
console(config)# dce qcn enable
```

**dce qcn priority enable**

Use the **dce qcn priority enable** global configuration command to enable Quantized Congestion Notification (QCN) for a priority. Use the **no** form of this command to disable QCN for a priority.

**SYNTAX**

**dce qcn priority *priority* enable**

**no dce qcn priority *priority* enable**

**PARAMETERS**

*priority*—802.1Q Priority, range 0–7

**DEFAULT CONFIGURATION**

Disabled

**COMMAND MODE**

Global configuration

**USER GUIDELINES**

QCN can be enabled up to 7 priorities.

QCN can't be enabled for a priority that is mapped to Queue 0.

QCN Operating state is enabled for a priority only if that priority is mapped (by the `priority2queue` mapping function) to a queue that is not associated with non-QCN priorities. i.e. non-QCN priorities are not mapped to that queue.



**NOTE:** Multiple QCN priorities can be mapped to the same queue.

**EXAMPLE**

```
console(config)# dce qcn priority 7 enable
```

**dce qcn cnm priority** Use the **dce qcn cnm priority** global configuration command to configure the priority to use for all Congestion Notification Messages (CNMs) transmitted by the device. Use the no form of this command to return to default.

**SYNTAX**

```
dce qcn cnm priority priority
no dce qcn cnm priority
```

**PARAMETERS**

*priority*—802.1Q Priority, range 0–7

**DEFAULT CONFIGURATION**

6

**COMMAND MODE**

Global configuration

**EXAMPLE**

```
console(config)# dce qcn cnm priority 7
```

**dce qcn cp enable** Use the **dce qcn cp enable** interface configuration command to enable Congestion Point (CP) creation for an interface. Use the no form of this command to disable CP creation for an interface.

**SYNTAX**

```
dce qcn cp enable
no dce qcn cp enable
```

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

Disabled

**COMMAND MODE**

Interface configuration (Ethernet)

**USER GUIDELINES**

If CP creation is enabled for an interface, the system automatically creates a Congestion Point (CP) for a queue of that interface if at least QCN priority (Oper state) is mapped to that queue.

**EXAMPLE**

```
console(config-if)# dce qcn cp enable
```

**dce qcn cp set-point** Use the **dce qcn cp set-point** global configuration command to configure the QCN set-point of an egress queue. Use the **no** form of this command to return to default.

**SYNTAX**

**dce qcn cp set-point** *bytes*

**no dce qcn cp set-point**

**PARAMETERS**

*bytes*—Specifies the set point in bytes. The value should be a multiple of 512

Range 512–4294966784

**DEFAULT CONFIGURATION**

Product-specific, should be 20% of the queue size

**COMMAND MODE**

Global configuration

**EXAMPLE**

```
console(config)# dce qcn cp set-point 1024
```

**dce qcn cp feedback-weight** Use the **dce qcn cp feedback-weight** global configuration command configures the Feedback Weight of a QCN egress queue. Use the **no** form of this command to return to default.

**SYNTAX**

**dce qcn cp feedback-weight** [-]*number*

**no dce qcn cp feedback-weight**

**PARAMETERS**

[-]*number*—Specifies the Feedback Weight. The weight cpW is equal to two to the power of this object. Thus, if this number contains a -1, cpW = 1/2.

Range -8-7

#### DEFAULT CONFIGURATION

The number is 1->cpW=2

#### COMMAND MODE

Global configuration

#### EXAMPLE

```
console(config)# dce qcn cp feedback-weight -7
```

### **dce qcn cp min-sample-base**

Use the **dce qcn cp min-sample-base** global configuration command to configure the minimum number of bytes to enqueue in a QCN egress queue between transmissions of Congestion Notification Messages. Use the **no** form of this command to return to default.

#### SYNTAX

**dce qcn cp min-sample-base** *bytes*

**no dce qcn cp min-sample-base**

#### PARAMETERS

*bytes*—Specifies the minimal sample base in bytes. the value should be a multiple of 16.

Range 10000-4294967280

#### DEFAULT CONFIGURATION

150000

#### COMMAND MODE

Global configuration

#### EXAMPLE

```
console(config)# dce qcn cp min-sample-base 20000
```

### **show dce qcn**

To display the information on the Quantized Congestion Notification (QCN) feature, use the **show dce qcn** command in EXEC mode.

#### SYNTAX

**show dce qcn** [*interface-id*]

**PARAMETERS**

*[interface-id]*—Specifies an interface ID. The interface ID must be an Ethernet port.

**DEFAULT CONFIGURATION**

EXEC

**COMMAND MODE**

Interface configuration (Ethernet)

**USER GUIDELINES**

LLDP should be enabled for rx and tx in order that DCBX would be active.

**EXAMPLE**

```
console# show dce qcn
```

```
QCN is Enabled
CNM priority: 7
```

Priority	QCN Admin	Queue	QCN Oper
0	Disabled	3	Disabled
1	Disabled	1	Disabled
2	Disabled	2	Disabled
3	Disabled	4	Disabled
4	Disabled	5	Disabled
5	Disabled	6	Disabled
6	Disabled	7	Disabled
7	Enabled	8	Enabled

```
Congestion Points
```

```
cpW = 1/128
min-sample-base = 20000
```

```
Set-Point for an egress queues: 1024
```

Interface	CP status
te0/1	Enabled
te0/2	Disabled
te0/3	Disabled
te0/4	Disabled
te0/5	Disabled
.	
.	
.	
te0/47	Disabled
te0/48	Disabled

**dce dcbx enable** To enable the DCB Capability Exchange Protocol (DCBX) on an interface, use the **dce dcbx enable** command in interface configuration mode. To disable DCBX on an interface, use the **no** form of this command.

#### SYNTAX

**dce dcbx enable**  
**no dce dcbx enable**

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT CONFIGURATION

Enabled

#### COMMAND MODE

Interface configuration (Ethernet)

#### USER GUIDELINES

LLDP should be enabled for rx and tx in order that DCBX would be active.

#### EXAMPLE

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# dce dcbx enable
```

**dce dcbx advertise priority-groups** To advertise the DCBX priority-groups TLV on an interface, use the **dce dcbx advertise priority-groups** command in interface configuration mode. To disable the advertisement on the interface, use the **no** form of this command.

#### SYNTAX

**dce dcbx advertise priority-groups**  
**no dce dcbx advertise priority-groups**

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT CONFIGURATION

Enabled

#### COMMAND MODE

Interface configuration (Ethernet)

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# dce dcbx advertise priority-groups
```

**dce dcbx advertise priority-flow-control**

To advertise the DCBX priority-flow-control TLV on an interface, use the **dce dcbx advertise priority-flow-control** command in interface configuration mode. To disable the advertisement on the interface, use the **no** form of this command.

**SYNTAX**

```
dce dcbx advertise priority-flow-control
no dce dcbx advertise priority-flow-control
```

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

Enabled

**COMMAND MODE**

Interface configuration (Ethernet)

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# dce dcbx advertise priority-flow-control
```

**dce dcbx advertise application-protocol**

To advertise the DCBX application and protocol mapping TLV on an interface, use the **dce dcbx advertise application-protocol** command in interface configuration mode. To disable the advertisement on the interface, use the **no** form of this command.

**SYNTAX**

```
dce dcbx advertise application-protocol
no dce dcbx advertise application-protocol
```

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

Enabled

**COMMAND MODE**

Interface configuration (Ethernet)

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# dce dcbx advertise application-protocol
```

**dce application-protocol enable**

Use the **dce application-protocol enable global configuration** to enable application to priority mapping. Use the **no** form of this command to disable the mapping.

**SYNTAX**

**dce application-protocol enable**  
**no dce application-protocol enable**

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

Disabled

**COMMAND MODE**

Interface configuration (Ethernet)

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# dce application-protocol enable
```

**dce application-protocol map**

Use the **dce application-protocol map** global configuration command to map applications to priorities. Use the **no** form of this command to delete mapping.

**SYNTAX**

**dce application-protocol map {*ethtype number* | *port number*} to *priority1* [*priority2 ... priority8*]**  
**no dce application-protocol map {*ethtype number* | *port number*}**

**PARAMETERS**

**ethtype *number***—Ethernet type

**port *number*}**—TCP/UDP Port number

***priority***—802.1Q Priority

Range ***priority*** 0–7

**DEFAULT CONFIGURATION**

No mapping is defined.

**COMMAND MODE**

Global configuration

**EXAMPLE**

```
console(config)# dce application-protocol map port 21 to priority 6
```

**show dce dcbx** To display the DCB Capability Exchange (DCBX) information for specific interface, use the **show dce dcbx** command in privileged EXEC mode.

**SYNTAX**

**show dce dcbx ethernet** *interface-id*

**PARAMETERS**

*interface-id*—Specifies an interface ID. The interface ID must be an Ethernet port.

**COMMAND MODE**

Privileged EXEC

**DEFAULT CONFIGURATION****COMMAND MODE**

Privileged EXEC

**USER GUIDELINES****EXAMPLE**

```
console# show dce dcbx tengigabitethernet 0/1
```

```
DCBX state is enabled.
```

```
DCBX control TLV
```

```
Max version 1
Oper Version 1
```

```
Priorities Groups TLV
```

```
Max Version: 2
Oper Version: 2
```

Field	Local	Remote
Advertisement	Enabled	Disabled
Enable	Enabled	Disabled
Willing	false	false

Error	Yes	No
Num of TCs	7	0

Priority to priority-groups mapping

Priority	Priority Group	
	Local	Remote
0	15	0
1	15	0
2	15	0
3	15	0
4	15	0
5	15	0
6	15	0
7	15	0

Priority-groups BW allocation

Priority Group	BW Allocation	
	Local	Remote
0	12	0
1	12	0
2	12	0
3	12	0
4	13	0
5	13	0
6	13	0
7	13	0

Priority flow control TLV

Max Version: 2  
Oper Version: 2

Field	Local	Remote
Advertisement	Enabled	Disabled
Enable	Enabled	Disabled
Willing	false	false
Error	Yes	No
Num of TCs	8	0

Priority	Flow Control	
	Local	Remote
0	Disabled	Disabled
1	Disabled	Disabled
2	Disabled	Disabled
3	Disabled	Disabled
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Enabled	Disabled

```
Application TLV
```

```
Max Version: 2
Oper Version: 2
```

Field	Local	Remote
Advertisement	Enabled	Disabled
Enable	Enabled	Disabled
Willing	false	false
Error	Yes	No

```
Application to priority mapping
```

Application	Priority	
	Local	Remote
Port 21	6	

```
console#
```

**wrr-queue bandwidth (ETS)** Use the **wrr-queue bandwidth** global configuration command to allocate bandwidth to queues. Use the **no** form of this command to return to default.

#### SYNTAX

```
wrr-queue bandwidth percentage1 [percentage 2 .. percentage8]
```

```
no wrr-queue bandwidth
```

#### PARAMETERS

*percentage 2 .. percentage8*—The BW in percentage allocated to queues. Percentage1 specifies the bandwidth for Queue 1, percentage2 specifies the bandwidth for Queue 2 and so on. The sum should be 100. Unspecified percentage defaults to 0.

Range *percentage 0–100*

#### DEFAULT CONFIGURATION

```
Percentage5 .. percentage8= 13
```

```
Percentage1 .. percentage4= 12
```

#### COMMAND MODE

```
Global configuration
```

**EXAMPLE**

```
console(config)# wrr-queue bandwidth 30 20 10 10 10 10 5 5
```

**show dce ets** To display the information on the Enhanced Transmission Selection (ETS) feature, use the **show dce ets** command in EXEC mode.

**SYNTAX**

**show dce ets**

**PARAMETERS**

This command has no arguments or keywords.

**COMMAND MODE**

Privileged EXEC

**EXAMPLE**

```
console# show dce ets
Priority assignment table

  Priority   Queue
  - - - - -
0           3
1           1
2           2
3           4
4           5
5           6
6           7
7           8

Transmission Selection Algorithm
Queue           Transmission Selection Algorithm
-----
1               SP
2               SP
3               SP
4               SP
5               SP
6               SP
7               SP
8               SP

BW allocation
Queue           Bandwidth
-----
1               30%
2               20%
3               10%
4               10%
5               10%
6               10%
7               5%
8               5%
```

```
console#
```

**dce cut-through enable (global)** Use the **dce cut-through enable** global configuration command to enable cut-through. Use the **no** form of this command to disable cut-through.

#### SYNTAX

**dce cut-through enable**  
**no dce cut-through enable**

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT CONFIGURATION

Disabled

#### COMMAND MODE

Global configuration

#### USER GUIDELINES

The configuration must be applied only after reboot.

#### EXAMPLE

```
console(config)# dce cut-through enable
This setting will take effect only after copying running configuration to
startup configuration and resetting the device
console(config)#
```

**dce cut-through enable (interface)** Use the **dce cut-through enable** interface configuration command to enable cut-through for an interface. Use the **no** form of this command to disable cut-through for the interface.

#### SYNTAX

**dce cut-through enable**  
**no dce cut-through enable**

#### PARAMETERS

This command has no arguments or keywords.

#### DEFAULT CONFIGURATION

Disabled

#### COMMAND MODE

Interface configuration (Ethernet)

**USER GUIDELINES**

The oper state of Cut Through for the interface can be enabled only for 10G ports. Packets are subject to Cut Through if Cut Through is enabled (oper state) for the ingress interface and for the packet's priority (with the **dce cut-through priority enable** global configuration command). For untagged packets, Cut Through should be enabled for untagged packets for the ingress interface (with the **dce cut-through untagged enable** interface configuration command).

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# dce cut-through enable
```

**dce cut-through priority enable**

Use the **dce cut-through priority enable** global configuration command to enable cut-through for a priority. Use the **no** form of this command to disable cut-through for the priority.

**SYNTAX**

**dce cut-through priority *priority* enable**  
**no dce cut-through priority *priority* enable**

**PARAMETERS**

*priority*—802.1Q Priority

Range *priority* 0–7

**DEFAULT CONFIGURATION**

Disabled

**COMMAND MODE**

Global configuration

**EXAMPLE**

```
console(config)# dce cut-through priority 7 enable
```

**dce cut-through untagged enable**

Use the **dce cut-through untagged enable** interface configuration command to enable cut-through for untagged packets for an interface. Use the **no** form of this command to disable cut-through for untagged packets.

**SYNTAX**

**dce cut-through untagged enable**

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT CONFIGURATION**

Disabled

**COMMAND MODE**

Interface configuration (Ethernet)

**EXAMPLE**

```
console(config)# interface tengigabitethernet 0/1
console(config-if)# dce cut-through untagged enable
```

**dce cut-through packet-length**

Use the **dce cut-through packet-length** global configuration command to configure the default packet length that is assigned to a packet in the Cut-Through mode. Use the **no** form of this command to return to default.

**SYNTAX**

**dce cut-through packet-length** *bytes*

**no dce cut-through packet-length**

**PARAMETERS**

*bytes*—Specifies the default packet length in bytes.

*bytes* range 257–16383

**DEFAULT CONFIGURATION**

1522

**COMMAND MODE**

Global configuration

**USER GUIDELINES**

In the current version, the command only affects the buffer allocation mechanism. The buffer management counts the number of buffers for each packet that is allocated per packet in the size configured by this command.

A new value for this parameter is applied only after reboot.

**EXAMPLE**

```
console(config)# dce cut-through packet-length 1024
This setting will take effect only after copying running configuration to
startup configuration and resetting the device
console(config)#
```

**show dce cut-through** To display the information on cut-through, use the **show dce cut-through** command in EXEC mode.

#### SYNTAX

**show dce cut-through** [*interface-id*]

#### PARAMETERS

[*interface-id*]*—*Specifies an interface ID. The interface ID must be an Ethernet port.

#### DEFAULT CONFIGURATION

#### COMMAND MODE

EXEC

#### EXAMPLE

```

console# show dce cut-through

Cut Through is disabled (Would be enabled after reset)

Default packet length: 1522 (Would be 1024 after reboot)

Priority 0: Disabled
Priority 1: Disabled
Priority 2: Disabled
Priority 3: Disabled
Priority 4: Disabled
Priority 5: Disabled
Priority 6: Disabled
Priority 7: Enabled

Interface Admin    Oper    Untagged
-----
te0/1      Disabled Disabled Enabled
te0/2      Disabled Disabled Disabled
te0/3      Disabled Disabled Disabled
te0/4      Disabled Disabled Disabled
.
.
.
te0/47     Disabled Disabled Disabled
te0/48     Disabled Disabled Disabled

```

**dce fip-snooping enable (Global)** To enable FIP snooping for the device, use the **dce fip-snooping enable** command in the Global Configuration mode. To disable FIP snooping for the device, use the no form of this command.

#### SYNTAX

**dce fip-snooping enable**  
**no dce fip-snooping enable**

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT**

Disabled

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

```
console(config)# dce fip-snooping enable
```

**dce fip-snooping enable (Interface)**

To enable FIP snooping for an interface, use the **dce fip-snooping enable** command in interface Configuration mode. To disable FIP snooping for the interface, use the no form of this command.

**SYNTAX**

```
dce fip-snooping enable {enode | fcf | non-fcoe }  
no dce fip-snooping enable
```

**PARAMETERS**

**enode**—Specify that the port is connected to FCoE node.

**fcf**—Specify that the port is connected to Fiber Channel Forwarder and or Enodes.

**non-fcoe**—Specify that the port is not connected to FCoE node of Forwarder.

**DEFAULT**

Disabled

**COMMAND MODE**

Interface configuration mode (Ethernet, Port-channel)

**USER GUIDELINES**

If the administrator knows that a port is connected only to Enodes, then the port type should be enode; Otherwise some of the Enode rules would not be applied.

**Example**

```
console(config-if)# dce fip-snooping enable enode
```

**dce fip-snooping  
fcf-address-filtering  
enable**

To enable filtering of packets based on configured list of MAC addresses of FCFs, use the **dce fip-snooping fcf-address-filtering enable** command in global configuration mode. To disable filtering, use the no form of this command.

**SYNTAX**

**dce fip-snooping fcf-address-filtering enable**  
**no dce fip-snooping fcf-address-filtering enable**

**PARAMETERS**

This command has no arguments or keywords.

**DEFAULT**

Disabled

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

```
console(config)# dce fip-snooping fcf-address-filtering enable
```

**dce fip-snooping  
fcf-address-filtering  
list**

To add a MAC address to the FCF MAC addresses list, use the **dce fip-snooping fcf-address-filtering list** command in global configuration mode. To remove an address, use the no form of this command.

**SYNTAX**

**dce fip-snooping fcf-address-filtering list** *mac-address*  
**no dce fip-snooping fcf-address-filtering list** [*mac-address*]

**PARAMETERS**

**mac-address**—Specify a MAC address to add to the list

**DEFAULT**

The list is empty

**COMMAND MODE**

Global Configuration mode

**EXAMPLE**

```
console(config)# dce fip-snooping fcf-address-filtering list 0010.0D48.37FF
```

**dce fip-snooping tunnel** To add a static tunnel to an interface for FIP snooping, use the **dce fip-snooping tunnel** command in Interface Configuration mode. To remove a tunnel, use the no form of this command.

#### SYNTAX

**dce fip-snooping tunnel** *source-mac-address destination-mac-address*

**no dce fip-snooping tunnel** *source-mac-address destination-mac-address*

#### PARAMETERS

**source-mac-address**—Specify the source MAC address

**destination-mac-address**—Specify the destination MAC address

#### DEFAULT

No tunnels are configured

#### COMMAND MODE

Interface configuration mode (Ethernet, Port-channel)

#### EXAMPLE

```
console(config)# dce fip-snooping tunnel 0010.0D48.37FF 0010.0D48.38FF
```

**clear dce fip-snooping tunnel** To clear dynamic tunnels of FIP snooping, use the **clear dce fip-snooping tunnel** command in Privileged EXEC mode.

#### SYNTAX

**clear dce fip-snooping tunnel** { *interface-id* | \*} { *source-mac-address* | \*} { *destination-mac-address* | \*}

**clear dce fip-snooping tunnel all**

#### PARAMETERS

**interface-id**—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel

**source-mac-address**—Specify the source MAC address

**destination-mac-address**—Specify the destination MAC address

**all**—Clear all tunnels

#### COMMAND MODE

Privileged EXEC mode

**EXAMPLE**

```
console# clear dce fip-snooping tunnel te1 0010.0D48.87FF 0010.0D48.88FF
```

**show dce fip-snooping configuration**

To display the FIP snooping configuration, use the **show dce fip-snooping configuration** command in EXEC mode

**SYNTAX**

**show dce fip-snooping configuration** [*interface-id*]

**PARAMETERS**

**interface-id**—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel

**COMMAND MODE**

EXEC mode

**EXAMPLE**

```
console> show dce fip-snooping configuration
```

```
FIP snooping is enabled
FCF MAC address filtering is enabled
FCF MAC addresses list: 0060.704C.73FF, 0060.708C.73FF
```

Interface	Snooping	Port type
te1	Enabled	FCF
te2	Enabled	Enode
te3	Enabled	Non-FCOE
te4	Disabled	

**show dce fip-snooping tunnels**

To display the FIP snooping tunnels, use the **show dce fip-snooping tunnels** command in EXEC mode.

**SYNTAX**

**show dce fip-snooping tunnels** [**dynamic|static**] [**interface** *interface-id*]

**PARAMETERS**

**dynamic**—Displays only dynamic tunnels

**static**—Displays only static tunnels

**interface-id**—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel

**COMMAND MODE**

EXEC mode

**EXAMPLE**

```
console> show dce fip-snooping tunnels
```

Static tunnels:

Interface	Source Address	Destination Address
te1	0060.704C.1238	0060.704C.73FF

Dynamic tunnels:

Interface	Source Address	Destination Address	S_ID
te1	0060.704C.1238	0060.704C.73FF	0.0.1
te1	0060.704C.1239	0060.704C.73FF	0.0.2

# SECTION IV

## APPENDICES

This section provides additional information and includes these items:

- ◆ ["Troubleshooting" on page 855](#)



---

**PROBLEMS ACCESSING THE MANAGEMENT INTERFACE**
**Table 8: Troubleshooting Chart**

Symptom	Action
Cannot connect using Telnet, web browser, or SNMP software	<ul style="list-style-type: none"> <li>◆ Be sure the switch is powered up.</li> <li>◆ Check network cabling between the management station and the switch.</li> <li>◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled.</li> <li>◆ Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway.</li> <li>◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected.</li> <li>◆ If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag.</li> <li>◆ If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.</li> </ul>
Cannot connect using Secure Shell	<ul style="list-style-type: none"> <li>◆ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.</li> <li>◆ Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station.</li> <li>◆ Be sure you have generated both an RSA and DSA public key on the switch, exported this key to the SSH client, and enabled SSH service.</li> <li>◆ Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password.</li> <li>◆ Be sure you have imported the client's public key to the switch (if public key authentication is used).</li> </ul>
Cannot access the on-board configuration program via a serial port connection	<ul style="list-style-type: none"> <li>◆ Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to 115200 bps.</li> <li>◆ Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.</li> </ul>
Forgot or lost the password	<ul style="list-style-type: none"> <li>◆ Contact your local distributor.</li> </ul>

---

## USING SYSTEM LOGS

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Set up your terminal emulation software so that it can capture all console output to a file. Then enter the "show tech-support" command to record all system settings in this file.
9. Contact your distributor's service engineer, and send a detailed description of the problem, along with the file used to record your system settings.

For example:

```
Console(config)#logging on
Console(config)#logging host 192.168.1.22 severity 7
Console(config)#snmp-server host 192.168.1.23
:
```

# INDEX

## C

console port, required connections 52

## D

default settings, system 50

### DHCP

dynamic configuration 55

## I

### IPv4 address

dynamic configuration 55

setting 54

## L

log-in, web interface 60

## M

main menu, web interface 62

## P

passwords 54

problems, troubleshooting 855

## S

sFlow interface 139

sFlow receiver 138

sFlow statistics 140

## T

troubleshooting 855

## W

### web interface

access requirements 59

configuration buttons 61

home page 60

menu list 62

panel display 61



