SMC Networks

MANAGEMENT GUIDE

SMC8124PL2

TigerSwitch™ 10/100/1000
24-Port Managed Switch with PoE

TigerSwitch 10/100/1000 Management Guide

From SMC's Tiger line of feature-rich workgroup LAN solutions

SMC
Networks
20 Mason
Irvine, CA 92618
Phone: (949) 679-8000

May 2007
Pub. # 149100034100A
E052007-DT-R01

Limited Warranty

Limited Warranty Statement: SMC Networks, Inc. ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC Web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" SMC product. A product is considered to be "Active" while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:
http://www.smc.com/index.cfm?action=customer_service_warranty.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL

NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.

20 Mason

Irvine, CA 92618

Contents

Chapter 1: Introduction 1-1

Key Features 1-1
Description of Software Features 1-2
System Defaults 1-5

Chapter 2: Initial Configuration 2-1

Connecting to the Switch 2-1
Configuration Options 2-1
Required Connections 2-2
Remote Connections 2-3
Basic Configuration 2-3
Console Connection 2-3
Setting Passwords 2-4
Setting an IP Address 2-4
Manual Configuration 2-5
Dynamic Configuration 2-5
Enabling SNMP Management Access 2-6
Community Strings (for SNMP version 1 and 2c clients) 2-7
Trap Receivers 2-7
Configuring Access for SNMP Version 3 Clients 2-8
Saving Configuration Settings 2-8
Managing System Files 2-9

Chapter 3: Configuring the Switch 3-1

Using the Web Interface 3-1
Navigating the Web Browser Interface 3-2
Home Page 3-2
Configuration Options 3-2
Panel Display 3-3
Main Menu 3-3
Basic Configuration 3-10
Displaying System Information 3-10
Displaying Switch Hardware/Software Versions 3-11
Displaying Bridge Extension Capabilities 3-12
Setting the Switch’s IP Address 3-14
Manual Configuration 3-15
Using DHCP/BOOTP 3-16
Enabling Jumbo Frames 3-17

Managing Firmware 3-18
Downloading System Software from a Server 3-18
Saving or Restoring Configuration Settings 3-20
Downloading Configuration Settings from a Server 3-21
Console Port Settings 3-22
Telnet Settings 3-24
Configuring Event Logging 3-26
Displaying Log Messages 3-26
System Log Configuration 3-27
Remote Log Configuration 3-29
Simple Mail Transfer Protocol 3-30
Resetting the System 3-32
Setting the System Clock 3-32
Configuring SNTP 3-32
Setting the Time Zone 3-33
Simple Network Management Protocol 3-34
Enabling the SNMP Agent 3-36
Setting Community Access Strings 3-36
Specifying Trap Managers and Trap Types 3-37
Configuring SNMPv3 Management Access 3-39
Setting the Local Engine ID 3-40
Specifying a Remote Engine ID 3-40
Configuring SNMPv3 Users 3-41
Configuring Remote SNMPv3 Users 3-43
Configuring SNMPv3 Groups 3-45
Setting SNMPv3 Views 3-48
User Authentication 3-50
Configuring User Accounts 3-50
Configuring Local/Remote Logon Authentication 3-51
Configuring HTTPS 3-54
Replacing the Default Secure-site Certificate 3-56
Configuring the Secure Shell 3-56
Configuring the SSH settings 3-58
Generating the Host Key Pair 3-59
Generating the User Public Key Pair 3-61
Configuring Port Security 3-63
Configuring 802.1X Port Authentication 3-64
Displaying 802.1X Global Settings 3-66
Configuring 802.1X Global Settings 3-66
Configuring Port Settings for 802.1X 3-67
Displaying 802.1X Statistics 3-70
Access Control Lists 3-72
Configuring Access Control Lists 3-72
Setting the ACL Name and Type 3-72
Configuring a Standard IP ACL 3-73

Configuring an Extended IP ACL 3-74
Configuring a MAC ACL 3-77
Binding a Port to an Access Control List 3-78
Filtering Management Access 3-79
Port Configuration 3-81
Displaying Connection Status 3-81
Configuring Interface Connections 3-83
Creating Trunk Groups 3-85
Statically Configuring a Trunk 3-86
Enabling LACP on Selected Ports 3-88
Configuring LACP Parameters 3-89
Displaying LACP Port Counters 3-91
Displaying LACP Settings and Status for the Local Side 3-92
Displaying LACP Settings and Status for the Remote Side 3-94
Setting Broadcast Storm Thresholds 3-96
Configuring Port Mirroring 3-97
Configuring Rate Limits 3-98
Rate Limit Configuration 3-98
Showing Port Statistics 3-99
Power over Ethernet Settings 3-104
Switch Power Status 3-105
Setting a Switch Power Budget 3-106
Displaying Port Power Status 3-106
Configuring Port PoE Power 3-107
Address Table Settings 3-108
Setting Static Addresses 3-108
Displaying the Address Table 3-109
Changing the Aging Time 3-110
Spanning Tree Algorithm Configuration 3-111
Displaying Global Settings 3-112
Configuring Global Settings 3-114
Displaying Interface Settings 3-118
Configuring Interface Settings 3-121
VLAN Configuration 3-123
Overview 3-123
Assigning Ports to VLANs 3-123
Forwarding Tagged/Untagged Frames 3-125
Displaying Basic VLAN Information 3-126
Displaying Current VLANs 3-126
Creating VLANs 3-128
Adding Static Members to VLANs (VLAN Index) 3-129
Adding Static Members to VLANs (Port Index) 3-131
Configuring VLAN Behavior for Interfaces 3-132
Configuring Private VLANs 3-133
Displaying Current Private VLANs 3-134

Configuring Private VLANs 3-135
Associating VLANs 3-136
Displaying Private VLAN Interface Information 3-136
Configuring Private VLAN Interfaces 3-137
Configuring Protocol VLANs 3-139
Configuring Protocol VLAN Basic Settings 3-139
Configuring Protocol VLAN System 3-140
LLDP 3-140
Configuring Basic LLDP Time Information 3-140
Configuring LLDP Port and Trunk Information 3-141
Displaying LLDP Local and Remote Device Information 3-143
Class of Service Configuration 3-145
Setting the Default Priority for Interfaces 3-146
Mapping CoS Values to Egress Queues 3-147
Enabling CoS 3-149
Selecting the Queue Mode 3-149
Setting the Service Weight for Traffic Classes 3-150
Mapping Layer 3/4 Priorities to CoS Values 3-151
Selecting IP DSCP Priority 3-151
Mapping DSCP Priority 3-152
Quality of Service 3-153
Configuring Quality of Service Parameters 3-154
Configuring a Class Map 3-154
Creating QoS Policies 3-157
Attaching a Policy Map to Ingress Queues 3-160
Multicast Filtering 3-161
IGMP Protocol 3-161
Layer 2 IGMP (Snooping and Query) 3-162
Configuring IGMP Snooping and Query Parameters 3-162
Displaying Interfaces Attached to a Multicast Router 3-164
Specifying Static Interfaces for a Multicast Router 3-165
Displaying Port Members of Multicast Services 3-166
Assigning Ports to Multicast Services 3-167
Multicast VLAN Registration 3-168
Configuring Global MVR Settings 3-169
Displaying MVR Interface Status 3-170
Displaying Port Members of Multicast Groups 3-171
Configuring MVR Interface Status 3-172
Assigning Static Multicast Groups to Interfaces 3-174
DHCP Snooping 3-175
DHCP Snooping Configuration 3-176
DHCP Snooping VLAN Configuration 3-176
DHCP Snooping Information Option Configuration 3-177
DHCP Snooping Port Configuration 3-178
DHCP Snooping Binding Information 3-179

IP Source Guard 3-180
IP Source Guard Port Configuration 3-180
Static IP Source Guard Binding Configuration 3-181
Dynamic IP Source Guard Binding Information 3-182
Switch Clustering 3-183
Cluster Configuration 3-184
Cluster Member Configuration 3-185
Cluster Member Information 3-185
Cluster Candidate Information 3-186
UPnP 3-187
UPnP Configuration 3-188

Chapter 4: Command Line Interface 4-1

Using the Command Line Interface 4-1
Accessing the CLI 4-1
Console Connection 4-1
Telnet Connection 4-1
Entering Commands 4-3
Keywords and Arguments 4-3
Minimum Abbreviation 4-3
Command Completion 4-3
Getting Help on Commands 4-3
Showing Commands 4-3
Partial Keyword Lookup 4-5
Negating the Effect of Commands 4-5
Using Command History 4-5
Understanding Command Modes 4-5
Exec Commands 4-6
Configuration Commands 4-6
Command Line Processing 4-7
Command Groups 4-8
Line Commands 4-9
line 4-10
login 4-11
password 4-12
timeout login response 4-13
exec-timeout 4-13
password-thresh 4-14
silent-time 4-15
databits 4-15
parity 4-16
speed 4-16
stopbits 4-17
disconnect 4-17

show line 4-18
General Commands 4-19
enable 4-19
disable 4-20
configure 4-20
show history 4-21
reload 4-21
end 4-22
exit 4-22
quit 4-23
System Management Commands 4-23
Device Designation Commands 4-24
prompt 4-24
hostname 4-25
User Access Commands 4-25
username 4-25
enable password 4-26
IP Filter Commands 4-27
management 4-27
show management 4-28
Web Server Commands 4-29
ip http port 4-29
ip http server 4-30
ip http secure-server 4-30
ip http secure-port 4-31
Telnet Server Commands 4-32
ip telnet server 4-32
ip telnet server port 4-32
Secure Shell Commands 4-33
ip ssh server 4-35
ip ssh timeout 4-36
ip ssh authentication-retries 4-37
ip ssh server-key size 4-37
delete public-key 4-38
ip ssh crypto host-key generate 4-38
ip ssh crypto zeroize 4-39
ip ssh save host-key 4-39
show ip ssh 4-40
show ssh 4-40
show public-key 4-41
Event Logging Commands 4-43
logging on 4-43
logging history 4-44
logging host 4-45
logging facility 4-45

logging trap 4-46
clear logging 4-46
show logging 4-47
show log 4-48
SMTP Alert Commands 4-49
logging sendmail host 4-49
logging sendmail level 4-50
logging sendmail source-email 4-51
logging sendmail destination-email 4-51
logging sendmail 4-52
show logging sendmail 4-52
Time Commands 4-53
sntp client 4-53
sntp server 4-54
sntp poll 4-55
show sntp 4-55
clock timezone 4-56
calendar set 4-56
show calendar 4-57
System Status Commands 4-57
show startup-config 4-57
show running-config 4-59
show system 4-60
show users 4-61
show version 4-62
Frame Size Commands 4-63
jumbo frame 4-63
Flash/File Commands 4-64
copy 4-64
delete 4-67
dir 4-67
whichboot 4-68
boot system 4-69
Authentication Commands 4-70
Authentication Sequence 4-70
authentication login 4-70
authentication enable 4-71
RADIUS Client 4-72
radius-server host 4-72
radius-server port 4-73
radius-server key 4-74
radius-server retransmit 4-74
radius-server timeout 4-75
show radius-server 4-75
TACACS+ Client 4-76

tacacs-server host	4-76
tacacs-server port	4-76
tacacs-server key	4-77
show tacacs-server	4-77
Port Security Commands	4-78
port security	4-78
802.1X Port Authentication	4-80
dot1x system-auth-control	4-80
dot1x default	4-81
dot1x max-req	4-81
dot1x port-control	4-81
dot1x operation-mode	4-82
dot1x re-authenticate	4-83
dot1x re-authentication	4-83
dot1x timeout quiet-period	4-83
dot1x timeout re-authperiod	4-84
dot1x timeout tx-period	4-84
show dot1x	4-85
Access Control List Commands	4-88
IP ACLs	4-89
access-list ip	4-89
permit, deny (Standard ACL)	4-90
permit, deny (Extended ACL)	4-91
show ip access-list	4-92
ip access-group	4-92
show ip access-group	4-93
map access-list ip	4-93
show map access-list ip	4-94
ACL Information	4-95
show access-list	4-95
show access-group	4-95
SNMP Commands	4-96
snmp-server	4-96
show snmp	4-97
snmp-server community	4-98
snmp-server contact	4-99
snmp-server location	4-99
snmp-server host	4-100
snmp-server enable traps	4-102
snmp-server engine-id	4-103
show snmp engine-id	4-104
snmp-server view	4-105
show snmp view	4-105
snmp-server group	4-106
show snmp group	4-107

snmp-server user 4-109
show snmp user 4-110
Interface Commands 4-111
interface 4-111
description 4-112
speed-duplex 4-112
negotiation 4-113
capabilities 4-114
flowcontrol 4-115
shutdown 4-116
clear counters 4-116
show interfaces status 4-117
show interfaces counters 4-118
show interfaces switchport 4-119
Broadcast Commands 4-121
broadcast packet-rate 4-121
switchport broadcast 4-121
Mirror Port Commands 4-122
port monitor 4-122
show port monitor 4-123
Rate Limit Commands 4-124
rate-limit 4-124
Link Aggregation Commands 4-125
channel-group 4-126
lacp 4-127
lacp system-priority 4-128
lacp admin-key (Ethernet Interface) 4-129
lacp admin-key (Port Channel) 4-130
lacp port-priority 4-131
show lacp 4-131
Address Table Commands 4-135
mac-address-table static 4-135
clear mac-address-table dynamic 4-136
show mac-address-table 4-137
mac-address-table aging-time 4-138
show mac-address-table aging-time 4-138
Spanning Tree Commands 4-139
spanning-tree 4-139
spanning-tree mode 4-140
spanning-tree forward-time 4-141
spanning-tree hello-time 4-142
spanning-tree max-age 4-142
spanning-tree priority 4-143
spanning-tree pathcost method 4-144
spanning-tree transmission-limit 4-144

spanning-tree spanning-disabled 4-145
spanning-tree cost 4-145
spanning-tree port-priority 4-146
spanning-tree edge-port 4-147
spanning-tree portfast 4-148
spanning-tree link-type 4-148
spanning-tree protocol-migration 4-149
show spanning-tree 4-150
VLAN Commands 4-152
Editing VLAN Groups 4-152
vlan database 4-152
vlan 4-153
Configuring VLAN Interfaces 4-154
interface vlan 4-154
switchport mode 4-155
switchport acceptable-frame-types 4-155
switchport ingress-filtering 4-156
switchport native vlan 4-157
switchport allowed vlan 4-157
switchport forbidden vlan 4-158
Displaying VLAN Information 4-159
show vlan 4-159
Configuring Private VLANs 4-160
private-vlan 4-161
private vlan association 4-162
switchport mode private-vlan 4-162
switchport private-vlan host-association 4-163
switchport private-vlan mapping 4-164
show vlan private-vlan 4-164
GVRP and Bridge Extension Commands 4-165
bridge-ext gvrp 4-165
show bridge-ext 4-166
switchport gvrp 4-166
show gvrp configuration 4-167
garp timer 4-167
show garp timer 4-168
Priority Commands 4-169
Priority Commands (Layer 2) 4-170
queue mode 4-170
switchport priority default 4-171
queue bandwidth 4-172
queue cos-map 4-172
show queue mode 4-173
show queue bandwidth 4-174
show queue cos-map 4-174

Priority Commands (Layer 3 and 4) 4-175
map ip dscp (Global Configuration) 4-175
map ip dscp (Interface Configuration) 4-176
show map ip dscp 4-177
Multicast Filtering Commands 4-178
IGMP Snooping Commands 4-178
ip igmp snooping 4-178
ip igmp snooping vlan static 4-179
ip igmp snooping version 4-179
ip igmp snooping immediate-leave 4-180
show ip igmp snooping 4-180
show mac-address-table multicast 4-181
IGMP Query Commands (Layer 2) 4-182
ip igmp snooping querier 4-182
ip igmp snooping query-count 4-182
ip igmp snooping query-interval 4-183
ip igmp snooping query-max-response-time 4-184
ip igmp snooping router-port-expire-time 4-185
Static Multicast Routing Commands 4-185
ip igmp snooping vlan mrouter 4-185
show ip igmp snooping mrouter 4-186
IGMP Filtering and Throttling Commands 4-187
ip igmp filter (Global Configuration) 4-187
ip igmp profile 4-188
permit, deny 4-189
range 4-189
ip igmp filter (Interface Configuration) 4-190
ip igmp max-groups 4-191
ip igmp max-groups action 4-191
show ip igmp filter 4-192
show ip igmp profile 4-193
show ip igmp throttle interface 4-193
Multicast VLAN Registration Commands 4-194
mvr (Global Configuration) 4-194
mvr (Interface Configuration) 4-195
show mvr 4-197
LLDP 4-199
lldp transmit-interval 4-201
lldp transmit-delay 4-201
lldp transmit-hold 4-202
lldp reinit-delay 4-202
lldp notification-interval 4-203
lldp 4-204
lldp basic-tlv management-address 4-204
lldp basic-tlv description 4-205

lldp basic-tlv system-capabilities 4-206
lldp basic-tlv system-description 4-206
lldp basic-tlv system-name 4-207
lldp notification 4-207
lldp dot1-tlv port-vlan-id 4-208
lldp dot1-tlv port-protocol-vlan-id 4-209
lldp dot1-tlv vlan-name 4-209
lldp dot1-tlv protocol-identity 4-210
lldp dot3-tlv mac-phy 4-210
lldp dot3-tlv link-aggregation 4-211
lldp dot3-tlv power-via-mdi 4-211
lldp dot3-tlv maximum-frame-size 4-212
show lldp config 4-212
show lldp info local-device 4-213
show lldp info remote-device 4-214
show lldp info statistics 4-215
UPnP 4-216
UPnP Configuration 4-216
upnp device 4-217
upnp device ttl 4-217
upnp device advertise duration 4-218
show upnp 4-218
IP Interface Commands 4-219
Basic IP Configuration 4-219
ip address 4-219
ip dhcp restart 4-220
ip default-gateway 4-221
show ip interface 4-222
show ip redirects 4-222
ping 4-222
IP Source Guard Commands 4-223
ip source-guard 4-224
ip source-guard binding 4-225
show ip source-guard 4-227
show ip source-guard binding 4-227
DHCP Snooping Commands 4-227
ip dhcp snooping 4-228
ip dhcp snooping vlan 4-230
ip dhcp snooping trust 4-230
ip dhcp snooping verify mac-address 4-231
ip dhcp snooping information option 4-232
ip dhcp snooping information policy 4-233
ip dhcp snooping database flash 4-233
show ip dhcp snooping 4-234
show ip dhcp snooping binding 4-234

Switch Cluster Commands 4-235
cluster 4-235
cluster commander 4-236
cluster ip-pool 4-236
cluster member 4-237
rcommand 4-238
show cluster 4-238
show cluster members 4-239
show cluster candidates 4-239

Appendix A: Software Specifications **A-1**

Software Features A-1
Management Features A-2
Standards A-2
Management Information Bases A-3

Appendix B: Troubleshooting **B-1**

Problems Accessing the Management Interface B-1
Using System Logs B-2

Glossary

Index

Tables

Table 1-1	Key Features	1-1
Table 1-2	System Defaults	1-5
Table 3-1	Configuration Options	3-2
Table 3-2	Main Menu	3-3
Table 3-3	Logging Levels	3-27
Table 3-4	SNMPv3 Security Models and Levels	3-35
Table 3-5	Supported Notification Messages	3-45
Table 3-6	HTTPS Support	3-55
Table 3-7	802.1X Statistics	3-70
Table 3-8	LACP Port Counter Information	3-91
Table 3-9	LACP Settings	3-92
Table 3-10	LACP Remote Side Settings	3-94
Table 3-11	Port Statistics	3-100
Table 3-12	Egress Queue Priority Mapping	3-147
Table 3-13	CoS Priority Levels	3-147
Table 3-14	Mapping DSCP Priority	3-152
Table 4-1.	Command Modes	4-5
Table 4-2.	Configuration Commands	4-7
Table 4-3.	Keystroke Commands	4-7
Table 4-4.	Command Group Index	4-8
Table 4-5.	Line Command Syntax	4-9
Table 4-6.	General Commands	4-19
Table 4-7.	System Management Commands	4-23
Table 4-8.	Device Designation Commands	4-24
Table 4-9.	User Access Commands	4-25
Table 4-10.	Default Login Settings	4-26
Table 4-11.	IP Filter Commands	4-27
Table 4-12.	Web Server Command	4-29
Table 4-13.	HTTPS System Support	4-31
Table 4-14.	Telnet Server Commands	4-32
Table 4-15.	Secure Shell Commands	4-33
Table 4-16.	show ssh - display description	4-41
Table 4-17.	Event Logging Commands	4-43
Table 4-18.	Logging Levels	4-44
Table 4-19.	show logging flash/ram - display description	4-48
Table 4-20.	show logging trap - display description	4-48
Table 4-21.	SMTP Alert Commands	4-49
Table 4-22.	Time Commands	4-53
Table 4-23.	System Status Commands	4-57
Table 4-24.	Frame Size Commands	4-63
Table 4-25.	Flash/File Commands	4-64
Table 4-26.	File Directory Information	4-68

Table 4-27.	Authentication Commands	4-70
Table 4-28.	Authentication Sequence	4-70
Table 4-29.	RADIUS Client Commands	4-72
Table 4-30.	TACACS+ Client Commands	4-76
Table 4-31.	Port Security Commands	4-78
Table 4-32.	802.1X Port Authentication Commands	4-80
Table 4-33.	Access Control List Commands	4-88
Table 4-34.	IP ACL Commands	4-89
Table 4-35.	Egress Queue Priority Mapping	4-94
Table 4-36.	ACL Information	4-95
Table 4-37.	SNMP Commands	4-96
Table 4-38.	show snmp engine-id - display description	4-104
Table 4-39.	show snmp view - display description	4-106
Table 4-40.	show snmp group - display description	4-108
Table 4-41.	show snmp user - display description	4-110
Table 4-42.	Interface Commands	4-111
Table 4-43.	show interfaces switchport - display description	4-120
Table 4-44.	Broadcast Commands	4-121
Table 4-45.	Mirror Port Commands	4-122
Table 4-46.	Rate Limit Commands	4-124
Table 4-47.	Link Aggregation Commands	4-125
Table 4-48.	show lacp counters - display description	4-132
Table 4-49.	show lacp internal - display description	4-133
Table 4-50.	show lacp neighbors - display description	4-134
Table 4-52.	Address Table Commands	4-135
Table 4-51.	show lacp sysid - display description	4-135
Table 4-53.	Spanning Tree Commands	4-139
Table 4-54.	VLAN Commands	4-152
Table 4-55.	Editing VLAN Groups	4-152
Table 4-56.	Configuring VLAN Interfaces	4-154
Table 4-57.	Displaying VLAN Information	4-159
Table 4-58.	Private VLAN Commands	4-160
Table 4-59.	GVRP and Bridge Extension Commands	4-165
Table 4-60.	Priority Commands	4-169
Table 4-61.	Priority Commands (Layer 2)	4-170
Table 4-62.	Default CoS Priority Levels	4-173
Table 4-63.	Priority Commands (Layer 3 and 4)	4-175
Table 4-64.	Mapping IP DSCP to CoS Values	4-176
Table 4-65.	Multicast Filtering Commands	4-178
Table 4-66.	IGMP Snooping Commands	4-178
Table 4-67.	IGMP Query Commands (Layer 2)	4-182
Table 4-68.	Static Multicast Routing Commands	4-185
Table 4-69.	IGMP Filtering and Throttling Commands	4-187
Table 4-70.	Multicast VLAN Registration Commands	4-194
Table 4-71.	show mvr - display description	4-198

Table 4-72.	show mvr interface - display description	4-198
Table 4-73.	show mvr members - display description	4-199
Table 4-74.	LLDP Commands	4-199
Table 4-75.	UPnP Commands	4-216
Table 4-76.	IP Interface Commands	4-219
Table 4-77.	IP Source Guard Commands	4-224
Table 4-78.	DHCP Snooping Commands	4-227
Table 4-79.	Switch Cluster Commands	4-235
Table 2-1.	Troubleshooting Chart	B-1

Figures

Figure 3-1.	Homepage	3-2
Figure 3-2.	Panel Display	3-3
Figure 3-3.	System Information	3-10
Figure 3-4.	Switch Information	3-12
Figure 3-5.	Bridge Extension Configuration	3-13
Figure 3-6.	Manual IP Configuration	3-15
Figure 3-7.	DHCP IP Configuration	3-16
Figure 3-8.	Enabling Jumbo Frames	3-17
Figure 3-9.	Copy Firmware	3-19
Figure 3-10.	Setting the Startup Code	3-19
Figure 3-11.	Deleting Files	3-19
Figure 3-12.	Downloading Configuration Settings for Startup	3-21
Figure 3-13.	Setting the Startup Configuration Settings	3-21
Figure 3-14.	Console Port Setting	3-23
Figure 3-15.	Enabling Telnet	3-25
Figure 3-16.	Displaying Logs	3-27
Figure 3-17.	System Logs	3-28
Figure 3-18.	Remote Logs	3-29
Figure 3-19.	Enabling and Configuring SMTP	3-31
Figure 3-20.	Resetting the System	3-32
Figure 3-21.	SNTP Configuration	3-33
Figure 3-22.	Setting the Time Zone	3-34
Figure 3-23.	Enabling the SNMP Agent	3-36
Figure 3-24.	Configuring SNMP Community Strings	3-37
Figure 3-25.	Configuring SNMP Trap Managers	3-39
Figure 3-26.	Setting an Engine ID	3-40
Figure 3-27.	Setting an Engine ID	3-41
Figure 3-28.	Configuring SNMPv3 Users	3-42
Figure 3-29.	Configuring Remote SNMPv3 Users	3-44
Figure 3-30.	Configuring SNMPv3 Groups	3-47
Figure 3-31.	Configuring SNMPv3 Views	3-49
Figure 3-32.	Access Levels	3-51
Figure 3-33.	Authentication Settings	3-53
Figure 3-34.	HTTPS Settings	3-55
Figure 3-35.	SSH Server Settings	3-59
Figure 3-36.	SSH Host-Key Settings	3-60
Figure 3-37.	SSH User Public-Key Settings	3-62
Figure 3-38.	Configuring Port Security	3-64
Figure 3-39.	802.1X Global Information	3-66
Figure 3-40.	802.1X Global Configuration	3-67
Figure 3-41.	802.1X Port Configuration	3-68
Figure 3-42.	Displaying 802.1X Port Statistics	3-71

Figure 3-43. Naming and Choosing ACLs 3-73
Figure 3-44. Configuring Standard IP ACLs 3-74
Figure 3-45. Configuring Extended IP ACLs 3-76
Figure 3-46. Configuring MAC ACLs 3-78
Figure 3-47. Mapping ACLs to Port Ingress Queues 3-79
Figure 3-48. Filtering Management Access 3-80
Figure 3-49. Port Status Information 3-81
Figure 3-50. Configuring Port Attributes 3-84
Figure 3-51. Static Trunk Configuration 3-87
Figure 3-52. LACP Port Configuration 3-88
Figure 3-53. LACP Aggregation Port Configuration 3-90
Figure 3-54. Displaying LACP Port Counters Information 3-92
Figure 3-55. Displaying LACP Port Information 3-93
Figure 3-56. Displaying Remote LACP Port Information 3-95
Figure 3-57. Enabling Port Broadcast Control 3-96
Figure 3-58. Configuring a Mirror Port 3-98
Figure 3-59. Configuring Input Port Rate Limiting 3-99
Figure 3-60. Displaying Port Statistics 3-102
Figure 3-61. Displaying Etherlike and RMON Statistics 3-103
Figure 3-62 Displaying the Global PoE Status 3-105
Figure 3-63 Setting the Switch Power Budget 3-106
Figure 3-64 Displaying Port PoE Status 3-107
Figure 3-65 Configuring Port PoE Power 3-108
Figure 3-66. Mapping Ports to Static Addresses 3-109
Figure 3-67. Displaying the MAC Dynamic Address Table 3-110
Figure 3-68. Setting the Aging Time 3-111
Figure 3-69. Displaying the Spanning Tree Algorithm 3-114
Figure 3-70. Configuring the Spanning Tree Algorithm 3-117
Figure 3-71. Displaying STA - Port Status Information 3-120
Figure 3-72. Configuring Spanning Tree Algorithm per Port 3-122
Figure 3-73. Displaying Basic VLAN Information 3-126
Figure 3-74. Displaying VLAN Information by Port Membership 3-127
Figure 3-75. Creating Virtual LANs 3-129
Figure 3-76. Configuring VLAN Port Attributes 3-130
Figure 3-77. Assigning VLAN Port and Trunk Groups 3-131
Figure 3-78. Configuring VLAN Ports 3-133
Figure 3-79. Private VLAN Information 3-134
Figure 3-80. Private VLAN Configuration 3-135
Figure 3-81. Private VLAN Association 3-136
Figure 3-82. Private VLAN Port Information 3-137
Figure 3-83. Private VLAN Port Configuration 3-138
Figure 3-84. Protocol VLAN Configuration 3-139
Figure 3-85. Protocol VLAN Port Configuration 3-140
Figure 3-86. LLDP Configuration 3-141
Figure 3-87. LLDP Port Configuration 3-142

Figure 3-88. LLDP Local Device Information 3-143
Figure 3-89. LLDP Remote Device Information 3-143
Figure 3-90. Port Priority Configuration 3-146
Figure 3-91. Configuring Class of Service 3-148
Figure 3-92. Enable Traffic Classes 3-149
Figure 3-93. Setting the Queue Mode 3-149
Figure 3-94. Configuring Queue Scheduling 3-150
Figure 3-95. IP DSCP Priority Status 3-151
Figure 3-96. Mapping IP DSCP Priority to Class of Service Values 3-152
Figure 3-97. Configuring Class Maps 3-156
Figure 3-98. Configuring Policy Maps 3-159
Figure 3-99. Service Policy Settings 3-160
Figure 3-100. Configuring Internet Group Management Protocol 3-164
Figure 3-101. Mapping Multicast Switch Ports to VLANs 3-165
Figure 3-102. Static Multicast Router Port Configuration 3-166
Figure 3-103. Displaying Port Members of Multicast Services 3-167
Figure 3-104. Specifying Multicast Port Membership 3-168
Figure 3-105. MVR Global Configuration 3-170
Figure 3-106. MVR Port Information 3-171
Figure 3-107. MVR Group IP Information 3-172
Figure 3-108. MVR Port Configuration 3-173
Figure 3-109. MVR Group Member Configuration 3-174
Figure 3-110. DHCP Snooping Configuration 3-176
Figure 3-111. DHCP Snooping VLAN Configuration 3-177
Figure 3-112. DHCP Snooping Information Option Configuration 3-178
Figure 3-113. DHCP Snooping Port Configuration 3-178
Figure 3-114. DHCP Snooping Binding Information 3-179
Figure 3-115. IP Source Guard Port Configuration 3-180
Figure 3-116. Static IP Source Guard Binding Configuration 3-182
Figure 3-117. Dynamic IP Source Guard Binding Information 3-183
Figure 3-118. Cluster Configuration 3-184
Figure 3-119. Cluster Member Configuration 3-185
Figure 3-120. Cluster Member Information 3-186
Figure 3-121. Cluster Candidate Information 3-186
Figure 3-122. UPnP Configuration 3-188

Chapter 1: Introduction

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 1-1 Key Features

Feature	Description
Configuration Backup and Restore	Backup to TFTP server
Authentication	Console, Telnet, web – User name / password, RADIUS, TACACS+ Web – HTTPS; Telnet – SSH SNMP v1/v2c/v3– Community strings Port – IEEE 802.1X, MAC address filtering
Access Control Lists	Supports up to 32 IP
DHCP Client	Supported
Port Configuration	Speed, duplex mode and flow control
Rate Limiting	Input rate limiting per port
Port Mirroring	One port mirrored to single analysis port
Port Trunking	Supports up to 8 trunks using either static or dynamic trunking (LACP)
Broadcast Storm Control	Supported
Static Address	Up to 8K MAC addresses in the forwarding table
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 Protocol	Supports standard STP and Rapid Spanning Tree Protocol (RSTP)
Virtual LANs	Up to 255 using IEEE 802.1Q, port-based, protocol-based, or private VLANs
LLDP	Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain.
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, Differentiated Services Code Point (DSCP), and TCP/UDP Port

Table 1-1 Key Features (Continued)

Feature	Description
Multicast Filtering	Supports IGMP snooping and query

Description of Software Features

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

Configuration Backup and Restore – You can save the current configuration settings to a file on a TFTP server, and later download this file to restore the switch configuration settings.

Authentication – This switch authenticates management access via the console port, Telnet or 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 the Extensible Authentication Protocol over LANs (EAPOL) to request a user name and password 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/web/Telnet management access, and MAC address filtering for port access.

Access Control Lists – ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can by 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 the 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.

Rate Limiting – This feature controls the maximum rate for traffic received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into the network. Packets that exceed the acceptable amount of traffic are dropped.

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

Port Trunking – Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using IEEE 802.3ad Link Aggregation Control Protocol (LACP). 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.

Broadcast Storm Control – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast 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.

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 1.5 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

Spanning Tree Protocol – The switch supports these spanning tree protocols:

Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol adds a level of fault tolerance by allowing two or more redundant connections to be created between a pair of LAN segments. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 10% of that required by 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.

Virtual LANs – The switch supports up to 255 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 private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.

Traffic Prioritization – This switch prioritizes each packet based on the required level of service, using eight 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.

Multicast Filtering – Multicast filtering is a system where network devices forward multicast traffic only to the ports that are registered with the multicast group. Without mulicast filtering the data packet will be broadcast to all endstations within a LAN or VLAN. The purpose is to keep the non-multicast group members from receiving unsolicited packets and to prevent a possible reduction in network performance. The switch uses IGMP Snooping and Query at Layer 2 and IGMP at Layer 3 to manage multicast group registration.

System Defaults

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file (page 3-20).

The following table lists some of the basic system defaults.

Table 1-2 System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443
SNMP	Community Strings	"public" (read only) "private" (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read only); private (read/write)

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input limits	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	500 packets per second
Spanning Tree Protocol	Status	Enabled, RSTP (Defaults: All values based on IEEE 802.1w)
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Enabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Weighted Round Robin	Queue: 0 1 2 3 4 5 6 7 Weight: 1 2 4 6 8 10 12 14
	IP DSCP Priority	Disabled
IP Settings	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Enabled
	BOOTP	Disabled
Multicast Filtering	IGMP Snooping	Snooping: Enabled Querier: Enabled

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
System Log	Status	Enabled
	Messages Logged	Levels 0-6 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled (but no server defined)
SNTP	Clock Synchronization	Disabled

Chapter 2: Initial Configuration

Connecting to the Switch

Configuration Options

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

Note: The IP address for this switch is unassigned by default. To change this address, see “Setting an IP Address” on page 22-4.

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 Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The switch’s Web management interface can be accessed from any computer attached to the network.

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

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

The switch’s Web interface, CLI configuration program, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by limiting input rates
- Control port access through IEEE 802.1X security or static address filtering
- Filter packets using Access Control Lists (ACLs)
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IGMP multicast filtering
- Upload and download system firmware via TFTP
- Upload and download switch configuration files via TFTP

- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to 8 static or LACP trunks
- Enable port mirroring
- Set broadcast storm control on any port
- 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 to any of these baud rates: 9600, 19200, 38400, 57600, 115200 (Note: Set to 9600 baud to view all system initialization messages.)
   - 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.
   - With HyperTerminal, select Terminal keys, not Windows keys.

Notes: **1.** When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

2. Refer to "Line Commands" on page 44-9 for a complete description of console configuration options.

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

For a description of how to use the CLI, see “Using the Command Line Interface” on page 44-1. For a list of all the CLI commands and detailed information on using the CLI, refer to “Command Groups” on page 44-8.

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, DHCP or BOOTP 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 or BOOTP, see “Setting an IP Address” on page 22-4.

Note: This switch supports four concurrent Telnet/SSH sessions.

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

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

Basic Configuration

Console Connection

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

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

1. To initiate your console connection, press <Enter>. The “User Access Verification” procedure starts.
2. At the Username prompt, enter “admin.”
3. The Password is blank.

4. The session is opened and the CLI displays the “Console#” prompt indicating you have access at the Privileged Exec level.

Setting Passwords

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

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

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

Note: ‘0’ specifies the password in plain text, ‘7’ specifies the password in encrypted form.

```
Username: admin
Password:

      CLI session with the SMC8124PL2 is opened.
      To end the CLI session, enter [Exit].

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

Setting an IP Address

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

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

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers 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 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.

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

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

To assign an IP address to the switch, complete the following steps:

1. From the Privileged Exec level 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
Console(config)#
```

Dynamic Configuration

If you select the “bootp” or “dhcp” option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to use the “ip dhcp restart client” command to start broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

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

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

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. At the interface-configuration mode prompt, use one of the following commands:
   - To obtain IP settings via DHCP, type “ip address dhcp” and press <Enter>.
   - To obtain IP settings via BOOTP, type “ip address bootp” and press <Enter>.
3. Type “end” to return to the Privileged Exec mode. Press <Enter>.
4. Type “ip dhcp restart client” to begin broadcasting service requests. Press <Enter>.
5. Wait a few minutes, and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.
6. 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#ip dhcp restart client
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as SMC EliteView. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

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

The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e., an SNMPv3 construct) for the default “public” community string that provides read access to the entire MIB tree, and a default view for the “private” community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see page 3-48).

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

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

The default strings are:

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

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

To configure a community string, complete the following steps:

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

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

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

Trap Receivers

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

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

where “host-address” is the IP address for the trap receiver, “community-string” specifies access rights for a version 1/2c host, or is the user name of a version 3 host, “version” indicates the SNMP client version, and “auth | noauth | priv” means that authentication, no authentication, or authentication and privacy is used for v3 clients. Then press <Enter>. For a more detailed description of these parameters, see “snmp-server host” on page 44-100. The following example creates a trap host for each type of SNMP client.

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

Configuring Access for SNMP Version 3 Clients

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

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

For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to “Simple Network Management Protocol” on page 33-34, or refer to the specific CLI commands for SNMP starting on page 4-96.

Saving Configuration Settings

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

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

1. From the Privileged Exec mode prompt, type “copy running-config startup-config” and press <Enter>.

2. Enter the name of the start-up file. Press <Enter>.

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

Managing System Files

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

The three types of files are:

- **Configuration** — This file stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. A file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. See "Saving or Restoring Configuration Settings" on page 33-20 for more information.
- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and Web management interfaces. See "Managing Firmware" on page 33-18 for more information.
- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows.

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

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

Chapter 3: Configuring the Switch

Using the Web Interface

This switch provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 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 Chapter 4: “Command Line Interface.”

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

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See “Setting an IP Address” on page 2-4.)
2. Set user names and passwords using an out-of-band serial connection. Access to the Web agent is controlled by the same user names and passwords as the onboard configuration program. (See “Setting Passwords” on page 2-4.)
3. After you enter a user name and password, you will have access to the system configuration program.

Notes:

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

2. 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.

3. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch’s response time to management commands issued through the web interface. See “Configuring Interface Settings” on page 3-121.

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.

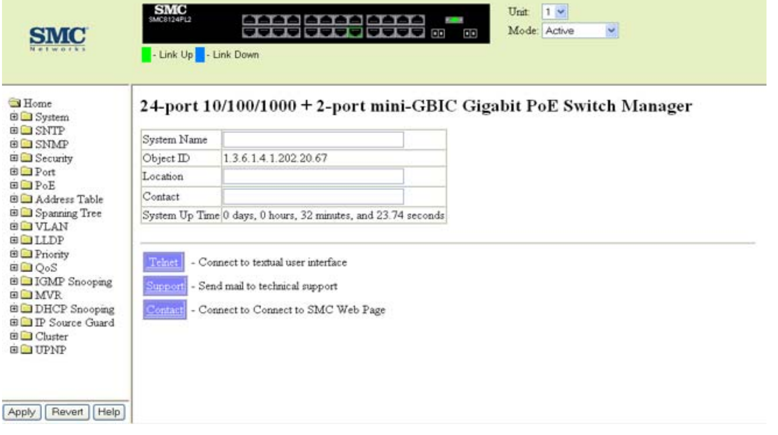


Figure 3-1. Homepage

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 3-1 Configuration Options

Button	Action
Revert	Cancels specified values and restores current values prior to pressing “Apply.”
Apply	Sets specified values to the system.
Help	Links directly to webhelp.

Notes: 1. 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.”

2. 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). Clicking on the image of a port opens the Port Configuration page as described on page 3-83.

Figure 3-2. Panel Display

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 3-2 Main Menu

Menu	Description	Page
System		3-10
System Information	Provides basic system description, including contact information	3-10
Switch Information	Shows the number of ports, hardware/firmware version numbers, and power status	3-11
Bridge Extension Configuration	Shows the bridge extension parameters	3-12
IP Configuration	Sets the IP address for management access	3-14
Jumbo Frames	Enables or disables jumbo frames	3-17
File Management		3-18
Copy Operation	Allows the transfer and copying files	3-18
Delete	Allows deletion of files from the flash memory	3-20
Set Start-Up	Sets the start-up file	3-18

Table 3-2 Main Menu (Continued)

Menu	Description	Page
Line		3-22
Console	Sets console port connection parameters	3-22
Telnet	Sets Telnet connection parameters	3-24
Log		3-26
Logs	Stores and displays error messages	3-26
System Logs	Sends error messages to a logging process	3-27
Remote Logs	Configures the logging of messages to a remote logging process	3-29
SMTP	Sends an SMTP client message to a participating server.	3-30
Reset	Restarts the switch	3-32
SNTP		3-32
Configuration	Configures SNTP client settings, including broadcast mode or a specified list of servers	3-32
Clock Time Zone	Sets the local time zone for the system clock	3-33
SNMP		3-34
Configuration	Configures community strings and related trap functions	3-36
Agent Status	Enables or disables SNMP Agent Status	3-36
SNMPv3		3-39
Engine ID	Sets SNMPv3 Engine ID	3-40
Remote Engine ID	Adds a Remote Engine ID and IP Host	3-40
Users	Creates or deletes user accounts	3-41
Remote Users	Creates or deletes remote user accounts	3-43
Groups	Creates or deletes SNMPv3 Groups	3-45
Views	Creates or deletes SNMPv3 Views	3-48
Security		3-50
User Accounts	Assigns a new password for the current user	3-50
Authentication Settings	Configures authentication sequence, RADIUS and TACACS	3-51
HTTPS Settings	Configures secure HTTP settings	3-54
SSH		3-56
Settings	Configures Secure Shell server settings	3-63
Host-Key Settings	Generates the host key pair (public and private)	3-59
SSH User Public-Key Settings	Copies the user key pair (public and private)	3-61

Table 3-2 Main Menu (Continued)

Menu	Description	Page
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	3-63
802.1X		3-64
Information	Displays global configuration settings	3-66
Configuration	Configures protocol parameters	3-66
Port Configuration	Sets the authentication mode for individual ports	3-67
Statistics	Displays protocol statistics for the selected port	3-70
ACL		3-72
Configuration	Configures packet filtering based on IP or MAC addresses	3-72
Port Binding	Binds a port to the specified ACL	3-78
IP Filter	Sets IP addresses of clients allowed management access	3-79
Port		3-79
Port Information	Displays port connection status	3-81
Trunk Information	Displays trunk connection status	3-81
Port Configuration	Configures port connection settings	3-83
Trunk Configuration	Configures trunk connection settings	3-83
Trunk Membership	Specifies ports to group into static trunks	3-86
LACP		3-88
Configuration	Allows ports to dynamically join trunks	3-88
Aggregation Port	Configures system priority, admin key, and port priority	3-89
Port Counters Information	Displays statistics for LACP protocol messages	3-91
Port Internal Information	Displays settings and operational state for local side	3-92
Port Neighbors Information	Displays settings and operational state for remote side	3-94
Port Broadcast Control	Sets the broadcast storm threshold for each port	3-96
Trunk Broadcast Control	Sets the broadcast storm threshold for each trunk	3-96
Mirror Port Configuration	Sets the source and target ports for mirroring	3-97
Rate Limit		3-98
Input Port Configuration	Sets the input rate limit for each ports	3-98
Input Trunk Configuration	Sets the input rate limit for each trunks	3-98
Output Port Configuration	Sets the output rate limit for each ports	3-98
Output Trunk Configuration	Sets the output rate limit for each trunks	3-98
Port Statistics	Lists Ethernet and RMON port statistics	3-99

Table 3-2 Main Menu (Continued)

Menu	Description	Page
PoE		
Power Status	Displays the status of global power parameters	3-105
Power Config	Configures the power budget for the switch	3-106
Power Port Status	Displays the status of port power parameters	3-106
Power Port Config	Configures port power parameters	3-107
Address Table		3-108
Static Addresses	Displays entries for interface, address or VLAN	3-108
Dynamic Addresses	Displays or edits static entries in the Address Table	3-109
Address Aging	Sets timeout for dynamically learned entries	3-110
Spanning Tree		3-111
STA		3-112
Information	Displays STA values used for the bridge	3-112
Configuration	Configures global bridge settings for STA, and RSTP	3-114
Port Information	Displays individual port settings for STA	3-118
Trunk Information	Displays individual trunk settings for STA	3-118
Port Configuration	Configures individual port settings for STA	3-121
Trunk Configuration	Configures individual trunk settings for STA	3-121
VLAN		3-123
802.1Q VLAN		3-123
Basic Information	Displays information on the VLAN type supported by this switch	3-126
Current Table	Shows the current port members of each VLAN and whether or not the port is tagged or untagged	3-126
Static List	Used to create or remove VLAN groups	3-128
Static Table	Modifies the settings for an existing VLAN	3-129
Static Membership by Port	Configures membership type for interfaces, including tagged, untagged or forbidden	3-131
Port Configuration	Specifies default PVID and VLAN attributes	3-132
Trunk Configuration	Specifies default trunk VID and VLAN attributes	3-132
Private VLAN		3-133
Information	Displays Private VLAN feature information	3-134
Configuration	This page is used to create/remove primary or community VLANs	3-135

Table 3-2 Main Menu (Continued)

Menu	Description	Page
Association	Each community VLAN must be associated with a primary VLAN	3-136
Port Information	Shows VLAN port type, and associated primary or secondary VLANs	3-136
Port Configuration	Sets the private VLAN interface type, and associates the interfaces with a private VLAN	3-137
Trunk Information	Shows VLAN trunk type, and associated primary or secondary VLANs	3-136
Trunk Configuration	Sets the private VLAN interface type, and associates the interfaces with a private VLAN	3-137
Protocol VLAN		3-139
Configuration	Configures protocol VLANs.	3-139
Port Configuration	Configures protocol VLAN port type, and associated protocol VLANs.	3-140
LLDP		3-140
Configuration	Configures basic LLDP time parameters	3-140
Port Configuration	Configures a port for receive and, or transmit status, allows sending of SNMP notication messages, and configures TLV information.	3-141
Trunk configuration	Configures a trunkt for receive and, or transmit status, allows sending of SNMP notication messages, and configures TLV information.	3-141
Local Information	Displays information about the local device.	3-143
Remote Port Information	Displays information about ports on a remote device	3-143
Remote Trunk Information	Displays information about trunks ona remote device	3-143
Remote Information Details	Sets the port and, or trunk to display information about	3-143
Device Statistics	Displays device statistics	3-143
Device Statistics Details	Allows the user to select the port or trunk on which to display statistical information	3-143
Priority		3-145
Default Port Priority	Sets the default priority for each port	3-146
Default Trunk Priority	Sets the default priority for each trunk	3-146
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	3-147
Traffic Classes Status	Enables/disables traffic class priorities.	3-149
Queue Mode	Sets queue mode to strict priority or Weighted Round-Robin	3-149
Queue Scheduling	Configures Weighted Round Robin queueing	3-150
IP DSCP Priority Status	Globally selects IP DSCP Priority, or disables it.	3-151

Table 3-2 Main Menu (Continued)

Menu	Description	Page
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	3-152
QoS		3-153
DiffServ		3-153
Class Map	Sets Class Maps	3-154
Policy Map	Sets Policy Maps	3-157
Service Policy	Defines service policy settings for ports	3-160
IGMP Snooping		3-161
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	3-162
IGMP Filter Configuration	Enables multicast filtering; sets IGMP profiles	3-167
IGMP Immediate Leave	Enables the immediate leave function	3-168
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router for each VLAN ID	3-164
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router	3-165
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	3-166
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	3-167
MVR		3-168
Configuration	Globally enables MVR, sets the MVR VLAN, adds multicast stream addresses	3-169
Port Information	Displays MVR interface type, MVR operational and activity status, and immediate leave status	3-170
Trunk Information	Displays MVR interface type, MVR operational and activity status, and immediate leave status	3-170
Group IP Information	Displays the ports attached to an MVR multicast stream	3-171
Port Configuration	Configures MVR interface type and immediate leave status	3-172
Trunk Configuration	Configures MVR interface type and immediate leave status	3-172
Group Member Configuration	Statically assigns MVR multicast streams to an interface	3-174
DHCP Snooping		3-175
Configuration	Enables DHCP Snooping and DHCP Snooping MAC-Address Verification	3-176
VLAN Configuration	Enables DHCP Snooping for a VLAN	3-176
Information Option Configuration	Enables DHCP Snooping Information Option	3-177

Table 3-2 Main Menu (Continued)

Menu	Description	Page
Port Configuration	Selects the DHCP Snooping Information Option policy	3-178
Binding Information	Displays the DHCP Snooping binding information	3-179
IP Source Guard		3-180
Port Configuration	Enables IP source guard and selects filter type per port	3-180
Static Configuration	Adds a static addresses to the source-guard binding table	3-181
Dynamic Information	Displays the source-guard binding table for a selected interface	3-182
Cluster		3-183
Configuration	Globally enables clustering for the switch	3-184
Member Configuration	Adds switch Members to the cluster	3-185
Member Information	Displays cluster Member switch information	3-185
Candidate Information	Displays network Candidate switch information	3-186
UPNP		3-187
Configuration	Configues basic UPnP parameters	3-188

Basic Configuration

Displaying System Information

You can easily identify the system by displaying the device name, location and contact information.

Field Attributes

- **System Name** – Name assigned to the switch system.
- **Object ID** – MIB II object ID for switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.

These additional parameters are displayed for the CLI.

- **MAC Address** – The physical layer address for this switch.
- **Web server** – Shows if management access via HTTP is enabled.
- **Web server port** – Shows the TCP port number used by the web interface.
- **Web secure server** – Shows if management access via HTTPS is enabled.
- **Web secure server port** – Shows the TCP port used by the HTTPS interface.
- **Telnet server** – Shows if management access via Telnet is enabled.
- **Telnet port** – Shows the TCP port used by the Telnet interface.
- **Jumbo Frame** – Shows if jumbo frames are enabled.
- **POST result** – Shows results of the power-on self-test

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows access to the Command Line Interface via Telnet.)

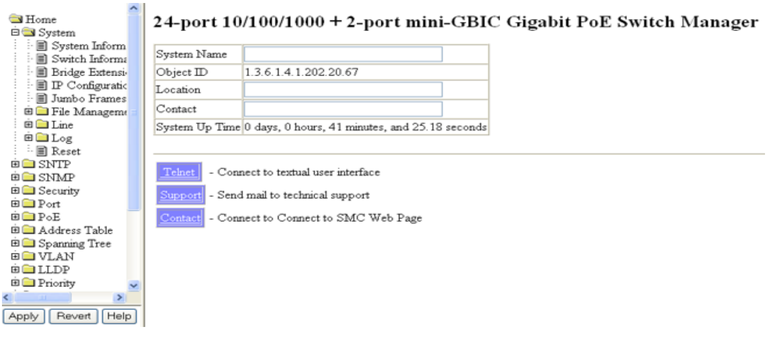


Figure 3-3. System Information

CLI – Specify the hostname, location and contact information.

```
Console(config)#hostname R&D 5                                      4-25
Console(config)#snmp-server location WC 9                           4-99
Console(config)#snmp-server contact Geoff                           4-99
Console(config)#exit
Console#show system                                                 4-60
System Description: SMC Networks SMC8124PL2
System OID String: 1.3.6.1.4.1.259.6.10.94
System Information
 System Up Time:          0 days, 0 hours, 7 minutes, and 22.65 seconds
 System Name:             R&D 5
 System Location:         WC 9
 System Contact:          Geoff
 MAC Address (Unit1):     00-00-35-28-00-03
 Web Server:              Enabled
 Web Server Port:         80
 Web Secure Server:       Enabled
 Web Secure Server Port:  443
 Telnet Server:           Enable
 Telnet Server Port:      23
 Jumbo Frame:             Disabled

 POST Result:
DUMMY Test 1 ................. PASS
UART Loopback Test ........... PASS
DRAM Test .................... PASS
Timer Test ................... PASS

Done All Pass.
Console#
```

Displaying Switch Hardware/Software Versions

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

Field Attributes

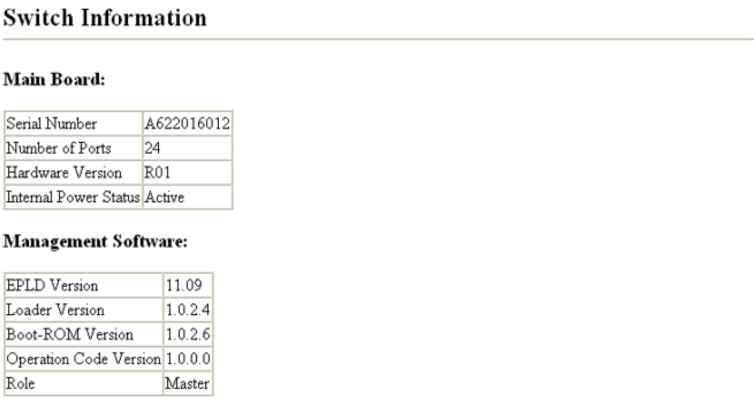
Main Board

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in RJ-45 ports and expansion ports.
- **Hardware Version** – Hardware version of the main board.
- **Internal Power Status** – Displays the status of the internal power supply.

Management Software

- **EPLD Version** – Version number of the Electronically Programmable Logic Device code.
- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Displays the switch as a master or slave unit.

Web – Click System, Switch Information.


Switch Information

Main Board:

Serial Number	A622016012
Number of Ports	24
Hardware Version	R01
Internal Power Status	Active

Management Software:

EPLD Version	11.09
Loader Version	1.0.2.4
Boot-ROM Version	1.0.2.6
Operation Code Version	1.0.0.0
Role	Master

Figure 3-4. Switch Information

CLI – Use the following command to display version information.

```
Console#show version                                                    4-62
Unit 1
 Serial Number:
 Hardware Version:
 EPLD Version:             0.01
 Number of Ports:          28
 Main Power Status:        Up
 Redundant Power Status:   Not present

Agent (Master)
 Unit ID:                  1
 Loader Version:           1.0.0.0
 Boot ROM Version:         1.0.0.3
 Operation Code Version:   1.0.0.8

Console#
```

Displaying Bridge Extension Capabilities

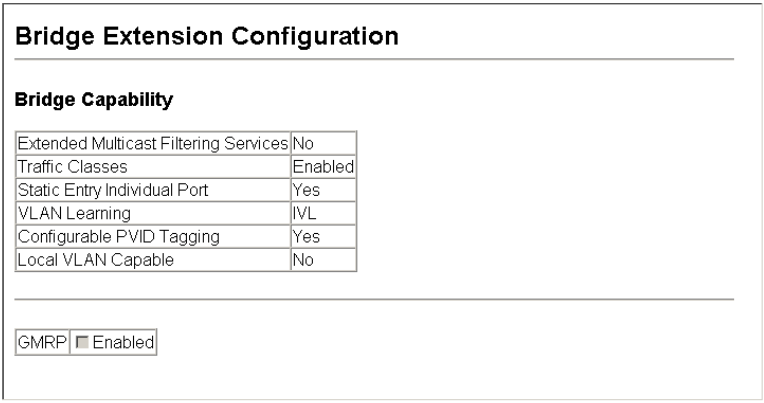
The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

Field Attributes

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to “Displaying Private VLAN Interface Information” on page 3-136.)

- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to “Setting Static Addresses” on page 3-108.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to “VLAN Configuration” on page 3-123.)
- **Local VLAN Capable** – This switch supports multiple local bridges; i.e., multiple spanning trees. (Refer to “VLAN Configuration” on page 3-161.)
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Web – Click System, Bridge Extension Configuration.


Bridge Extension Configuration

Bridge Capability

Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Learning	IVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

GMRP	Enabled

Figure 3-5. Bridge Extension Configuration

CLI – Enter the following command.

```
Console#show bridge-ext                                                    4-166
 Max Support VLAN Numbers:                256
 Max Support VLAN ID:                     4094
 Extended Multicast Filtering Services:   No
 Static Entry Individual Port:            Yes
 VLAN Learning:                           IVL
 Configurable PVID Tagging:               Yes
 Local VLAN Capable:                      No
 Traffic Classes:                         Enabled
 GMRP:                                    Disabled
Console#
```

Setting the Switch's IP Address

This section describes how to configure an initial IP interface for management access over the network. The IP address for this switch is unassigned by default. To manually configure an address, you need to change the switch's default settings (IP address 0.0.0.0 and netmask 255.0.0.0) to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment (if routing is not enabled on this switch).

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. 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.

Command Usage

- This section describes how to configure a single local interface for initial access to the switch. To configure multiple IP interfaces on this switch, you must set up an IP interface for each VLAN (page 3-115).
- To enable routing between the different interfaces on this switch, you must enable IP routing (page 3-114).
- To enable routing between the interfaces defined on this switch and external network interfaces, you must configure static routes (page 3-128) or use dynamic routing; i.e., either RIP (page 3-130) or OSPF (page 3-140).
- The precedence for configuring IP interfaces is the IP / General / Routing Interface menu (page 3-115), static routes (page 3-128), and then dynamic routing.

Command Attributes

- Management VLAN – ID of the configured VLAN (1-4093, no leading zeroes). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.
- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)
- **IP Address** – Address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)
- **Gateway IP Address** – IP address of the gateway router between this device and management stations that exist on other network segments. (Default: 0.0.0.0)
- **MAC Address** – The physical layer address for this switch.
- **Restart DHCP** – Requests a new IP address from the DHCP server.

Manual Configuration

Web – Click System, IP Configuration. Select the VLAN through which the management station is attached, set the IP Address Mode to “Static,” enter the IP address, subnet mask and gateway, then click Apply.

and specify a “Primary” interface,

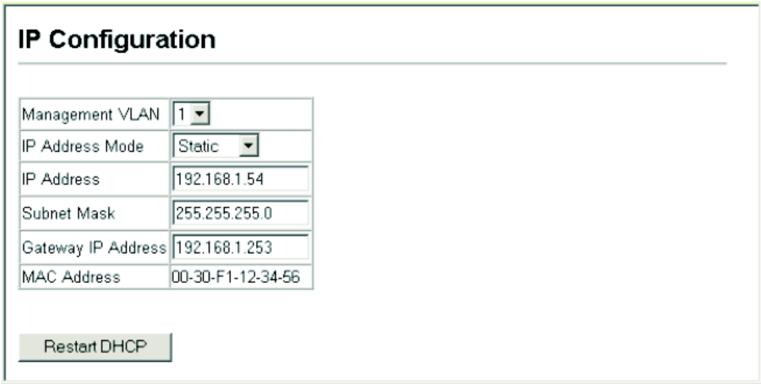


Figure 3-6. Manual IP Configuration

CLI – Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1                                    4-111
Console(config-if)#ip address 10.1.0.254 255.255.255.0              4-219
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254                    4-221
Console(config)#
```

Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services.

Web – Click System, IP Configuration. Specify the VLAN to which the management station is attached, set the IP Address Mode to DHCP or BOOTP. Click Apply to save your changes. Then click Restart DHCP to immediately request a new address. Note that the switch will also broadcast a request for IP configuration settings on each power reset.

IP, General, Routing Interface

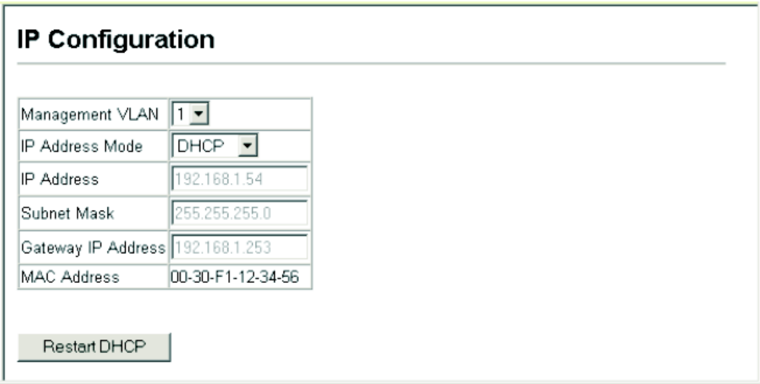


Figure 3-7. DHCP IP Configuration

Note: If you lose your management connection, use a console connection and enter "show ip interface" to determine the new switch address.

CLI – Specify the management interface, and set the IP address mode to DHCP or BOOTP, and then enter the "ip dhcp restart" command.

```
Console#config
Console(config)#interface vlan 1                                4-111
Console(config-if)#ip address dhcp                              4-219
Console(config-if)#end
Console#ip dhcp restart                                         4-220
Console#show ip interface                                       4-222
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service via the CLI.

Web – If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart                                          4-220
Console#
```

Enabling Jumbo Frames

You can enable jumbo frames to support data packets up to 9000 bytes in size.

Command Usage

- This section describes how to configure a single local interface for initial access to the switch. To configure multiple IP interfaces on this switch, you must set up an IP interface for each VLAN (page 3-115).
- To enable routing between the different interfaces on this switch, you must enable IP routing (page 3-114).
- To enable routing between the interfaces defined on this switch and external network interfaces, you must configure static routes (page 3-128) or use dynamic routing; i.e., either RIP (page 3-130) or OSPF (page 3-140).
- The precedence for configuring IP interfaces is the IP / General / Routing Interface menu (page 3-115), static routes (page 3-128), and then dynamic routing.

Command Attributes

- Jumbo Packet Status – Check the box to enable jumbo frames.

Web – Click IP, General, Routing Interface System, Jumbo Frames.and specify a “Primary” interface,

Figure 3-8. Enabling Jumbo Frames

CLI – Specify the jumbo frame status.

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

Managing Firmware

You can upload/download firmware to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version.

Note: Runtime code can also be upgraded by using Batch Upgrade. Batch Upgrade can discover switches on local, or other networks. After discovering the switches, Batch Upgrade can then be set to automatically upgrade the runtime code on all discovered switches. Batch Upgrade is provided in the Batch Upgrade folder in the CD provided with this switch. For details see the Batch Upgrade document in this Batch Upgrade folder.

Command Attributes

- File Transfer Method – The firmware copy operation includes these options.
  - file to file – Copies a file within the switch directory, assigning it a new name.
  - file to tftp – Copies a file from the switch to a TFTP server.
  - tftp to file – Copies a file from a TFTP server to the switch.
- **TFTP Server IP Address** – The IP address of a TFTP server.
- File Type – Specify opcode (operational code) to copy firmware.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

Note: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch. The currently designated startup version of this file cannot be deleted.

Downloading System Software from a Server

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

Web – Click System, File Management, Copy Operation. Select “tftp to file” as the file transfer method, enter the IP address of the TFTP server, set the file type to “opcode,” enter the file name of the software to download, select a file on the switch to overwrite or specify a new file name, then click Apply. If you replaced the current firmware used for startup and want to start using the new operation code, reboot the system via the System/Reset menu.

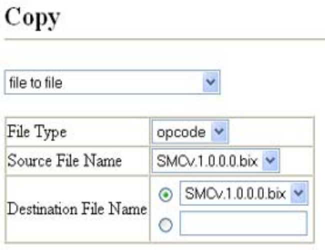


Figure 3-9. Copy Firmware

If you download to a new destination file, go to the System, File Management, Set Start-Up menu, mark the operation code file used at startup, and click Apply. To start the new firmware, reboot the system via the System/Reset menu.

Set Start-Up

Note: You can only change one file type at a time.

	Name	Type	Startup	Size(bytes)
○	Factory_Default_Config.cfg	Config_File	N	455
⦿	startup1.cfg	Config_File	Y	2925
⦿	SMCv.1.0.0.0.bix	Operation_Code	Y	3504976

Figure 3-10. Setting the Startup Code

To delete a file select System, File Management, Delete. Select the file name from the given list by checking the tick box and click Apply. Note that the file currently designated as the startup code cannot be deleted.

Delete

	Name	Type	Startup	Size (bytes)
☐	Factory_Default_Config.cfg	Config_File	N	455
☐	startup1.cfg	Config_File	Y	2925
☐	SMCv.1.0.0.0.bix	Operation_Code	Y	3504976

Figure 3-11. Deleting Files

CLI – Enter the IP address of the TFTP server, select “config” or “opcode” file type, then enter the source and destination file names, set the new file to start up the system, and then restart the switch.

```
Console#copy tftp file                                              4-64
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: v1000-18.bix
Destination file name: V1.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode:V1.0                             4-69
Console(config)#exit
Console#reload                                                      4-21
```

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server. The configuration file can be later downloaded to restore the switch’s settings.

Command Attributes

- File Transfer Method – The firmware copy operation includes these options.
  - file to file – Copies a file within the switch directory, assigning it a new name.
  - file to running-config – Copies a file in the switch to the running configuration.
  - file to startup-config – Copies a file in the switch to the startup configuration.
  - file to tftp – Copies a file from the switch to a TFTP server.
  - running-config to file – Copies the running configuration to a file.
  - running-config to startup-config – Copies the running config to the startup config.
  - running-config to tftp – Copies the running configuration to a TFTP server.
  - startup-config to file – Copies the startup configuration to a file on the switch.
  - startup-config to running-config – Copies the startup config to the running config.
  - startup-config to tftp – Copies the startup configuration to a TFTP server.
  - tftp to file – Copies a file from a TFTP server to the switch.
  - tftp to running-config – Copies a file from a TFTP server to the running config.
  - tftp to startup-config – Copies a file from a TFTP server to the startup config.
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Type** – Specify config (configuration) to copy configuration file.
- **File Name** — The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

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

Downloading Configuration Settings from a Server

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the file “Factory_Default_Config.cfg” can be copied to the TFTP server, but cannot be used as the destination on the switch.

Web – Click System, File Management, Copy Operation. Select “tftp to startup-config” or “tftp to file” and enter the IP address of the TFTP server. Specify the name of the file to download and select a file on the switch to overwrite or specify a new file name, then click Apply.

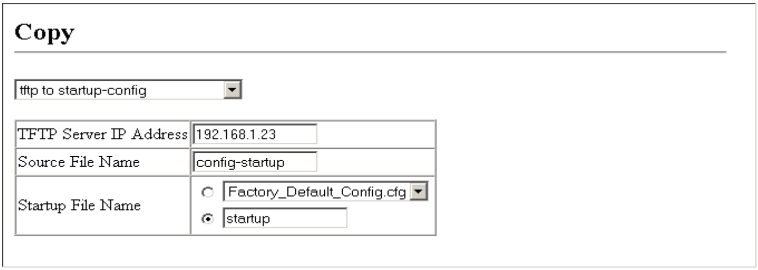


Figure 3-12. Downloading Configuration Settings for Startup

If you download to a new file name using “tftp to startup-config” or “tftp to file,” the file is automatically set as the start-up configuration file. To use the new settings, reboot the system via the System/Reset menu.

Note: You can also select any configuration file as the start-up configuration by using the System/File Management/Set Start-Up page.

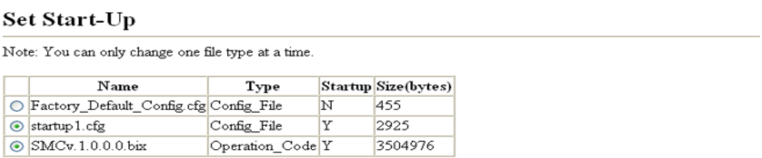


Figure 3-13. Setting the Startup Configuration Settings

CLI – Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config                                          4-64
TFTP server ip address: 192.168.1.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
```

To select another configuration file as the start-up configuration, use the **boot system** command and then restart the switch.

```
Console#config
Console(config)#boot system config: startup-new                           4-69
Console(config)#exit
Console#reload                                                            4-21
```

Console Port Settings

You can access the onboard configuration program by attaching a VT100 compatible device to the switch's serial console port. Management access through the console port is controlled by various parameters, including a password, timeouts, and basic communication settings. These parameters can be configured via the web or CLI interface.

Command Attributes

- Login Timeout – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0-300 seconds; Default: 0 seconds)
- Exec Timeout – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0-65535 seconds; Default: 600 seconds)
- Password Threshold – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)
- Silent Time – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 0-65535; Default: 0)
- Data Bits – Sets the number of data bits per character that are interpreted and generated by the console port. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character. (Default: 8 bits)

- Parity – Defines the generation of a parity bit. Communication protocols provided by some terminals can require a specific parity bit setting. Specify Even, Odd, or None. (Default: None)
- Speed – Sets the terminal line's baud rate for transmit (to terminal) and receive (from terminal). Set the speed to match the baud rate of the device connected to the serial port. (Range: 9600, 19200, or 38400 baud; Default: 9600 bps)
- Stop Bits – Sets the number of the stop bits transmitted per byte. (Range: 1-2; Default: 1 stop bit)

Available in CLI only:

- Password – Specifies a password for the line connection. When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. (Default: No password)
- Login – Enables password checking at login. You can select authentication by a single global password as configured for the Password parameter, or by passwords set up for specific user-name accounts. (Default: Local)

Web – Click System, Line, Console. Specify the console port connection parameters as required, then click Apply.

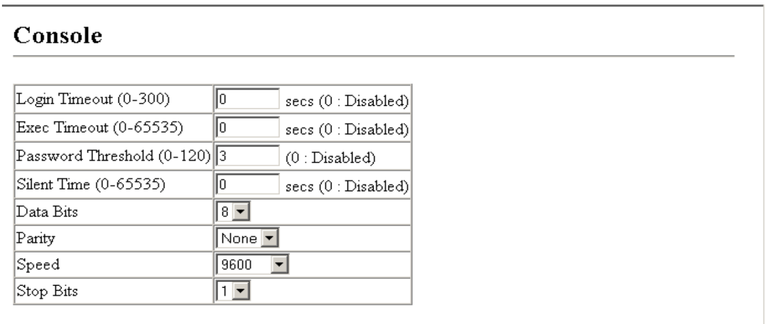


Figure 3-14. Console Port Setting

CLI – Enter Line Configuration mode for the console, then specify the connection parameters as required. To display the current console port settings, use the **show line** command from the Normal Exec level.

```
Console(config)#line console                                     4-10
Console(config-line)#login local                                 4-11
Console(config-line)#password 0 secret                           4-12
Console(config-line)#timeout login response 0                    4-13
Console(config-line)#exec-timeout 0                              4-13
Console(config-line)#password-thresh 3                           4-14
Console(config-line)#silent-time 60                              4-15
Console(config-line)#databits 8                                  4-15
Console(config-line)#parity none                                 4-16
Console(config-line)#speed 9600                                  4-16
Console(config-line)#stopbits 1                                  4-17
Console(config-line)#end
Console#show line                                                4-18
 Console configuration:
  Password threshold:  3 times
  Interactive timeout: Disabled
  Login timeout:       Disabled
  Silent time:         60
  Baudrate:            9600
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout:       300 sec
Console#
```

Telnet Settings

You can access the onboard configuration program over the network using Telnet (i.e., a virtual terminal). Management access via Telnet can be enabled/disabled and other various parameters set, including the TCP port number, timeouts, and a password. These parameters can be configured via the web or CLI interface.

Command Attributes

- **Telnet Status** – Enables or disables Telnet access to the switch. (Default: Enabled)
- **Telnet Port Number** – Sets the TCP port number for Telnet on the switch. (Default: 23)
- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0-300 seconds; Default: 300 seconds)
- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0-65535 seconds; Default: 600 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the

system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)

Available in CLI only:

- Password – Specifies a password for the line connection. When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. (Default: No password)
- **Login** – Enables password checking at login. You can select authentication by a single global password as configured for the Password parameter, or by passwords set up for specific user-name accounts. (Default: Local)

Web – Click System, Line, Telnet. Specify the connection parameters for Telnet access, then click Apply..

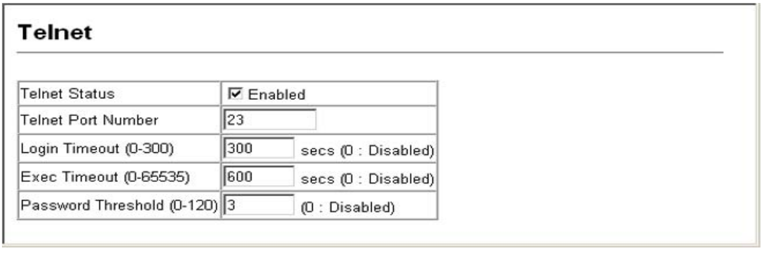


Figure 3-15. Enabling Telnet

CLI – Enter Line Configuration mode for a virtual terminal, then specify the connection parameters as required. To display the current virtual terminal settings, use the **show line** command from the Normal Exec level.

```
Console(config)#line vty                                       4-10
Console(config-line)#login local                               4-11
Console(config-line)#password 0 secret                         4-12
Console(config-line)#timeout login response 300                4-13
Console(config-line)#exec-timeout 600                          4-13
Console(config-line)#password-thresh 3                         4-14
Console(config-line)#end
Console#show line                                              4-18
 Console configuration:
  Password threshold:  3 times
  Interactive timeout: Disabled
  Login timeout:       Disabled
  Silent time:         Disabled
  Baudrate:            9600
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout: 300 sec
Console#
```

Configuring Event Logging

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

Displaying Log Messages

The Logs page allows you to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Web – Click System, Log, Logs.

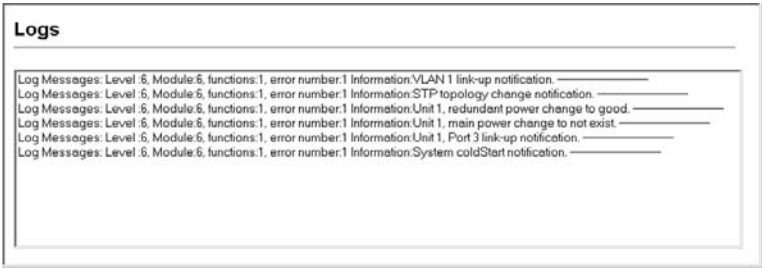


Figure 3-16. Displaying Logs

CLI – This example shows the event message stored in RAM.

```
Console#show log ram                                                  4-48
[1] 00:01:37 2001-01-01
   "DHCP request failed - will retry later."
   level: 4, module: 9, function: 0, and event no.: 10
[0] 00:00:35 2001-01-01
   "System coldStart notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#
```

System Log Configuration

The system allows you to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 6 to be logged to RAM.

Command Attributes

- **System Log Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)
- **Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)

Table 3-3 Logging Levels

Level	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only

Table 3-3 Logging Levels (Continued)

Level	Severity Name	Description
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

- **RAM Level** – Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

Note: The Flash Level must be equal to or less than the RAM Level.

Web – Click System, Log, System Logs. Specify System Log Status, set the level of event messages to be logged to RAM and flash memory, then click Apply.

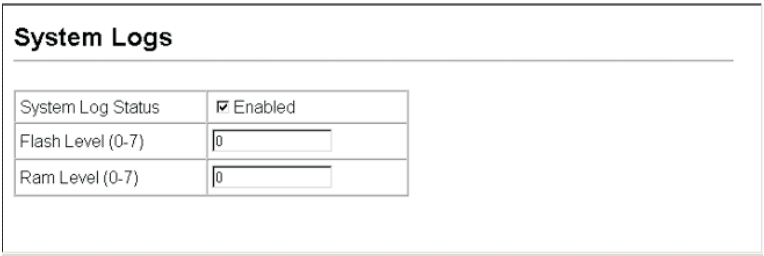


Figure 3-17. System Logs

CLI – Enable system logging and then specify the level of messages to be logged to RAM and flash memory. Use the **show logging** command to display the current settings.

```
Console(config)#logging on                                    4-43
Console(config)#logging history ram 0                         4-44
Console(config)#end
Console#show logging flash                                    4-47
Syslog logging: Enabled
History logging in FLASH: level emergencies
Console#
```

Remote Log Configuration

The Remote Logs page allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the error messages sent to only those messages below a specified level.

Command Attributes

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Enabled)
- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service. The attribute specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
- **Logging Trap** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- **Host IP List** – Displays the list of remote server IP addresses that receive the syslog messages. The maximum number of host IP addresses allowed is five.
- **Host IP Address** – Specifies a new server IP address to add to the Host IP List.

Web – Click System, Log, Remote Logs. To add an IP address to the Host IP List, type the new IP address in the Host IP Address box, and then click Add. To delete an IP address, click the entry in the Host IP List, and then click Remove.

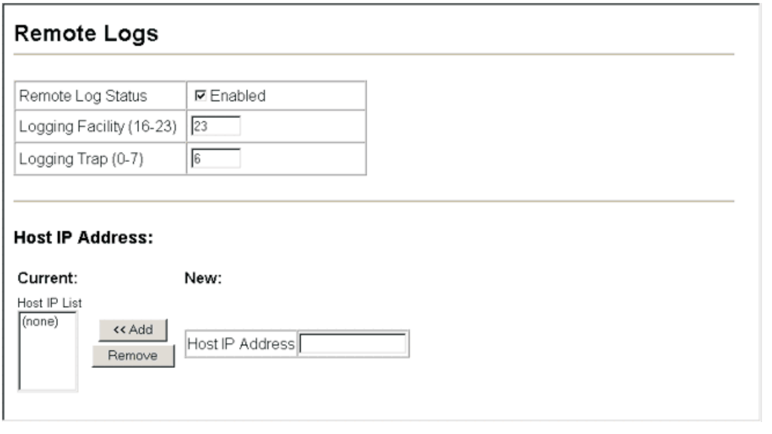


Figure 3-18. Remote Logs

CLI – Enter the syslog server host IP address, choose the facility type and set the logging trap.

```
Console(config)#logging host 192.168.1.15                              4-45
Console(config)#logging facility 23                                    4-45
Console(config)#logging trap 4                                         4-46
Console(config)#end
Console#show logging trap                                              4-47
Syslog logging:              Enabled
REMOTELOG status:            Enabled
REMOTELOG facility type:     local use 7
REMOTELOG level type:        Warning conditions
REMOTELOG server ip address: 192.168.1.15
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#
```

Simple Mail Transfer Protocol

SMTP (Simple Mail Transfer Protocol) is used to send email messages between servers. The messages can be retrieved using POP or IMAP clients.

Command Attributes

- **Admin Status** – Enables/disables the SMTP function. (Default: Enabled)
- **Email Source Address** – This command specifies SMTP servers email addresses that can send alert messages.
- **Severity** – Specifies the degree of urgency that the message carries.
  - Debugging – Sends a debugging notification. (Level 7)
  - Information – Sends informatative notification only. (Level 6)
  - Notifice – Sends notification of a normal but significant condition, such as a cold start. (Level 5)
  - Warning – Sends notification of a warning condition such as return false, or unexpected return. (Level 4)
  - Error – Sends notification that an error conditions has occurred, such as invalid input, or default used. (Level 3)
  - Critical – Sends notification that a critical condition has occurred, such as memory allocation, or free memory error - resource exhausted. (Level 2)
  - Alert – Sends urgent notification that immediate action must be taken. (Level 1)
  - Emergency – Sends an emergency notification that the system is now unusable. (Level 0)
- **SMTP Server List** – Specifies a list of recipient SMTP servers.
- **SMTP Server** – Specifies a new SMTP server address to add to the SMTP Server List.
- **Email Destination Address List** – Specifies a list of recipient Email Destination Address.

- **Email Destination Address** – This command specifies SMTP servers that may receive alert messages.

Web – Click System, Log, SMTP. To add an IP address to the Server IP List, type the new IP address in the Server IP Address box, and then click Add. To delete an IP address, click the entry in the Server IP List, and then click Remove.

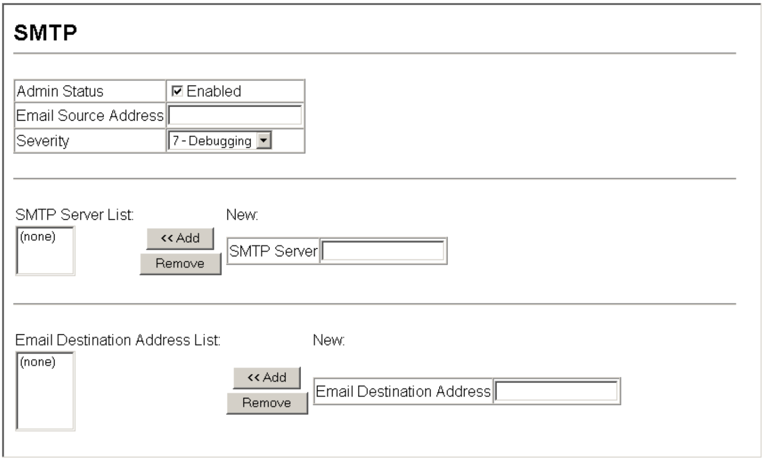


Figure 3-19. Enabling and Configuring SMTP

CLI – Enter the host ip address, followed by the mail severity level, source and destination email addresses and enter the sendmail command to complete the action. Use the show logging command to display SMTP information.

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#logging sendmail level 3
Console(config)#logging sendmail source-email
bill@this-company.com
Console(config)#logging sendmail destination-email
ted@this-company.com
Console(config)#logging sendmail
Console#
```

Resetting the System

Web – Click System, Reset. Click the Reset button to reboot the switch. When prompted, confirm that you want reset the switch.

Figure 3-20. Resetting the System

CLI – Use the **reload** command to restart the switch. When prompted, confirm that you want to reset the switch.

```
Console#reload                                                   4-21
System will be restarted, continue <y/n>?
```

Note: When restarting the system, it will always run the Power-On Self-Test.

Setting the System Clock

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock using the CLI. (See “calendar set” on page 4-56.) If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

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

Configuring SNTP

You can configure the switch to send time synchronization requests to specific time servers.

Command Attributes

- **SNTP Client** – Configures the switch to operate as an SNTP client. This requires at least one time server to be specified in the SNTP Server field. (Default: Disabled)
- **SNTP Poll Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)
- **SNTP Server** – Sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

Web – Select SNTP, Configuration. Modify any of the required parameters, and click Apply.

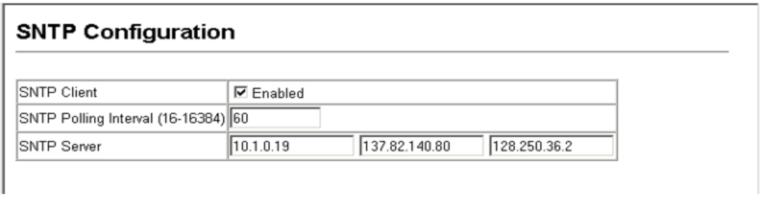


Figure 3-21. SNTP Configuration

CLI – This example configures the switch to operate as an SNTP unicast client and then displays the current time and settings.

```
Console(config)#sntp client                                          4-54
Console(config)#sntp poll 60                                         4-55
Console(config)#sntp server 10.1.0.19 137.82.140.80 128.250.36.2    4-54
Console(config)#exit
Console#show sntp
Current time:  Jan  6 14:56:05 2004
Poll interval: 60
Current  mode:  unicast
SNTP status : Enabled
SNTP server 10.1.0.19 137.82.140.80 128.250.36.2
Current server: 128.250.36.2
Console#
```

Setting the Time Zone

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

Command Attributes

- **Current Time** – Displays the current time.
- **Name** – Assigns a name to the time zone. (Range: 1-29 characters)
- **Hours (0-13)** – The number of hours before/after UTC**.**
- **Minutes (0-59)** – The number of minutes before/after UTC.
- **Direction** – Configures the time zone to be before (east) or after (west) UTC.

Web – Select SNTP, Clock Time Zone. Set the offset for your time zone relative to the UTC, and click Apply.

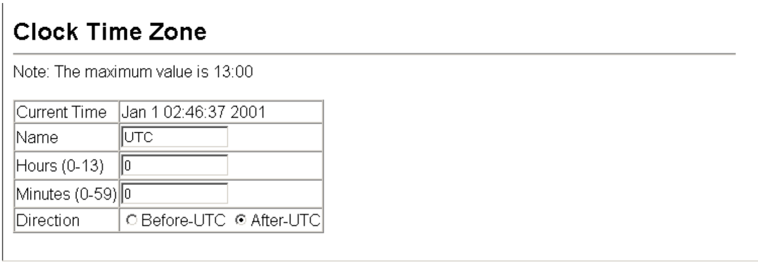


Figure 3-22. Setting the Time Zone

CLI - This example shows how to set the time zone for the system clock.

```
Console(config)#clock timezone Dhaka hours 6 minute 0 after-UTC    4-56
Console#
```

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3 clients. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as SMC EliteView. Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Access to the switch using from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having it's own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to "groups" that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as "views." The switch has a default view (all MIB objects) and default groups defined for security models v1 and v2c. The following table shows the security models and levels available and the system default settings.

Table 3-4 SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Notify View	Security
v1	noAuth NoPriv	public (read only)	defaultview	none	none	Community string only
v1	noAuth NoPriv	private (read/ write)	defaultview	defaultview	none	Community string only
v1	noAuth NoPriv	user defined	user defined	user defined	user defined	Community string only
v2c	noAuth NoPriv	public (read only)	defaultview	none	none	Community string only
v2c	noAuth NoPriv	private (read/ write)	defaultview	defaultview	none	Community string only
v2c	noAuth NoPriv	user defined	user defined	user defined	user defined	Community string only
v3	noAuth NoPriv	user defined	user defined	user defined	user defined	A user name match only
v3	Auth NoPriv	user defined	user defined	user defined	user defined	Provides user authentication via MD5 or SHA algorithms
v3	Auth Priv	user defined	user defined	user defined	user defined	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

Note: The predefined default groups and view can be deleted from the system. You can then define customized groups and views for the SNMP clients that require access.

Enabling the SNMP Agent

Enables SNMPv3 service for all management clients (i.e., versions 1, 2c, 3).

Command Attributes

- **SNMP Agent Status** – Enables SNMP on the switch.

Web – Click SNMP, Agent Status. Enable the SNMP Agent by marking the Enabled checkbox, and click Apply.

Figure 3-23. Enabling the SNMP Agent

CLI – The following example enables SNMP on the switch.

```
Console(config)#snmp-server                                         4-96
Console(config)#
```

Setting Community Access Strings

You may configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. All community strings used for IP Trap Managers should be listed in this table. For security reasons, you should consider removing the default strings.

Command Attributes

- **SNMP Community Capability** – The switch supports up to five community strings.
- **Current** – Displays a list of the community strings currently configured.
- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.
- Default strings: “public” (read-only access), “private” (read/write access)
- Range: 1-32 characters, case sensitive
- **Access Mode** – Specifies the access rights for the community string:
  - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
  - **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click Add.

Figure 3-24. Configuring SNMP Community Strings

CLI – The following example adds the string “spiderman” with read/write access.

```
Console(config)#snmp-server community spiderman rw                4-98
Console(config)#
```

Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as SMC EliteView). You can specify up to five management stations that will receive authentication failure messages and other notification messages from the switch.

Command Usage

- If you specify an SNMP Version 3 host, then the “Trap Manager Community String” is interpreted as an SNMP user name. If you use V3 authentication or encryption options (authNoPriv or authPriv), the user name must first be defined in the SNMPv3 Users page (page 3-41). Otherwise, the authentication password and/or privacy password will not exist, and the switch will not authorize SNMP access for the host. However, if you specify a V3 host with the no authentication (noAuth) option, an SNMP user account will be automatically generated, and the switch will authorize SNMP access for the host.
- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.
- To send an inform to a SNMPv2c host, complete these steps:

1. Enable the SNMP agent (page 3-36).
2. Enable trap informs as described in the following pages.
3. Create a view with the required notification messages (page 3-48).
4. Create a group that includes the required notify view (page 3-45).

- To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent (page 3-36).
2. Enable trap informs as described in the following pages.
3. Create a view with the required notification messages (page 3-48).
4. Create a group that includes the required notify view (page 3-45).
5. Specify a remote engine ID where the user resides (page 3-40).
6. Then configure a remote user (page 3-43).

Command Attributes

- **Trap Manager Capability** – This switch supports up to five trap managers.
- **Current** – Displays a list of the trap managers currently configured.
- **Trap Manager IP Address** – IP address of a new management station to receive notification messages.
- **Trap Manager Community String** – Specifies a valid community string for the new trap manager entry. Though you can set this string in the Trap Managers table, we recommend that you define this string in the SNMP Configuration page (for Version 1 or 2c clients), or define a corresponding “User Name” in the SNMPv3 Users page (for Version 3 clients). (Range: 1-32 characters, case sensitive)
- **Trap UDP Port** – Specifies the UDP port number used by the trap manager.
- **Trap Version** – Indicates if the user is running SNMP v1, v2c, or v3. (Default: v1)
- **Trap Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - **AuthPriv** – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Trap Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
  - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
  - **Retry times** – The maximum number of times to resend an inform message if

the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

- **Enable Authentication Traps**[1] – Issues a notification message to specified IP trap managers whenever authentication of an SNMP request fails. (Default: Enabled)
- **Enable Link-up and Link-down Traps** – Issues a notification message whenever a port link is established or broken. (Default: Enabled)

Web – Click SNMP, Configuration. Enter the IP address and community string for each management station that will receive trap messages, specify the UDP port, trap version, trap security level (for v3 clients), trap inform settings (for v2c/v3 clients), and then click Add. Select the trap types required using the check boxes for Authentication and Link-up/down traps, and then click Apply.

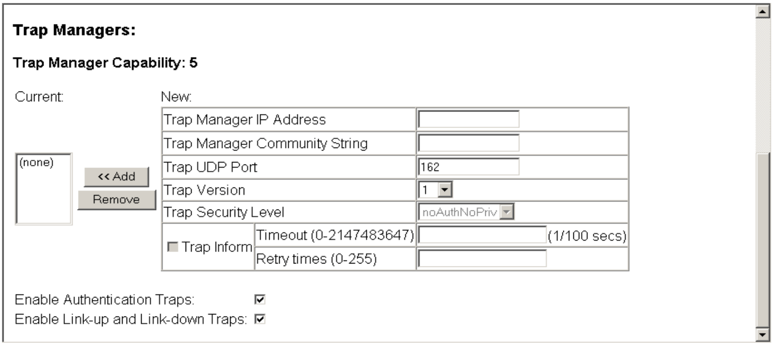


Figure 3-25. Configuring SNMP Trap Managers

CLI – This example adds a trap manager and enables authentication traps.

```
Console(config)#snmp-server host 10.1.19.23 inform private version 2c
udp-port 160                                                     4-100
Console(config)#snmp-server enable traps authentication          4-102
Console(config)#
```

Configuring SNMPv3 Management Access

To configure SNMPv3 management access to the switch, follow these steps:

1. If you want to change the default engine ID, it must be changed first before configuring other parameters.
2. Specify read and write access views for the switch MIB tree.
3. Configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy).

1. These are legacy notifications and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notification View (page 3-45).

4. Assign SNMP users to groups, along with their specific authentication and privacy passwords.

Setting the Local Engine ID

An SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

A new engine ID can be specified by entering 1 to 26 hexadecimal characters. If less than 26 characters are specified, trailing zeroes are added to the value. For example, the value “1234” is equivalent to “1234” followed by 22 zeroes.

Web – Click SNMP, SNMPv3, Engine ID. Enter an ID of up to 26 hexadecimal characters and then click Save.

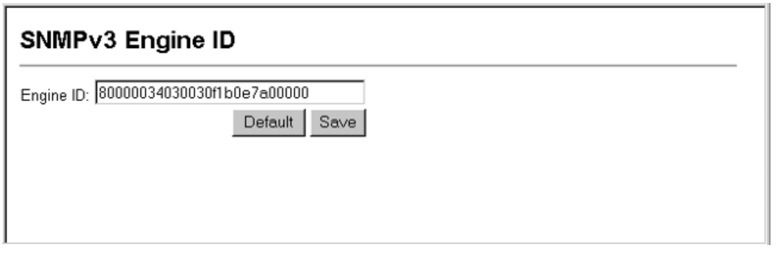


Figure 3-26. Setting an Engine ID

CLI – This example sets an SNMPv3 engine ID.

```
Console(config)#snmp-server engine-id local 12345abcdef          4-103
Console(config)#exit
Console#show snmp engine-id                                      4-104
Local SNMP engineID: 12345abcdef000000000000000
Local SNMP engineBoots: 1
Console#
```

Specifying a Remote Engine ID

To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent’s SNMP engine ID before you can send proxy requests or informs to it. (See “Specifying Trap Managers and Trap Types” on page 3-37 and “Configuring Remote SNMPv3 Users” on page 3-43.)

The engine ID can be specified by entering 1 to 26 hexadecimal characters. If less than 26 characters are specified, trailing zeroes are added to the value. For example, the value “1234” is equivalent to “1234” followed by 22 zeroes.

Web – Click SNMP, SNMPv3, Remote Engine ID. Enter an ID of up to 26 hexadecimal characters and then click Save.

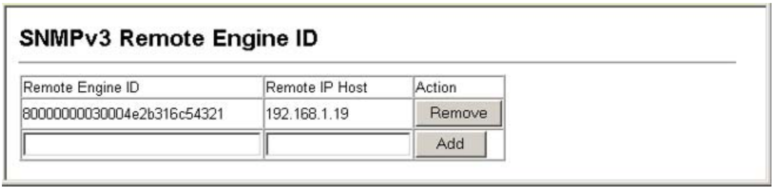


Figure 3-27. Setting an Engine ID

CLI – This example specifies a remote SNMPv3 engine ID.

```
Console(config)#snmp-server engineID remote 54321 192.168.1.19     4-103
Console(config)#exit
Console#show snmp engine-id                                         4-104
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                                               IP address
80000000030004e2b316c54321
192.168.1.19
Console#
```

Configuring SNMPv3 Users

Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

Command Attributes

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The security level used for the user:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).

- AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.
- **Actions** – Enables the user to be assigned to another SNMPv3 group.

Web – Click SNMP, SNMPv3, Users. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete. To change the assigned group of a user, click Change Group in the Actions column of the users table and select the new group.

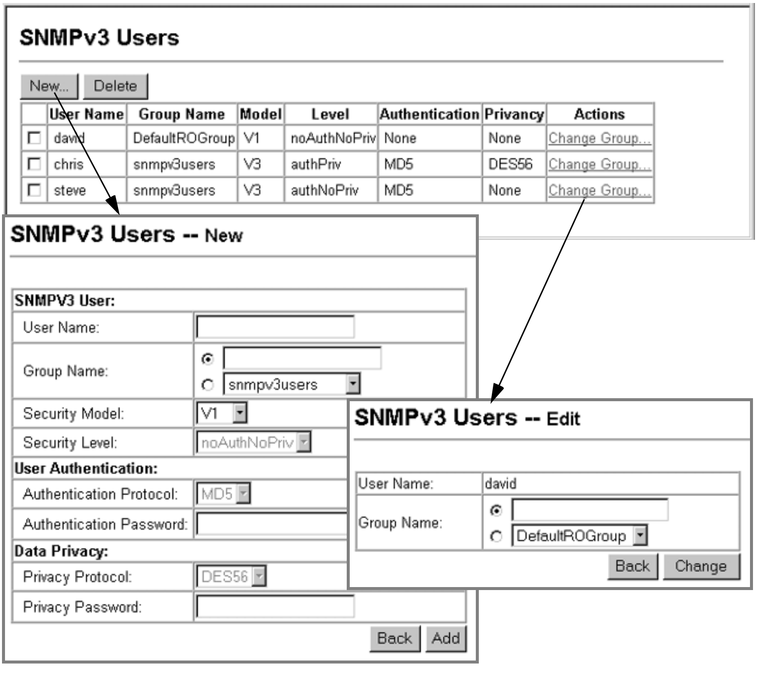


Figure 3-28. Configuring SNMPv3 Users

CLI – Use the **snmp-server user** command to configure a new user name and assign it to a group.

```
Console(config)#snmp-server user chris group r&d v3 auth md5 greenpeace
priv des56 einstien                                                4-109
Console(config)#exit
Console#show snmp user                                             4-110
EngineId: 80000034030001f488f5200000
User Name: chris
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Configuring Remote SNMPv3 Users

Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. (See “Specifying Trap Managers and Trap Types” on page 3-37 and “Specifying a Remote Engine ID” on page 3-40.)

Command Attributes

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Engine ID** – The engine identifier for the SNMP agent on the remote device where the remote user resides. Note that the remote engine identifier must be specified before you configure a remote user. (See “Specifying a Remote Engine ID” on page 3-40.)
- **Remote IP** – The Internet address of the remote device where the user resides.
- **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v1)
- **Security Level** – The security level used for the user:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)

- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.

Web – Click SNMP, SNMPv3, Remote Users. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete.

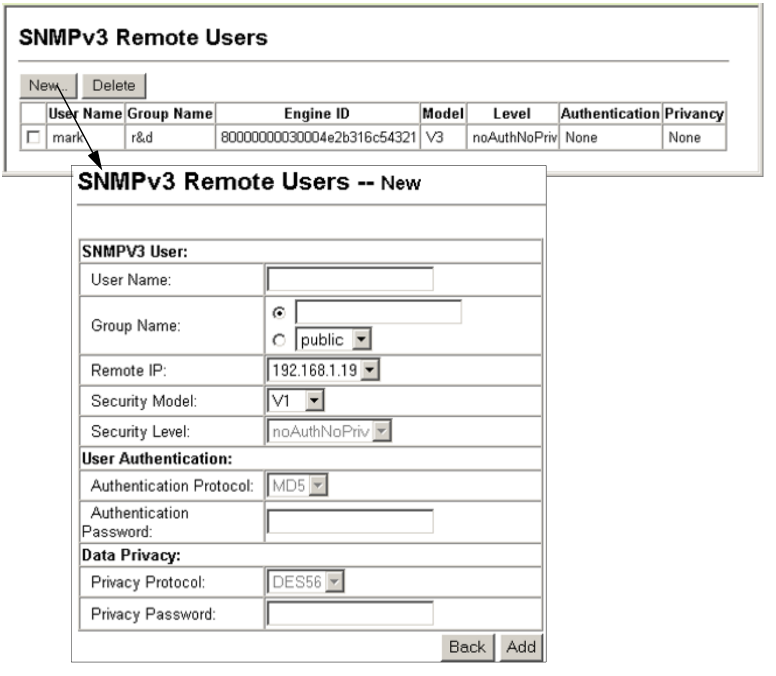


Figure 3-29. Configuring Remote SNMPv3 Users

CLI – Use the **snmp-server user** command to configure a new user name and assign it to a group.

```
Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3
auth md5 greenpeace priv des56 einstien                             4-109
Console(config)#exit
Console#show snmp user                                              4-110
No user exist.

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: none
Privacy Protocol: none
Storage Type: nonvolatile
Row Status: active

Console#
```

Configuring SNMPv3 Groups

An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

Command Attributes

- **Group Name** – The name of the SNMP group. (Range: 1-32 characters)
- **Model** – The group security model; SNMP v1, v2c or v3.
- **Level** – The security level used for the group:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications.
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Read View** – The configured view for read access. (Range: 1-64 characters)
- **Write View** – The configured view for write access. (Range: 1-64 characters)
- **Notify View** – The configured view for notifications. (Range: 1-64 characters)

Table 3-5 Supported Notification Messages

Object Label	Object ID	Description
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.

Table 3-5 Supported Notification Messages (Continued)

Object Label	Object ID	Description
topologyChange	1.3.6.1.2.1.17.0.2	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Discarding state. The trap is not sent if a newRoot trap is sent for the same transition.
SNMPv2 Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
warmStart	1.3.6.1.6.3.1.1.5.2	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.
linkDown[a]	1.3.6.1.6.3.1.1.5.3	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkUp[a]	1.3.6.1.6.3.1.1.5.4	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
authenticationFailure[a]	1.3.6.1.6.3.1.1.5.5	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
RMON Events (V2)		
risingAlarm	1.3.6.1.2.1.16.0.1	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
fallingAlarm	1.3.6.1.2.1.16.0.2	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

Table 3-5 Supported Notification Messages (Continued)

Object Label	Object ID	Description
Private Traps		
swPowerStatus ChangeTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.1	This trap is sent when the power state changes.
swIpFilterRejectTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.

a. These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu (page 3-39).

Web – Click SNMP, SNMPv3, Groups. Click New to configure a new group. In the New Group page, define a name, assign a security model and level, and then select read and write views. Click Add to save the new group and return to the Groups list. To delete a group, check the box next to the group name, then click Delete.

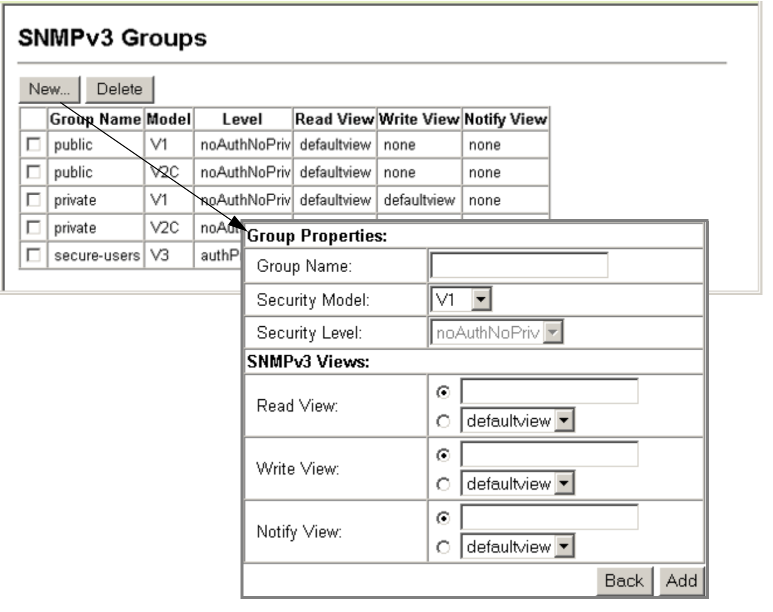


Figure 3-30. Configuring SNMPv3 Groups

CLI – Use the **snmp-server group** command to configure a new group, specifying the security model and level, and restricting MIB access to defined read and write views.

```
Console(config)#snmp-server group secure-users v3 priv read defaultview
write defaultview notify defaultview                                4-106
Console(config)#exit
Console#show snmp group                                             4-107
Group Name: secure-users
Security Model: v3
Read View: defaultview
Write View: defaultview
Notify View: defaultview
Storage Type: nonvolatile
Row Status: active

Console#
```

Setting SNMPv3 Views

SNMPv3 views are used to restrict user access to specified portions of the MIB tree. The predefined view “defaultview” includes access to the entire MIB tree.

Command Attributes

- **View Name** – The name of the SNMP view. (Range: 1-64 characters)
- **View OID Subtrees** – Shows the currently configured object identifiers of branches within the MIB tree that define the SNMP view.
- **Edit OID Subtrees** – Allows you to configure the object identifiers of branches within the MIB tree. Wild cards can be used to mask a specific portion of the OID string.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Web – Click SNMP, SNMPv3, Views. Click New to configure a new view. In the New View page, define a name and specify OID subtrees in the switch MIB to be included or excluded in the view. Click Back to save the new view and return to the SNMPv3 Views list. For a specific view, click on View OID Subtrees to display the current configuration, or click on Edit OID Subtrees to make changes to the view settings. To delete a view, check the box next to the view name, then click Delete.

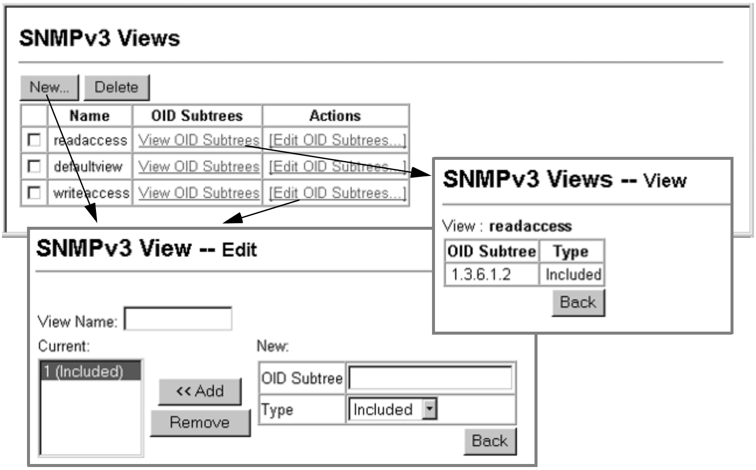


Figure 3-31. Configuring SNMPv3 Views

CLI – Use the **snmp-server view** command to configure a new view. This example view includes the MIB-2 interfaces table, and the wildcard mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a
1.3.6.1.2.1.2.2.1.1.* included                                  4-105
Console(config)#exit
Console#show snmp view                                          4-105
View Name: ifEntry.a
Subtree OID: 1.3.6.1.2.1.2.2.1.1.*
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: readaccess
Subtree OID: 1.3.6.1.2
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: nonvolatile
Row Status: active

Console#
```

User Authentication

You can restrict management access to this switch using the following options:

- **User Accounts** – Manually configure access rights on the switch for specified users.
- **Authentication Settings** – Use remote authentication to configure access rights.
- **HTTPS Settings** – Provide a secure web connection.
- **SSH Settings** – Provide a secure shell (for secure Telnet access).
- **Port Security** – Configure secure addresses for individual ports.
- **802.1X** – Use IEEE 802.1X port authentication to control access to specific ports.
- **ACL** - Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type).
- **IP Filter** – Filters management access to the web, SNMP or Telnet interface.

Configuring User Accounts

The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.”

Command Attributes

- Account List – Displays the current list of user accounts and associated access levels. (Default: admin, and guest)
- New Account – Displays configuration settings for a new account.
  - **User Name** – The name of the user.
  - (Maximum length: 8 characters; maximum number of users: 16)
  - **Access Level** – Specifies the user level.
    (Options: Normal and Privileged)
  - **Password** – Specifies the user password.
    (Range: 0-8 characters plain text, case sensitive)
  - **Confirm Password** – Re-enter the user password.
- **Change Password** – Sets a new password for the specified user name.
- **Add/Remove** – Adds or removes an account from the list.

Web – Click Security, User Accounts. To configure a new user account, specify a user name, select the user’s access level, then enter a password and confirm it. Click Add to save the new user account and add it to the Account List. To change the password for a specific user, enter the user name and new password, confirm the password by entering it again, then click Apply.

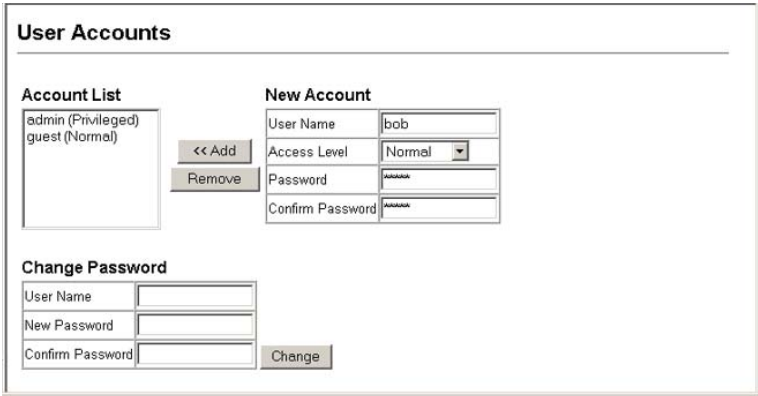


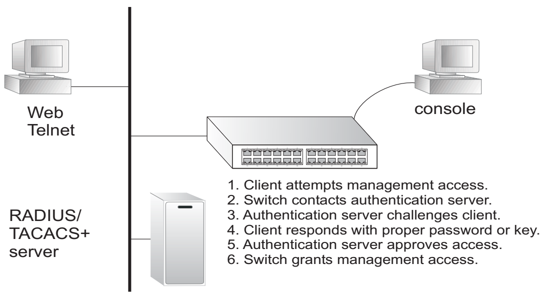
Figure 3-32. Access Levels

CLI – Assign a user name to access-level 15 (i.e., administrator), then specify the password.

```
Console(config)#username bob access-level 15                    4-25
Console(config)#username bob password 0 smith
Console(config)#
```

Configuring Local/Remote Logon Authentication

Use the Authentication Settings menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on RADIUS or TACACS+ protocols.



Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS -aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via the console port, web browser, or Telnet.
- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
  - **Local** – User authentication is performed only locally by the switch.
  - **Radius** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - **[authentication sequence]** – User authentication is performed by up to three authentication methods in the indicated sequence.
- RADIUS Settings
  - **Global** – Provides globally applicable RADIUS settings.
  - **ServerIndex** – Specifies one of five RADIUS servers that may be configured. The switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.
  - **Server Port Number** – Network (UDP) port of authentication server used for authentication messages.
    (Range: 1-65535; Default: 1812)
  - **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string.
    (Maximum length: 20 characters)

- **Number of Server Transmits** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
- **Timeout for a reply** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

• TACACS Settings

- **Server IP Address** – Address of the TACACS+ server.
  (Default: 10.11.12.13)
- **Server Port Number** – Network (TCP) port of TACACS+ server used for authentication messages.
  (Range: 1-65535; Default: 49)
- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string.
  (Maximum length: 20 characters)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI.
(See “username” on page 4-25.)

Web – Click Security, Authentication Settings. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click Apply.

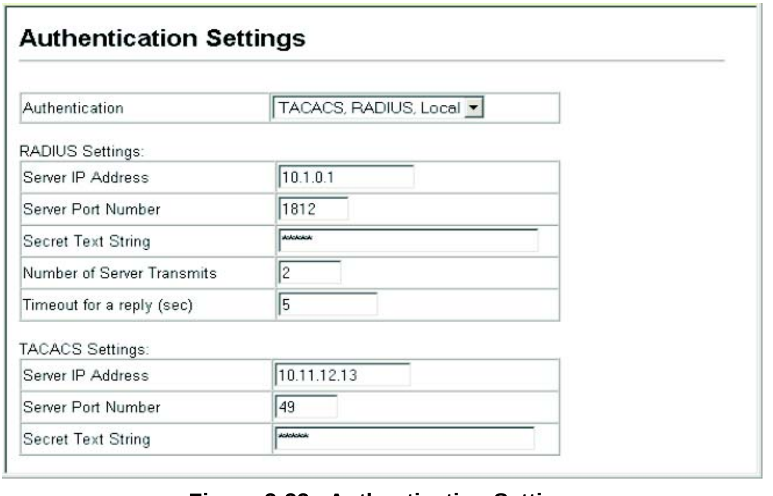


Figure 3-33. Authentication Settings

CLI – Specify all the required parameters to enable logon authentication.

```
Console(config)#authentication login radius                          4-70
Console(config)#radius-server host 192.168.1.25                      4-72
Console(config)#radius-server port 181                               4-73
Console(config)#radius-server key green                              4-74
Console(config)#radius-server retransmit 5                           4-74
Console(config)#radius-server timeout 10                             4-75
Console#show radius-server                                           4-75
Server IP address: 192.168.1.25
 Communication key with radius server:
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10
Console(config)#authentication login tacacs                          4-70
Console(config)#tacacs-server host 10.20.30.40                       4-76
Console(config)#tacacs-server port 200                               4-76
Console(config)#tacacs-server key green                              4-77
Console#show tacacs-server                                           4-77
Server IP address: 10.20.30.40
 Communication key with tacacs server: green
 Server port number: 200
Console(config)#
```

Configuring HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface.

Command Usage

- Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for Internet Explorer 5.x or above and Netscape Navigator 6.2 or above.
- The following web browsers and operating systems currently support HTTPS:

Table 3-6 HTTPS Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 3-56.

Command Attributes

- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- **Change HTTPS Port Number** – Specifies the UDP port number used for HTTPS/SSL connection to the switch's web interface. (Default: Port 443)
- **TFTP Server IP Address** – Specifies the TFTP Server where the authorized certificate will be saved.
- **Source Certificate File Name** – File name for the certificate.
- **Source Private File Name** – Private key file name.
- **Private Password** – Password for the private key.

Web – Click Security, HTTPS Settings. Enable HTTPS and specify the port number, then click Apply. To replace the default secure-site certificate, enter the TFTP Server IP Address, the Source Certificate File Name, the Source Private File Name, and the Private Password, then click Copy Certificate.

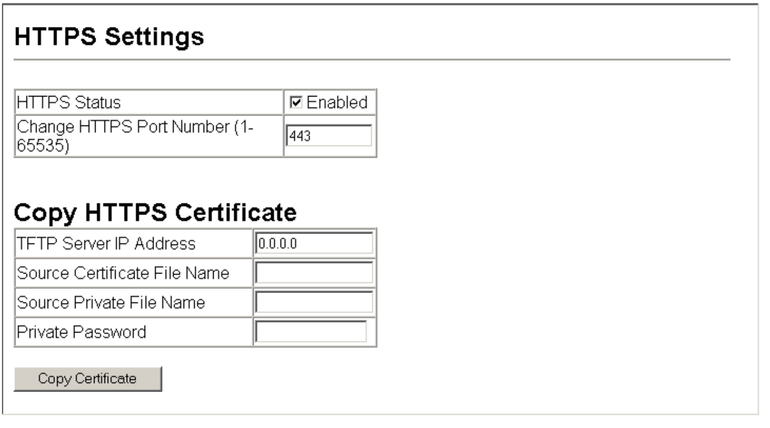


Figure 3-34. HTTPS Settings

CLI – This example enables the HTTP secure server and modifies the port number.

```
Console(config)#ip http secure-server                                        4-30
Console(config)#ip http secure-port 441                                      4-31
Console(config)#
```

Replacing the Default Secure-site Certificate

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

Note: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server, and use the following command at the switch's command-line interface to replace the default (unrecognized) certificate with an authorized one:

```
Console#copy tftp https-certificate                                          4-64
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

Note: The switch must be reset for the new certificate to be activated. To reset the switch, type: `Console#reload`

Configuring the Secure Shell

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

Notes: 1. You need to install an SSH client on the management station to access the switch for management via the SSH protocol.

2. The switch supports both SSH Version 1.5 and 2.0.

Command Usage

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified on the **Authentication Settings** page (page 3-51). If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch (SSH Host Key Settings) and enable the SSH server (Authentication Settings).

To use the SSH server, complete these steps:

1. *Generate a Host Key Pair* – On the SSH Host Key Settings page, create a host public/private key pair.

2. *Provide Host Public Key to Clients* – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

3. 10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254 15020245593199868544358361651999923329781766065830956 10825913212890233 76546801726272571413428762941301196195566782 59566410486957427888146206 5194174677298486546861571773939016477935594230357741309802273708779454 5 24083971752646358058176716709574804776117

4. *Import Client's Public Key to the Switch* – Use the **copy tftp public-key** command (page 4-64) to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch via the User Accounts page as described on page 3-50) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example:

   1024 35 1341081685609893921040944920155425347631641921872958921143173880 0555361616310517759408386863110929123222682851925437460310093718772119 9 6963178136627741416898513204911720483033925432410163799759237144901193 8 0060902539484084827178194372288402533115952134861022902978982721353267 1 3162943253281891504530639391 6643 steve@192.168.1.19

5. *Set the Optional Parameters* – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.

6. *Enable SSH Service* – On the SSH Settings page, enable the SSH server on the switch.

7. *Challenge-Response Authentication* – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access. The following exchanges take place during this process:

1. The client sends its public key to the switch.

2. The switch compares the client's public key to those stored in memory.

3. If a match is found, the switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.

4. The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.

5. The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Notes: 1. To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client’s keys.

2. The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

Configuring the SSH settings

The SSH server includes basic settings for authentication.

Field Attributes

- **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)
- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- **SSH Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1 to 120 seconds; Default: 120 seconds)
- **SSH Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process.
  (Range: 1-5 times; Default: 3)
- **SSH Server-Key Size** – Specifies the SSH server key size.
  (Range: 512-896 bits; Default:768)
  - The server key is a private key that is never shared outside the switch.

- The host key is shared with the SSH client, and is fixed at 1024 bits.

Web – Click Security, SSH, Settings. Enable SSH and adjust the authentication parameters as required, then click Apply. Note that you must first generate the host key pair on the SSH Host-Key Settings page before you can enable the SSH server.

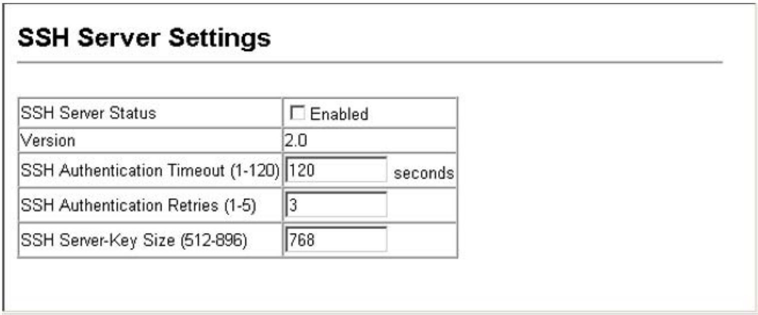


Figure 3-35. SSH Server Settings

CLI – This example enables SSH, sets the authentication parameters, and displays the current configuration. It shows that the administrator has made a connection via SHH, and then disables this connection.

```
Console(config)#ip ssh server                                      4-35
Console(config)#ip ssh timeout 100                                 4-36
Console(config)#ip ssh authentication-retries 5                    4-37
Console(config)#ip ssh server-key size 512                         4-37
Console(config)#end
Console#show ip ssh                                                4-40
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#show ssh                                                   4-40
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0    admin   2.0      cipher-3des   session-started
Console#disconnect 0                                               4-17
Console#
```

Generating the Host Key Pair

A host public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the proceeding section (Command Usage).

Field Attributes

- **Public-Key of Host-Key** – The public key for the host.
  - RSA: The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus.
  - DSA: The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.
- **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA, DSA, Both: Default: RSA)
- The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair.
- **Generate** – This button is used to generate the host key pair. Note that you must first generate the host key pair before you can enable the SSH server on the SSH Server Settings page.
- **Clear** – This button clears the host key from both volatile memory (RAM) and non-volatile memory (Flash).

Web – Click Security, SSH, Host-Key Settings. Select the host-key type from the drop-down box, select the option to save the host key from memory to flash (if required) prior to generating the key, and then click Generate.

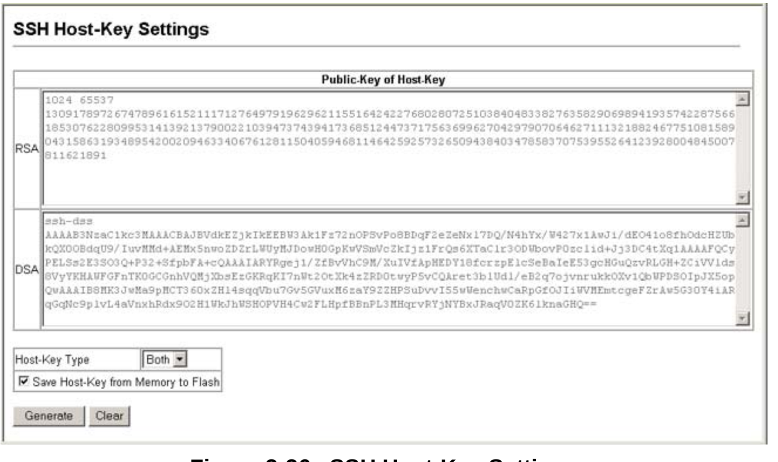


Figure 3-36. SSH Host-Key Settings

CLI – This example generates a host-key pair using both the RSA and DSA algorithms, stores the keys to flash memory, and then displays the host's public keys.

```
Console#ip ssh crypto host-key generate                              4-35
Console#ip ssh save host-key                                         4-35
Console#show public-key host                                         4-35
Host:
RSA:
1024 65537
127250922544926402131336514546131189679055192360076028653006761
8240969094744832010252487896597759216832222558465238779154647980739631403
3869257931051057652122430528078658854857892726029378660892368414232759121
2760325919683697053439336438445223335188287173896894511729290510813919642
025190932104328579045764891
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVXlME1sHL0EcE/
Re6hlasfEthIwmjhLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIICuKg6vjO
9XTs7XKc05xfzkBiKviDa+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6DkZAAAAF
QCNZn/x17dwpW8RrV DQnSWw4Qk+6QAAAIEAptkGeB6B5hwagH4g
UOCY6i1TmrmSiJgfwO9OqRPUMbCAkCC+uzxatOo7drnIZypMx+Sx5RUdMGgKS+9ywsa1cWqHe
FY5ilc3lDCNBueeLykZzVS+RS+azTKIk/zrJh8GLG Nq375R55yRxFvmcGIn
Q7IphPqyJ3o9MK8LFDfmJEAAACAL8A6tESiswP2OFqX7VGoEbzVDSOI RTMFy
3iUXtvGyQAOVSy67Mfc3lMtgqPRUOYXDiwIBp5NXgilCg5z7VqbmRm28mWc5a//f8TUAg
PNWKV6W0hqmshQdotVzDR1e+XKNTZj0uTwWfjO5Kytdn4MdoTHgrbl/DMdAfjnte8MZZs=

Console#
```

Generating the User Public Key Pair

A user public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the user public key to SSH clients and import the client's public key to the switch as described in the proceeding section (Command Usage).

Field Attributes

- **Public-Key of admin/user** – The public key for the adminstrator or user.
  - RSA: The first field indicates the size of the public key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus.
  - DSA: The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.
- User Name – The user type used for the public key pair.
- **Public-Key Type** – The key type used to generate the user public key pair (i.e., public and private keys). (Range: RSA, DSA, Both: Default: RSA)
- The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- **TFTP Server IP Address** – The TFTP server IP address location for the public key pair.
- **Source File Name** – The file name used for the public key pair.
- **Copy Public Key** – Save a copy of the public key pair.

- **Delete** – This button deletes the user public key process.

Web – Click Security, SSH, SSH User-Key Settings. Select the user type and public-key type from the drop-down box, enter the TFTP server IP address, input the source file name, and then click Copy Public Key.

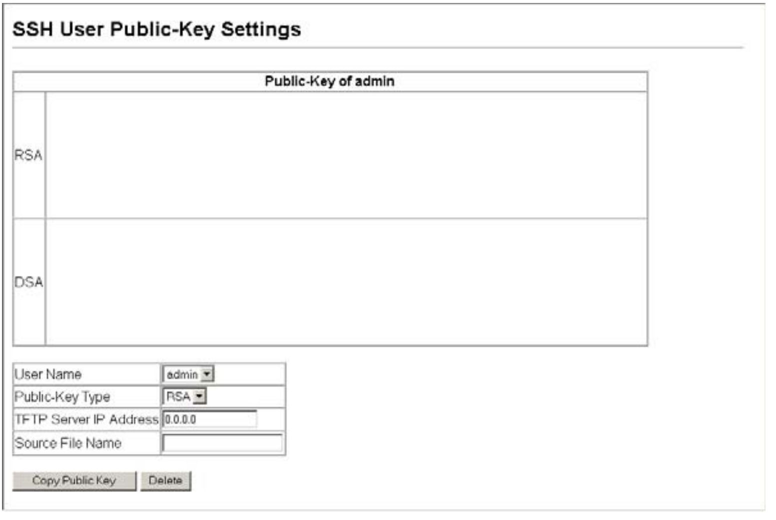


Figure 3-37. SSH User Public-Key Settings

CLI – This example generates a host-key pair using both the RSA and DSA algorithms, stores the keys to flash memory, and then displays the host's public keys.

```
Console#ip ssh crypto host-key generate                             4-35
Console#ip ssh save host-key                                        4-35
Console#show public-key host                                        4-35
Host:
RSA:
1024 65537
127250922544926402131336514546131189679055192360076028653006761
8240969094744832010252487896597759216832222558465238779154647980739631403
3869257931051057652122430528078658854857892726029378660892368414232759121
2760325919683697053439336438445223335188287173896894511729290510813919642
025190932104328579045764891
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVXlME1sHL0EcE/
Re6hlasfEthIwmjhLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIICuKg6vjO
9XTs7XKc05xfzkBiKviDa+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6DkZAAAAF
QCNZn/x17dwpW8RrV DQnSWw4Qk+6QAAAIEAptkGeB6B5hwagH4g
UOCY6i1TmrmSiJgfwO9OqRPUMbCAkCC+uzxatOo7drnIZypMx+Sx5RUdMGgKS+9ywsa1cWqHe
FY5ilc3lDCNBueeLykZzVS+RS+azTKIk/zrJh8GLG Nq375R55yRxFvmcGIn
Q7IphPqyJ3o9MK8LFDfmJEAAACAL8A6tESiswP2OFqX7VGoEbzVDSOI RTMFy
3iUXtvGyQAOVSy67Mfc3lMtgqPRUOYXDiwIBp5NXgilCg5z7VqbmRm28mWc5a//f8TUAg
PNWKV6W0hqmshQdotVzDR1e+XKNTZj0uTwWfjO5Kytdn4MdoTHgrbl/DMdAfjnte8MZZs=

Console#
```

Configuring Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port. Note that you can also restrict the maximum number of addresses that can be learned by a port.

To add new VLAN members at a later time, you can manually add secure addresses with the Static Address Table (page 3-108), or turn off port security to reenable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.

Command Usage

- A secure port has the following restrictions:
  - Cannot use port monitoring.
  - Cannot be a multi-VLAN port.
  - It cannot be used as a member of a static or dynamic trunk.
  - It should not be connected to a network interconnection device.
- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Port/Port Configuration page (Chapter).

Command Attributes

- **Port** – Port number.
- Name – Descriptive text (page 4-112).
- **Action** – Indicates the action to be taken when a port security violation is detected:
  - **None**: No action should be taken. (This is the default.)
  - **Trap**: Send an SNMP trap message.
  - **Shutdown**: Disable the port.
  - **Trap and Shutdown**: Send an SNMP trap message and disable the port.
- **Security Status** – Enables or disables port security on the port. (Default: Disabled)
- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)
- **Trunk** – Trunk number if port is a member (page 3-86 and 3-88).

Web – Click Security, Port Security. Set the action to take when an invalid address is detected on a port, set the maximum number of MAC addresses allowed on a port, and click Apply.

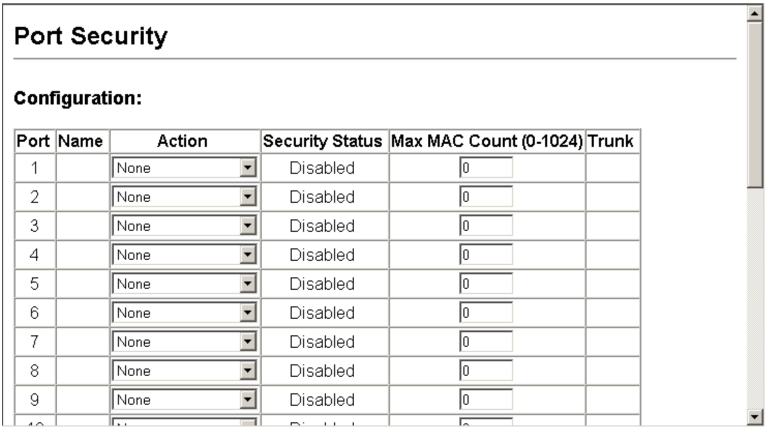


Figure 3-38. Configuring Port Security

CLI – This example sets the command mode to Port 5, sets the port security action to send a trap and disable the port, and then enables port security for the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown          4-78
Console(config-if)#port security
Console(config-if)#
```

Configuring 802.1X Port Authentication

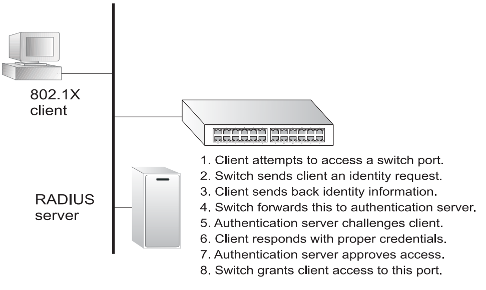
Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication.

Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The current version of the firmware supports only the MD5 authentication method.

The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.



The operation of 802.1X on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- Each switch port that will be used must be set to dot1x “Auto” mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server and 802.1X client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type. The current version of the firmware supports only the EAP-MD5 authetication type. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

Displaying 802.1X Global Settings

The 802.1X protocol provides client authentication.

Command Attributes

- **802.1X System Authentication Control** – The global setting for 802.1X.

Web – Click Security, 802.1X, Information.

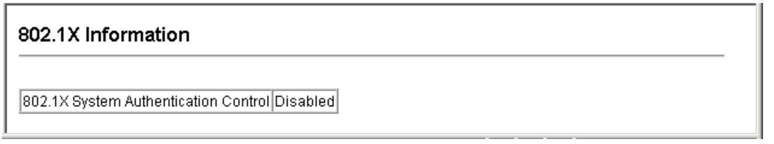


Figure 3-39. 802.1X Global Information

CLI – This example shows the default global setting for 802.1X.

```
Console#show dot1x                                                          4-85
Global 802.1X Parameters
 system-auth-control: Disabled

802.1X Port Summary

Port Name  Status         Operation Mode   Mode                   Authorized
1/1       disabled     Single-Host     ForceAuthorized n/a
1/2       disabled     Single-Host     ForceAuthorized n/a
.
.
.
802.1X Port Details

802.1X is disabled on port 1/1
.
.
.
802.1X is disabled on port 1/28
Console#
```

Configuring 802.1X Global Settings

The 802.1X protocol provides port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

Command Attributes

- **802.1X System Authentication Control** – Sets the global setting for 802.1X. (Default: Disabled)

Web – Select Security, 802.1X, Configuration. Enable dot1x globally for the switch and click Apply.

Figure 3-40. 802.1X Global Configuration

CLI – This enables 802.1X globally for the switch

```
Console(config)#dot1x system-auth-control                    4-80
Console(config)#
```

Configuring Port Settings for 802.1X

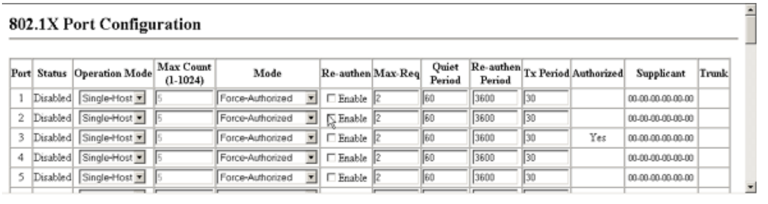
When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

Command Attributes

- **Port** – Port number.
- **Status** – Indicates if authentication is enabled or disabled on the port. (Default: Disabled)
- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Options: Single-Host, Multi-Host; Default: Single-Host)
- **Max Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-1024; Default: 5)
- **Mode** – Sets the authentication mode to one of the following options:
  - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise.
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Re-authen** – Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)
- **Max-Req** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)

- **Quiet Period** – Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Re-authen Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- **Tx Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **Authorized** –
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
  - *Blank* – Displays nothing when dot1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web – Click Security, 802.1X, Port Configuration. Modify the parameters required, and click Apply.


802.1X Port Configuration

Port	Status	Operation Mode	Max Count (1-1024)	Mode	Re-authen	Max-Req	Quiet Period	Re-authen Period	Tx Period	Authorized	Supplicant	Trunk
1	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
2	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
3	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30	Yes	00-00-00-00-00-00	
4	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
5	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	

Figure 3-41. 802.1X Port Configuration

CLI – This example sets the 802.1X parameters on port 2. For a description of the additional fields displayed in this example, see “show dot1x” on page 4-85.

```
Console(config)#interface ethernet 1/2                                  4-111
Console(config-if)#dot1x port-control auto                              4-81
Console(config-if)#dot1x re-authentication                              4-83
Console(config-if)#dot1x max-req 5                                      4-81
Console(config-if)#dot1x timeout quiet-period 30                        4-83
Console(config-if)#dot1x timeout re-authperiod 1800                     4-84
Console(config-if)#dot1x timeout tx-period 40                           4-84
Console(config-if)#exit
Console(config)#exit
Console#show dot1x                                                      4-85
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status        Operation Mode   Mode                  Authorized
1/1       disabled     Single-Host     ForceAuthorized n/a
1/2       enabled      Single-Host     auto            yes
.
.
.
1/28      disabled     Single-Host     ForceAuthorized n/a

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
 reauth-enabled: Enable
 reauth-period:  1800
 quiet-period:   30
 tx-period:      40
 supplicant-timeout:   30
 server-timeout: 10
 reauth-max:     2
 max-req:        5
Status              Authorized
Operation mode      Single-Host
Max count           5
Port-control        Auto
Supplicant          00-12-CF-49-5e-dc
Current Identifier  3

Authenticator State Machine
State               Authenticated
Reauth Count        0

Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  2

Reauthentication State Machine
State               Initialize
.
.
.
802.1X is disabled on port 1/28
Console#
```

Displaying 802.1X Statistics

This switch can display statistics for dot1x protocol exchanges for any port.

Statistical Values

Table 3-7 802.1X Statistics

Parameter	Descripton
Rx EXPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Web – Select Security, 802.1X, Statistics. Select the required port and then click Query. Click Refresh to update the statistics.

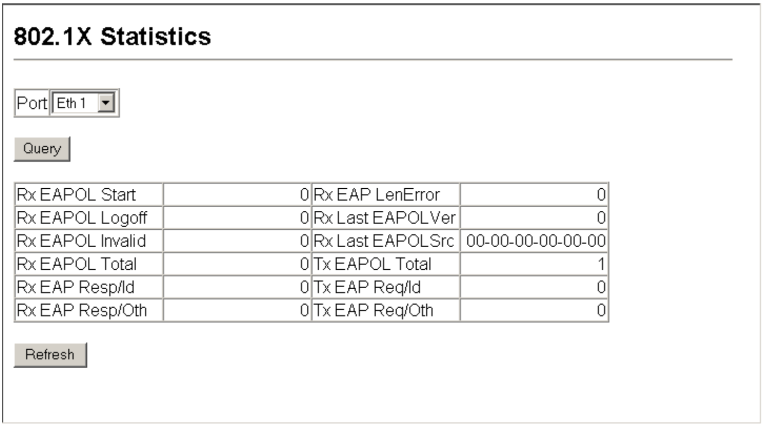


Figure 3-42. Displaying 802.1X Port Statistics

CLI – This example displays the 802.1X statistics for port 4.

```
Console#show dot1x statistics interface ethernet 1/4               4-85

Eth 1/4
Rx: EXPOL      EAPOL      EAPOL      EAPOL        EAP        EAP       EAP
    Start      Logoff     Invalid    Total      Resp/Id   Resp/Oth  LenError
        2          0          0       1007       672         0         0

    Last        Last
EAPOLVer     EAPOLSrc
       1     00-00-E8-98-73-21

Tx: EAPOL       EAP       EAP
    Total      Req/Id    Req/Oth
     2017      1005         0
Console#
```

Access Control Lists

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

Configuring Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

Command Usage

The following restrictions apply to ACLs:

- Each ACL can have up to 60 rules.
- This switch supports ACLs for ingress filtering only. However, you can only bind one IP ACL to any port for ingress filtering. In other words, only one ACL can be bound to an interface - Ingress IP ACL.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Ingress IP ACL for ingress ports.
2. Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
3. If no explicit rule is matched, the implicit default is permit all.

Setting the ACL Name and Type

Use the ACL Configuration page to designate the name and type of an ACL.

Command Attributes

- **Name** – Name of the ACL. (Maximum length: 16 characters)
- **Type** – There are three filtering modes:
  - Standard: IP ACL mode that filters packets based on the source IP address.
  - Extended: IP ACL mode that filters packets based on source or destination IP address, as well as protocol type and protocol port number.
  - MAC: MAC ACL mode that filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Web – Click Security, ACL, Configuration. Enter an ACL name in the Name field, select the list type (IP Standard, IP Extended, or MAC), and click Add to open the configuration page for the new list.

Figure 3-43. Naming and Choosing ACLs

CLI – This example creates a standard IP ACL named bill.

```
Console(config)#access-list ip standard bill                         4-89
Console(config-std-acl)#
```

Configuring a Standard IP ACL

Command Attributes

- **Action** – An ACL can contain all permit rules or all deny rules. (Default: Permit rules)
- **Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **IP Address** – Source IP address.
- **Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Web – Specify the action (i.e., Permit or Deny). Select the address type (Any, Host, or IP). If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range. Then click Add.

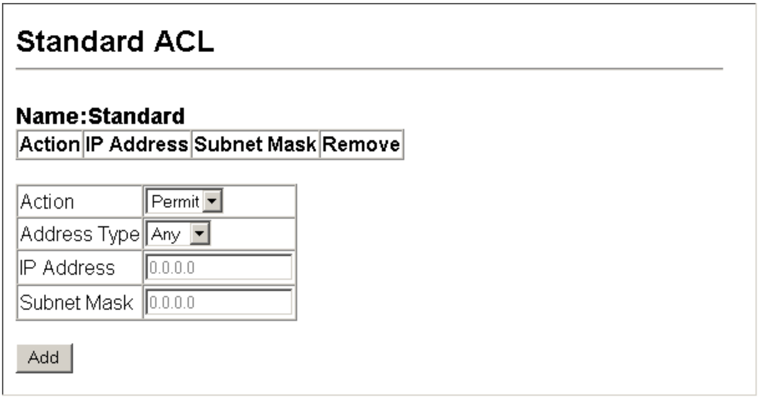


Figure 3-44. Configuring Standard IP ACLs

CLI – This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21                    4-90
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Configuring an Extended IP ACL

Command Attributes

- **Action** – An ACL can contain either all permit rules or all deny rules. (Default: Permit rules)
- **Src/Dst Address Type** – Specifies the source or destination IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **Src/Dst IP Address** – Source or destination IP address.
- **Src/Dst Subnet Mask** – Subnet mask for source or destination address. (See the description for SubMask on page 3-73.)
- **Service Type** – Packet priority settings based on the following criteria:
  - **Precedence** – IP precedence level. (Range: 0-7)
  - **TOS** – Type of Service level. (Range: 0-15)
  - **DSCP** – DSCP priority level. (Range: 0-64)

- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)
- **Src/Dst Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- **Src/Dst Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Code Bit Mask** – Decimal number representing the code bits to match.

The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit.

The following bits may be specified:

- 1 (fin) – Finish
- 2 (syn) – Synchronize
- 4 (rst) – Reset
- 8 (psh) – Push
- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use control-code 2, control bitmask 2
- Both SYN and ACK valid, use control-code 18, control bitmask 18
- SYN valid and ACK invalid, use control-code 2, control bitmask 18

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or IP). If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range. Set any other required criteria, such as service type, protocol type, or TCP control code. Then click Add.

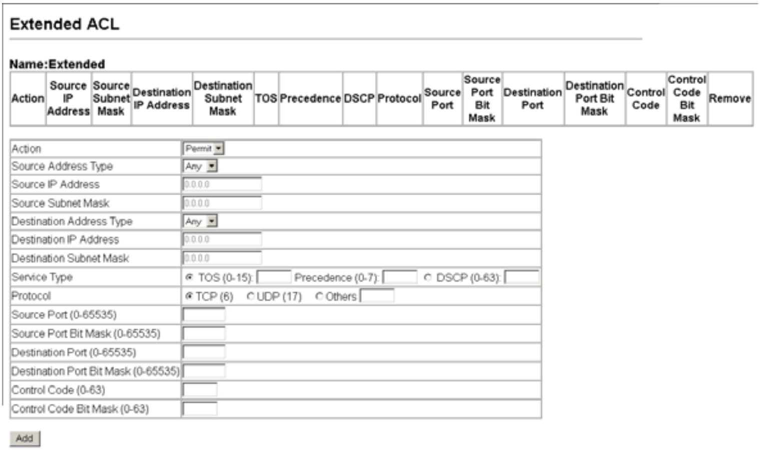


Figure 3-45. Configuring Extended IP ACLs

CLI – This example adds three rules:

1. Accept any incoming packets if the source address is in subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

2. Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

3. Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any          4-91
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any dport 80
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any tcp
control-code 2 2
Console(config-std-acl)#
```

Configuring a MAC ACL

Command Attributes

- **Action** – An ACL can contain permit rules, deny rules, or a combination of both. (Default: Permit rules)
- **Source/Destination Address Type** – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Bitmask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination Bit Mask** – Hexidecimal mask for source or destination MAC address.
- **VID** – VLAN ID. (Range: 1-4095)
- **VID Bit Mask** – VLAN bitmask. (Range: 1-4095)
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-fff hex.)

A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

- **Ethernet Type Bit Mask** – Protocol bitmask. (Range: 600-fff hex.)
- **Packet Format** – This attribute includes the following packet types:
  - Any – Any Ethernet packet type.
  - Untagged-eth2 – Untagged Ethernet II packets.
  - Untagged-802.3 – Untagged Ethernet 802.3 packets.
  - Tagged-eth2 – Tagged Ethernet II packets.
  - Tagged-802.3 – Tagged Ethernet 802.3 packets.

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or MAC). If you select "Host," enter a specific address (e.g., 11-22-33-44-55-66). If you select "MAC," enter a base address and a hexidecimal bitmask for an address range. Set any other required criteria, such as VID, Ethernet type, or packet format. Then click Add.

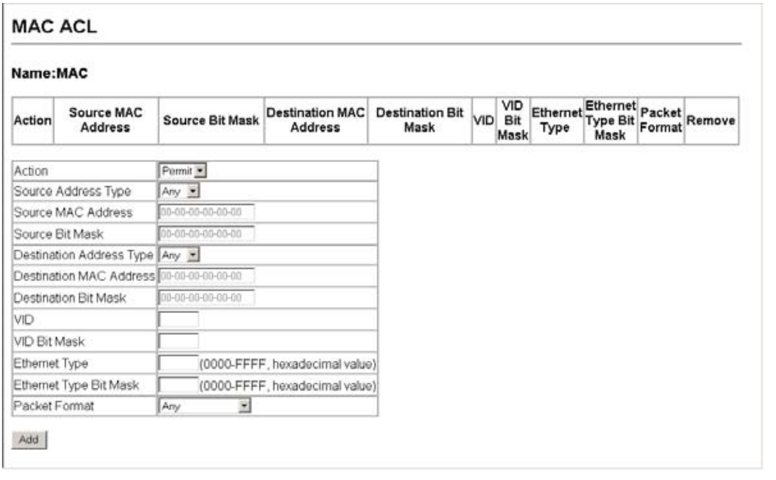


Figure 3-46. Configuring MAC ACLs

CLI – This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype
0800241
Console(config-mac-acl)#
```

Binding a Port to an Access Control List

After configuring the Access Control Lists (ACL), you can bind the ports that need to filter traffic to the appropriate ACLs. You can assign one IP access list to any port.

Command Usage

- Each ACL can have up to 60 rules.
- This switch supports ACLs for ingress filtering only. However, you can only bind one IP or MAC ACL to any port for ingress filtering. In other words, only one ACL can be bound to an interface - Ingress IP or MAC ACL.

Command Attributes

- Port – Fixed port or SFP module. (Range: 1-28)
- **IP** – Specifies the IP ACL to bind to a port.
- **MAC** – Specifies the MAC ACL to bind to a port.

- **IN** – ACL for ingress packets.
- *ACL Name* – Name of the ACL.

Web – Click Security, ACL, Port Binding. Mark the Enable field for the port you want to bind to an ACL for ingress traffic, select the required ACL from the drop-down list, then click Apply.

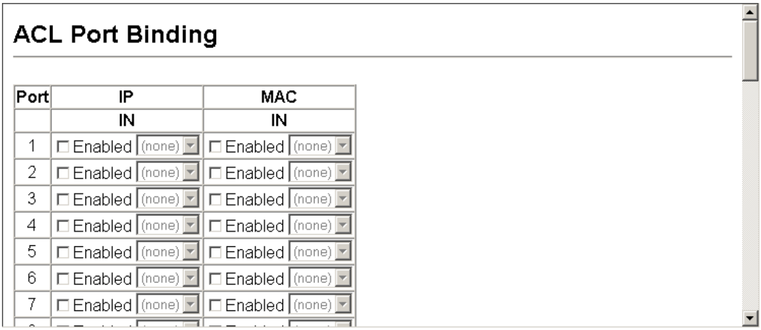


Figure 3-47. Mapping ACLs to Port Ingress Queues

CLI – This examples assigns an IP access list to port 1, and an IP access list to port 2.

```
Console(config)#interface ethernet 1/1                           4-111
Console(config-if)#ip access-group david in                      4-92
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

Filtering Management Access

You can specify the client IP addresses that are allowed management access to the switch through the web interface, SNMP, or Telnet.

Command Usage

- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.

- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Command Attributes

- **Web IP Filter** – Configures IP address(es) for the web group.
- **SNMP IP Filter** – Configures IP address(es) for the SNMP group.
- **Telnet IP Filter** – Configures IP address(es) for the Telnet group.
- **IP Filter List** – IP address which are allowed management access to this interface.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – The end address of a range.
- **Add/Remove Filtering Entry** – Adds/removes an IP address from the list.

Web – Click Security, IP Filter. Enter the addresses that are allowed management access to an interface, and click Add IP Filtering Entry.

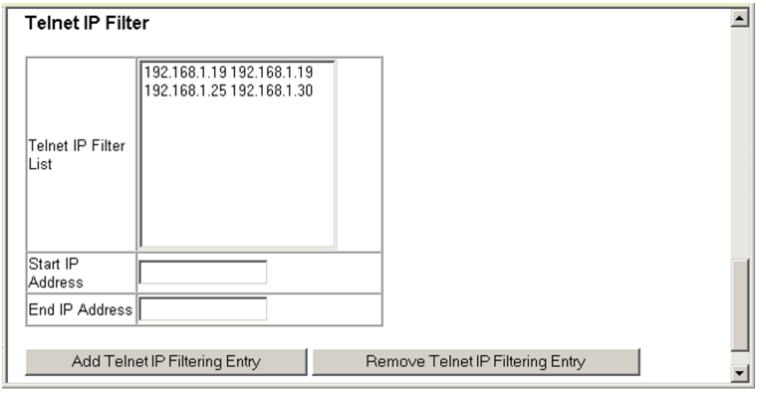


Figure 3-48. Filtering Management Access

CLI – This example restricts management access for Telnet clients.

```
Console(config)#management telnet-client 192.168.1.19             4-27
Console(config)#management telnet-client 192.168.1.25 192.168.1.30
Console#
```

Port Configuration

Displaying Connection Status

You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Field Attributes (Web)

- **Name** – Interface label.
- **Type** – Indicates the port type.
- (1000BASE-T, 1000BASE-SX, 1000BASE-LX or 100BASE-FX)
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- **Speed Duplex Status** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Flow Control Status** – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or None)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Media Type**[1] – Indicates the type of media used for ports 25 to 26.
- **Trunk Member**[1] – Shows if port is a trunk member.
- **Creation**[2] – Shows if a trunk is manually configured or dynamically set via LACP.

1: Port Information only.
2: Trunk Information only

Web – Click Port, Port Information or Trunk Information.

Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Media Type	Trunk Member
1		100Base-TX	Enabled	Down	10half	None	Enabled	None	
2		100Base-TX	Enabled	Down	10half	None	Enabled	None	
3		100Base-TX	Enabled	Up	100full	None	Enabled	None	
4		100Base-TX	Enabled	Down	10half	None	Enabled	None	
5		100Base-TX	Enabled	Down	10half	None	Enabled	None	
6		100Base-TX	Enabled	Down	10half	None	Enabled	None	
7		100Base-TX	Enabled	Down	10half	None	Enabled	None	
8		100Base-TX	Enabled	Down	10half	None	Enabled	None	
9		100Base-TX	Enabled	Down	10half	None	Enabled	None	
10		100Base-TX	Enabled	Down	10half	None	Enabled	None	
11		100Base-TX	Enabled	Down	10half	None	Enabled	None	
12		100Base-TX	Enabled	Down	10half	None	Enabled	None	
13		100Base-TX	Enabled	Down	10half	None	Enabled	None	
14		100Base-TX	Enabled	Down	10half	None	Enabled	None	
15		100Base-TX	Enabled	Down	10half	None	Enabled	None	
16		100Base-TX	Enabled	Down	10half	None	Enabled	None	
17		100Base-TX	Enabled	Down	10half	None	Enabled	None	

Figure 3-49. Port Status Information

Field Attributes (CLI)

Basic information:

- **Port type** – Indicates the port type.
- (1000BASE-T, 1000BASE-SX, 1000BASE-LX or 100BASE-FX)
- **MAC address** – The physical layer address for this port. (To access this item on the web, see “Setting the Switch’s IP Address” on page 3-14.)

Configuration:

- **Name** – Interface label.
- **Port admin** – Shows if the interface is enabled or disabled (i.e., up or down).
- **Speed-duplex** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Capabilities** – Specifies the capabilities to be advertised for a port during auto-negotiation. (To access this item on the web, see “Configuring Interface Connections” on page 3-48.) The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation
  - **Sym** - Transmits and receives pause frames for flow control
  - **FC** - Supports flow control
- **Broadcast storm** – Shows if broadcast storm control is enabled or disabled.
- Broadcast storm limit – Shows the broadcast storm threshold.
  (240 - 1488100 packets per second)
- **Flow control** – Shows if flow control is enabled or disabled.
- **LACP** – Shows if LACP is enabled or disabled.
- **Port Security** – Shows if port security is enabled or disabled.
- **Max MAC count** – Shows the maximum number of MAC address that can be learned by a port. (0 - 1024 addresses)
- **Port security action** – Shows the response to take when a security violation is detected. (shutdown, trap, trap-and-shutdown)

Current status:

- **Link Status** – Indicates if the link is up or down.
- Port Operation Status – Provides detailed information on port state. (Displayed only when the link is up.)
- **Operation speed-duplex** – Shows the current speed and duplex mode.
- **Flow control type** – Indicates the type of flow control currently in use.

(IEEE 802.3x, Back-Pressure or none)

CLI – This example shows the connection status for Port 5.

```
Console#show interfaces status ethernet 1/5                              4-117
Information of Eth 1/5
 Basic information:
  Port type: 100TX
  Mac address: 00-30-f1-47-58-46
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full
  Broadcast storm: Enabled
  Broadcast storm limit: 500 packets/second
  Flow control: Disabled
  Lacp: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
 Current status:
  Link status: Down
  Operation speed-duplex: 100full
  Flow control type: None
Console#
```

Configuring Interface Connections

You can use the Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

Command Attributes

- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode.
- **Flow Control** – Allows automatic or manual selection of flow control.
- **Autonegotiation (Port Capabilities)** – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control. The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation
  - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames.

(*The current switch chip only supports symmetric pause frames.*)

- **FC** - Supports flow control
- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)
- (Default: Autonegotiation enabled; Advertised capabilities for 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; 1000BASE-SX/LX/LH – 1000full)

- **Media Type** – Select the type of media to us for ports 25 to 26. (Options: Copper-Forced, SFP-Forced, SFP-Preferred-Auto; Default: SFP-Preferred-Auto)
- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see “Creating Trunk Groups” on page 3-85.

Note: Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.

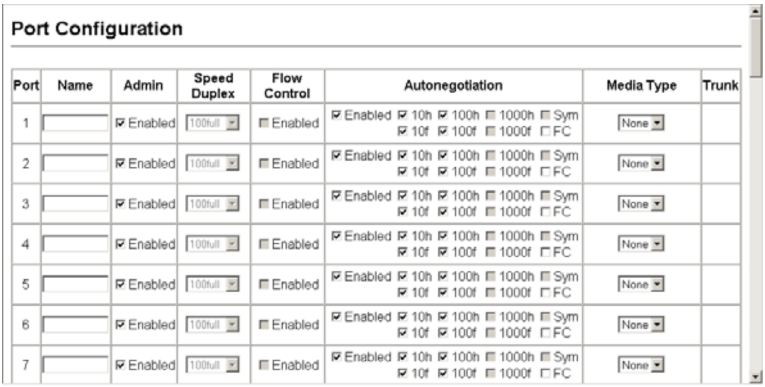


Figure 3-50. Configuring Port Attributes

CLI – Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13                          4-111
Console(config-if)#description RD SW#13                          4-112
Console(config-if)#shutdown                                      4-116
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                                4-113
Console(config-if)#speed-duplex 100half                          4-112
Console(config-if)#flowcontrol                                   4-115
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                          4-114
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
```

Creating Trunk Groups

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to 8 trunks at a time.

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

Command Usage

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

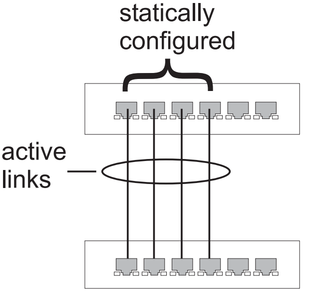
- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to 8 trunks on the switch, with up to eight ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.

- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

Statically Configuring a Trunk

Command Usage

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



Command Attributes

- **Member List** (Current) – Shows configured trunks (Trunk ID, Unit, Port).
- **New** – Includes entry fields for creating new trunks.
  - **Trunk** – Trunk identifier. (Range: 1-8)
  - **Port** – Port identifier. (Range: 1-28)

Web – Click Port, Trunk Membership. Enter a trunk ID in the Trunk field, select any of the switch ports from the scroll-down port list, and click Add. After you have completed adding ports to the member list, click Apply.

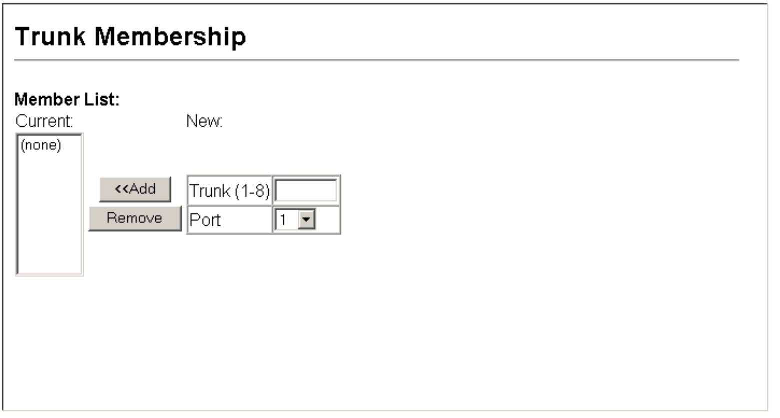


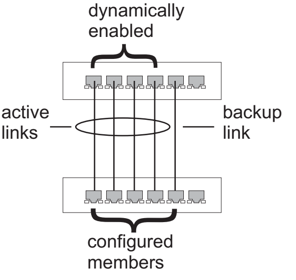
Figure 3-51. Static Trunk Configuration

CLI – This example creates trunk 2 with ports 1 and 2. Just connect these ports to two static trunk ports on another switch to form a trunk.

```
Console(config)#interface port-channel 2                                  4-111
Console(config-if)#exit
Console(config)#interface ethernet 1/1                                    4-111
Console(config-if)#channel-group 1                                        4-126
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1                             4-117
Information of Trunk 1
 Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-AA-AA-01
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
 Current status:
  Created by: User
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/1, Eth1/2,
Console#
```

Enabling LACP on Selected Ports

Command Usage



- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, and auto-negotiation.

Command Attributes

- **Member List** (Current) – Shows configured trunks (Port).
- **New** – Includes entry fields for creating new trunks.
  - **Port** – Port identifier. (Range: 1-28)

Web – Click Port, LACP, Configuration. Select any of the switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click Apply.

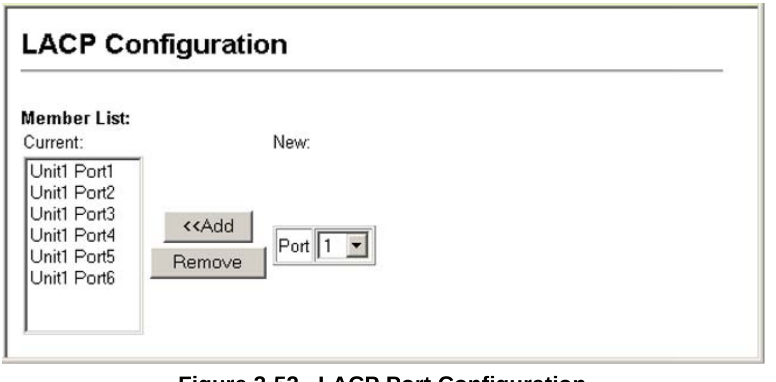


Figure 3-52. LACP Port Configuration

CLI – The following example enables LACP for ports 1 to 6. Just connect these ports to LACP-enabled trunk ports on another switch to form a trunk.

```
Console(config)#interface ethernet 1/1                                       4-111
Console(config-if)#lacp                                                      4-127
Console(config-if)#exit
.
.
.
Console(config)#interface ethernet 1/6
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                                4-117
Information of Trunk 1
 Basic information:
  Port type: 1000T
  Mac address: 22-22-22-22-22-2d
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
  Port security: Disabled
  Max MAC count: 0
  Port security action: None
 Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6,
Console#
```

Configuring LACP Parameters

Dynamically Creating a Port Channel

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP System Priority.
- Ports must have the same LACP port Admin Key.
- However, if the “port channel” Admin Key is set (page 4-142), then the port Admin Key must be set to the same value for a port to be allowed to join a channel group.

Note: If the port channel admin key (lacp admin key, page 4-130) is not set (through the CLI) when a channel group is formed (i.e., it has a null value of 0), this key is set to the same value as the port admin key used by the interfaces that joined the group (lacp admin key, as described in this section and on page 4-129).

Command Attributes

Set Port Actor – This menu sets the local side of an aggregate link; i.e., the ports on this switch.

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

- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations.
  (Range: 0-65535; Default: 32768)
  - Ports must be configured with the same system priority to join the same LAG.
  - System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG.
  (Range: 0-65535; Default: 1)
- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

Set Port Partner – This menu sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor. However, configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Web – Click Port, LACP, Aggregation Port. Set the System Priority, Admin Key, and Port Priority for the Port Actor. You can optionally configure these settings for the Port Partner. (Be aware that these settings only affect the administrative state of the partner, and will not take effect until the next time an aggregate link is formed with this device.) After you have completed setting the port LACP parameters, click Apply.

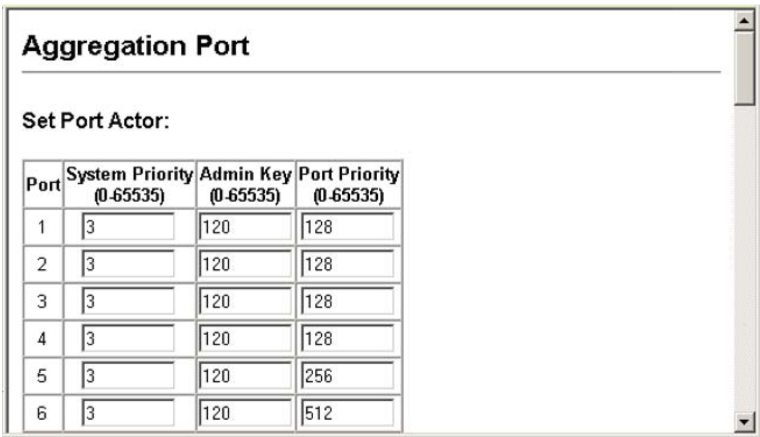


Figure 3-53. LACP Aggregation Port Configuration

CLI – The following example configures LACP parameters for ports 1-6. Ports 1-4 are used as active members of the LAG; ports 5 and 6 are set to backup mode.

```
Console(config)#interface ethernet 1/1                                   4-111
Console(config-if)#lacp actor system-priority 3                          4-128
Console(config-if)#lacp actor admin-key 120                              4-129
Console(config-if)#lacp actor port-priority 128                          4-131
Console(config-if)#exit
.
.
.
Console(config)#interface ethernet 1/6
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 512
Console(config-if)#end
Console#sh lacp sysid                                                    4-131
Channel Group    System Priority    System MAC Address
-------------------------------------------------------------------
            1               32768     00-00-E9-31-31-31
            2               32768     00-00-E9-31-31-31
            3               32768     00-00-E9-31-31-31
            4               32768     00-00-E9-31-31-31
            5               32768     00-00-E9-31-31-31
            6               32768     00-00-E9-31-31-31
Console#show lacp 1 internal                                             4-131
Channel group : 1
-------------------------------------------------------------------
Oper Key : 120
Admin Key : 120
Console#
```

Displaying LACP Port Counters

You can display statistics for LACP protocol messages.

Counter Information

Table 3-8 LACP Port Counter Information

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Receive	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Receive	Number of valid Marker PDUs received by this channel group.
Marker Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Marker Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

Web – Click Port, LACP, Port Counters Information. Select an interface port to display the corresponding information.

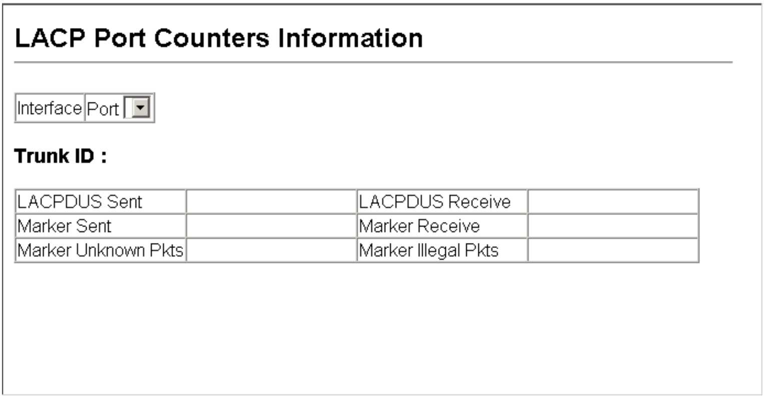


Figure 3-54. Displaying LACP Port Counters Information

CLI – The following example displays LACP counters for port channel 1.

```
Console#show 1 lacp counters                                          4-131
Channel group : 1
-------------------------------------------------------------------
Eth 1/ 1
-------------------------------------------------------------------
  LACPDUs Sent : 21
  LACPDUs Received : 21
  Marker Sent : 0
  Marker Received : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
.
.
.
Console#
```

Displaying LACP Settings and Status for the Local Side

You can display configuration settings and the operational state for the local side of an link aggregation.

Internal Configuration Information

Table 3-9 LACP Settings

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Interval	Number of seconds before invalidating received LACPDU information.

Table 3-9 LACP Settings

Field	Description
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor’s state parameters: Expired – The actor’s receive machine is in the expired state; Defaulted – The actor’s receive machine is using defaulted operational partner information, administratively configured for the partner. Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

Web – Click Port, LACP, Port Internal Information. Select a port channel to display the corresponding information.

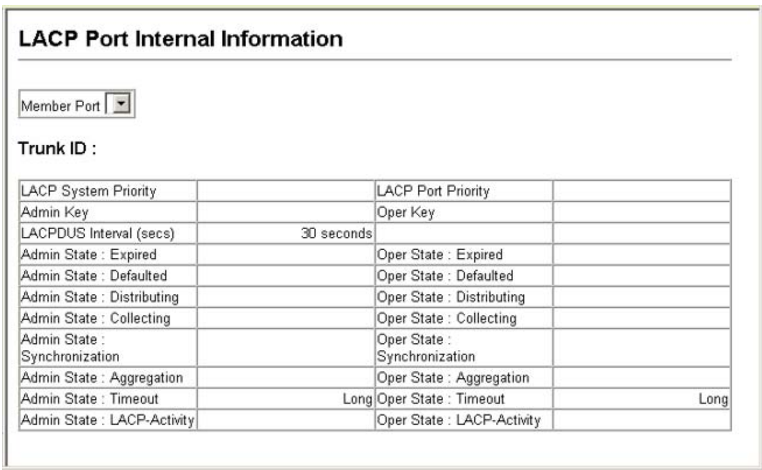


Figure 3-55. Displaying LACP Port Information

CLI – The following example displays the LACP configuration settings and operational state for the local side of port channel 1.

```
Console#show 1 lacp internal                                        4-131
Channel group : 1
-------------------------------------------------------------------
Oper Key : 4
Admin Key : 0
Eth 1/1
-------------------------------------------------------------------
  LACPDUs Internal : 30 sec
  LACP System Priority : 32768
  LACP Port Priority : 32768
  Admin Key : 4
  Oper Key : 4
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State : distributing, collecting, synchronization, aggregation,
               long timeout, LACP-activity
.
.
.
Console#
```

Displaying LACP Settings and Status for the Remote Side

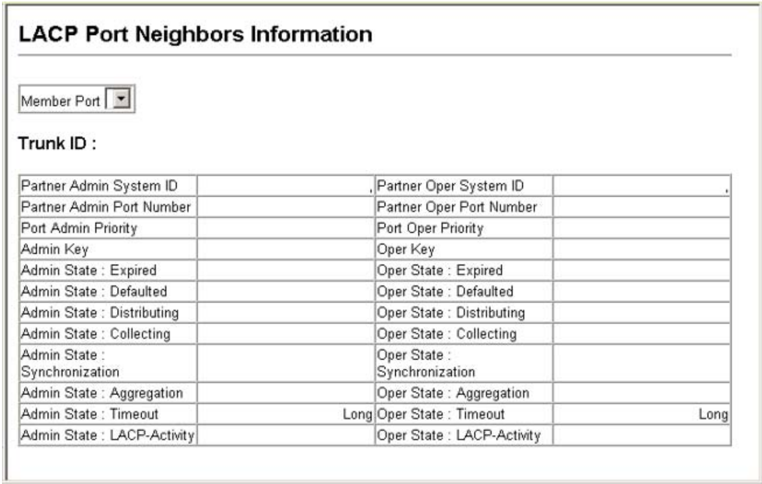
You can display configuration settings and the operational state for the remote side of an link aggregation.

Neighbor Configuration Information

Table 3-10 LACP Remote Side Settings

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

Web – Click Port, LACP, Port Neighbors Information. Select a port channel to display the corresponding information.



LACP Port Neighbors Information

Member Port

Trunk ID :

Partner Admin System ID	,	Partner Oper System ID	,
Partner Admin Port Number		Partner Oper Port Number	
Port Admin Priority		Port Oper Priority	
Admin Key		Oper Key	
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted		Oper State : Defaulted	
Admin State : Distributing		Oper State : Distributing	
Admin State : Collecting		Oper State : Collecting	
Admin State : Synchronization		Oper State : Synchronization	
Admin State : Aggregation		Oper State : Aggregation	
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	

Figure 3-56. Displaying Remote LACP Port Information

CLI – The following example displays the LACP configuration settings and operational state for the remote side of port channel 1.

```
Console#show 1 lacp neighbors                                      4-131
Channel group 1 neighbors
-------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------
  Partner Admin System ID : 32768, 00-00-00-00-00-00
  Partner Oper System ID : 32768, 00-00-00-00-00-01
  Partner Admin Port Number : 1
  Partner Oper Port Number : 1
  Port Admin Priority : 32768
  Port Oper Priority : 32768
  Admin Key : 0
  Oper Key : 4
  Admin State : defaulted, distributing, collecting, synchronization,
               long timeout,
  Oper State : distributing, collecting, synchronization, aggregation,
long timeout, LACP-activity
.
.
.
Console#
```

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

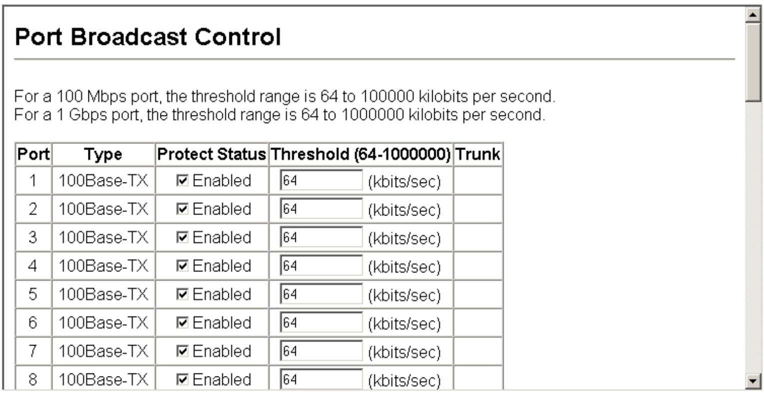
Command Usage

- Broadcast Storm Control is enabled by default.
- Broadcast control does not effect IP multicast traffic.
- The specified threshold applies to each individual port on the switch.

Command Attributes

- Port – Port number.
- Type – Indicates the port type. (100BASE-TX, 1000BASE-T, or SFP)
- **Protect Status** – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)
- **Threshold** – Threshold as percentage of port bandwidth. (Options: 64-1000000 packets per second; Default: 64 packets per second)
- **Trunk** – Shows if a port is a trunk member.

Web – Click Port, Port Broadcast Control or Trunk Broadcast Control. Set the threshold for each port, click **Apply**.



Port Broadcast Control

For a 100 Mbps port, the threshold range is 64 to 100000 kilobits per second.
For a 1 Gbps port, the threshold range is 64 to 1000000 kilobits per second.

Port	Type	Protect Status	Threshold (64-1000000)	Trunk
1	100Base-TX	☑ Enabled	64 (kbits/sec)	
2	100Base-TX	☑ Enabled	64 (kbits/sec)	
3	100Base-TX	☑ Enabled	64 (kbits/sec)	
4	100Base-TX	☑ Enabled	64 (kbits/sec)	
5	100Base-TX	☑ Enabled	64 (kbits/sec)	
6	100Base-TX	☑ Enabled	64 (kbits/sec)	
7	100Base-TX	☑ Enabled	64 (kbits/sec)	
8	100Base-TX	☑ Enabled	64 (kbits/sec)	

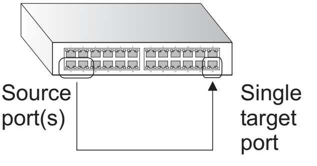
Figure 3-57. Enabling Port Broadcast Control

CLI – Specify any interface, and then enter the threshold. The following disables broadcast storm control for port 1, and then sets broadcast suppression at 500 packets per second for port 2.

```
Console(config)#interface ethernet 1/1                                    4-111
Console(config-if)#no switchport broadcast                                4-121
Console(config-if)#exit
Console(config)#broadcast packet-rate 500                                 4-121
Console(config)#exit
Console#show interfaces switchport ethernet 1/2                           4-119
Information of Eth 1/2
 Broadcast threshold: Enabled, 500 packets/second
 Lacp status: Disabled
 Ingress rate limit: disable,1000M bits per second
 Egress rate limit: disable,1000M bits per second
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
 Private-VLAN Mode:              NONE
 Private-VLAN host-association: NONE
 Private-VLAN Mapping:           NONE
Console#
```

Configuring Port Mirroring

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



Command Usage

- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Port** – The port whose traffic will be monitored. (Range: 1-28)
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)
- **Target Port** – The port that will “duplicate” or “mirror” the traffic on the source port. (Range: 1-28)

Web – Click Port, Mirror Port Configuration. Specify the source port, the traffic type to be mirrored, and the monitor port, then click **Add**.

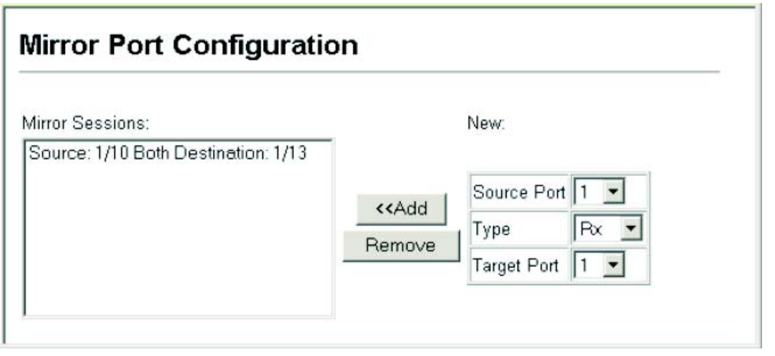


Figure 3-58. Configuring a Mirror Port

CLI – Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/10                      4-111
Console(config-if)#port monitor ethernet 1/13                4-122
Console(config-if)#
```

Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic coming into the switch. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Rate Limit Configuration

Use the rate limit configuration pages to apply rate limiting.

Command Usage

- Input and output rate limits can be enabled or disabled for individual interfaces.

Command Attribute

- **Port/Trunk** – Display the port number.
- **Input/Output Rate Limit Status**– Enables or disables the rate limit (Default: Enabled)

- **Input/Output Rate Limit Level** - Sets the rate limit level.

Web - Click Port, Rate Limit, Input/Output Port/Trunk Configuration. Enable the Rate Limit Status for the required interfaces, set the Rate Limit Level, and click Apply.

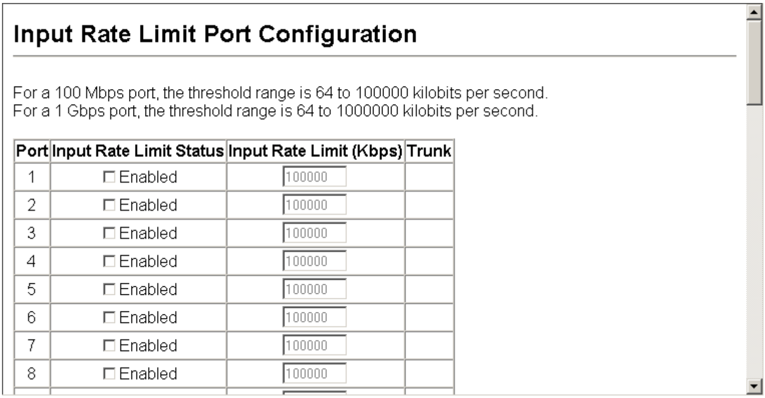


Figure 3-59. Configuring Input Port Rate Limiting

CLI - This example sets the rate limit for input traffic passing through port 3.

```
Console(config)#interface ethernet 1/3                                4-111
Console(config-if)#rate-limit input 25                                4-124
Console(config-if)#
```

Showing Port Statistics

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

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as SMC EliteView or HP OpenView.

Statistical Values

Table 3-11 Port Statistics

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
Etherlike Statistics	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.

Table 3-11 Port Statistics (Continued)

Parameter	Description
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

Table 3-11 Port Statistics (Continued)

Parameter	Description
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Web – Click Port, Port Statistics. Select the required interface, and click Query. You can also use the Refresh button at the bottom of the page to update the screen.

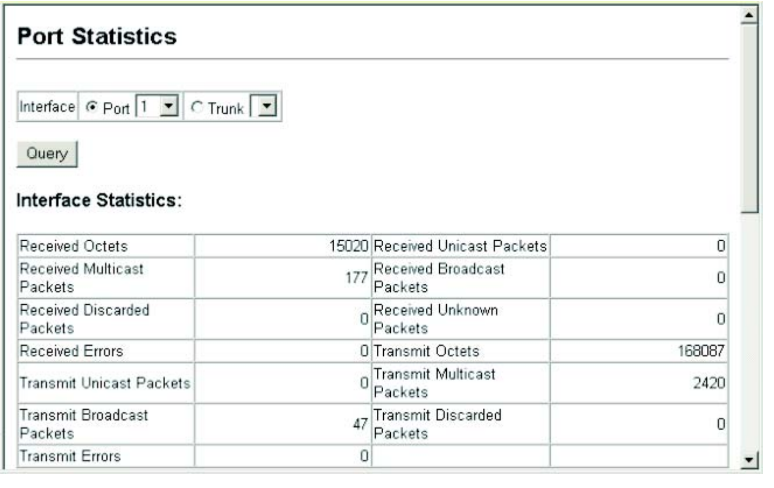


Figure 3-60. Displaying Port Statistics

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	188155	Collisions	0
Received Frames	0	64 Bytes Frames	2249
Broadcast Frames	47	65-127 Bytes Frames	459
Multicast Frames	2672	128-255 Bytes Frames	11
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

Refresh

Figure 3-61. Displaying Etherlike and RMON Statistics

CLI – This example shows statistics for port 13.

```
Console#show interfaces counters ethernet 1/13                          4-118
Ethernet 1/13
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets:
1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets:
871
```

Power over Ethernet Settings

This switch can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. Once configured to supply power, an automatic detection process is initialized by the switch that is authenticated by a PoE signature from the connected device. Detection and authentication prevent damage to non-802.3af compliant devices.

The switch's power management enables total switch power and individual port power to be controlled within a configured power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its allocated power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

Ports can be set to one of three power priority levels, critical, high, or low. To control the power supply within the switch's budget, ports set at critical or high priority have power enabled in preference to those ports set at low priority. For example, when a device is connected to a port set to critical priority, the switch supplies the required power, if necessary by dropping power to ports set for a lower priority. If power is dropped to some low-priority ports and later the power demands on the switch fall back within its budget, the dropped power is automatically restored.

Switch Power Status

Displays the Power over Ethernet parameters for the switch.

Command Attributes

- **Maximum Available Power** – The configured power budget for the switch.
- **System Operation Status** – The PoE power service provided to the switch ports.
- **Mainpower Consumption** – The amount of power being consumed by PoE devices connected to the switch.
- **Thermal Temperature**[2] – The internal temperature of the switch.
- **Software Version** – The version of software running on the PoE controller subsystem in the switch.

Web – Click PoE, Power Status.

Mainpower Status

Maximum Available Power	180 watts
System Operation Status	on
Mainpower Consumption	0 watts
Thermal Temperature	(in Celsius)
Software Version	Version 0x0122, Build 0x0E

Figure 3-62 Displaying the Global PoE Status

CLI – This example displays the current power status for the switch.

```
Console#show power mainpower                                              4-75
Unit 1 Mainpower Status
 Maximum Available Power : 180 watts
 System Operation Status : on
 Mainpower Consumption   : 0 watts
 Software Version        : Version 0x1B64, Build 0x07
Console#
```

2. This parameter is not supported for the current hardware.

Setting a Switch Power Budget

A maximum PoE power budget for the switch (power available to all switch ports) can be defined so that power can be centrally managed, preventing overload conditions at the power source. If the power demand from devices connected to the switch exceeds the power budget setting, the switch uses port power priority settings to limit the supplied power.

Command Attributes

Power Allocation – The power budget for the switch. If devices connected to the switch require more power than the switch budget, the port power priority settings are used to control the supplied power. (Range: 37 - 180 watts; Default: 180 Watts)

Web – Click PoE, Power Config. Specify the desired power budget for the switch. Click Apply.

Figure 3-63 Setting the Switch Power Budget

CLI – Use the **power mainpower maximum allocation** command to set the PoE power budget for the switch.

```
Console(config)#power mainpower maximum allocation 180              4-70
Console(config)#
```

Displaying Port Power Status

Use the Power Port Status page to display the current PoE power status for all ports.

Command Attributes

- **Port** – The port number.
- **Admin Status** – The administrative status of PoE power on the port.
- **Mode** – The current operating status of PoE power on the port.
- **Power Allocation** – The configured power budget for the port.
- **Power Consumption** – The current power consumption on the port.
- **Priority** – The port's configured power priority setting.

Web – Click PoE, Power Port Status.

Power Port Status

Port	Admin Status	Mode	Power Allocation (milliwatts)	Power Consumption (milliwatts)	Priority
1	Enabled	off	15400	0	low
2	Enabled	off	15400	0	low
3	Enabled	off	15400	0	low
4	Enabled	off	15400	0	low
5	Enabled	off	15400	0	low

Figure 3-64 Displaying Port PoE Status

CLI – This example displays the PoE status and priority of port 1.

```
Console#show power inline status                                          4-74
Interface  Admin   Oper Power(mWatt) Power(used)  Priority
---------- ------- ---- ------------ ------------ --------
Eth   1/ 1  enable  off        15400            0      low
Eth   1/ 2  enable  off        15400            0      low
Eth   1/ 3  enable   on        15400         7505      low
Eth   1/ 4  enable  off        15400            0      low
Eth   1/ 5  enable  off        15400            0      low
Eth   1/ 6  enable  off        15400            0      low
Eth   1/ 7  enable   on        15400         8597      low
:
Eth   1/23  enable  off        15400            0      low
Eth   1/24  enable  off        15400            0      low
Console#
```

Configuring Port PoE Power

If a device is connected to a switch port and the switch detects that it requires more than the power budget of the port, no power is supplied to the device (i.e., port power remains off).

If the power demand from devices connected to switch ports exceeds the power budget set for the switch, the port power priority settings are used to control the supplied power. For example:

- If a device is connected to a low-priority port and causes the switch to exceed its budget, port power is not turned on.
- If a device is connected to a critical or high-priority port and causes the switch to exceed its budget, port power is turned on, but the switch drops power to one or more lower-priority ports.

Note: Power is dropped from low-priority ports in sequence starting from port number 1.

Command Attributes

- **Port** – The port number on the switch.
- **Admin Status** – Enables PoE power on the port. Power is automatically supplied when a device is detected on the port, providing that the power demanded does not exceed the switch or port power budget. (Default: Enabled)
- **Priority** – Sets the power priority for the port. (Options: low, high, or critical; Default: low)
- **Power Allocation** – Sets the power budget for the port. (Range: 3000- 15400 milliwatts; Default: 15400 milliwatts)

Web – Click PoE, Power Port Configuration. Enable PoE power on selected ports, set the priority and the power budget, and then click Apply.

Power Port Configuration

Port	Admin Status	Priority	Power Allocation (3000-15400 milliwatts)	Trunk
1	Enabled	low	15400	
2	Enabled	low	15400	
3	Enabled	low	15400	
4	Enabled	low	15400	
5	Enabled	low	15400	

Figure 3-65 Configuring Port PoE Power

CLI – This example sets the PoE power budget for port 1 to 8 watts, the priority to high (2), and then enables the power.

```
Console(config)#interface ethernet 1/1                          4-133
Console(config-if)#power inline maximum allocation 8000          4-72
Console(config-if)#power inline priority 2                       4-73
Console(config-if)#power inline auto                             4-72
Console(config-if)#
```

Address Table Settings

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

Setting 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.

Command Attributes

- **Static Address Counts*** – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **VLAN** – ID of configured VLAN (1-4093).

* Web Only

Web – Click Address Table, Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address.

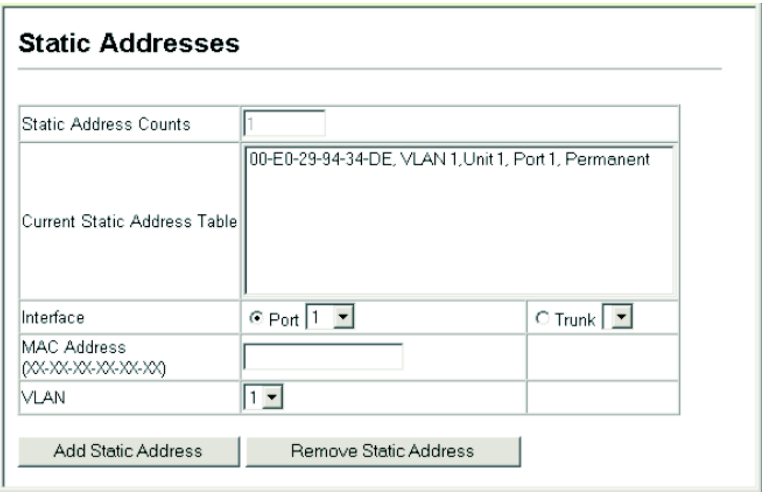


Figure 3-66. Mapping Ports to Static Addresses

CLI – This example adds an address to the static address table, but sets it to be deleted when the switch is reset.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
ethernet 1/1 vlan 1 delete-on-reset                                 4-135
Console(config)#
```

Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Attributes

- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.

- **VLAN** – ID of configured VLAN (1-4093).
- **Address Table Sort Key** – You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
- **Dynamic Address Counts** – The number of addresses dynamically learned.
- **Current Dynamic Address Table** – Lists all the dynamic addresses.

Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e., mark the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses, and then click **Query**.

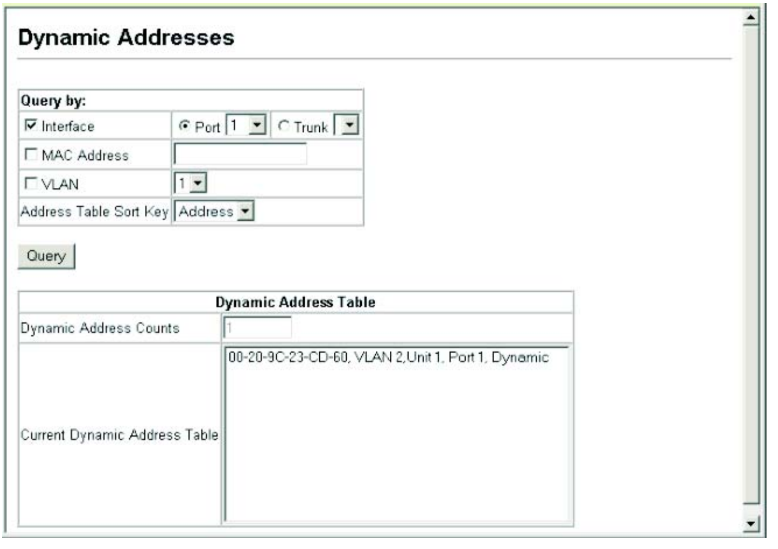


Figure 3-67. Displaying the MAC Dynamic Address Table

CLI – This example also displays the address table entries for port 1.

```
Console#show mac-address-table interface ethernet 1/1                4-137
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-E0-29-94-34-DE    1 Permanent
  Eth 1/ 1 00-20-9C-23-CD-60    2 Learned
Console#
```

Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

Command Attributes

- Aging Status – Enables/disables the function.
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-630 seconds; Default: 300 seconds)

Web – Click Address Table, Address Aging. Specify the new aging time, click **Apply**.

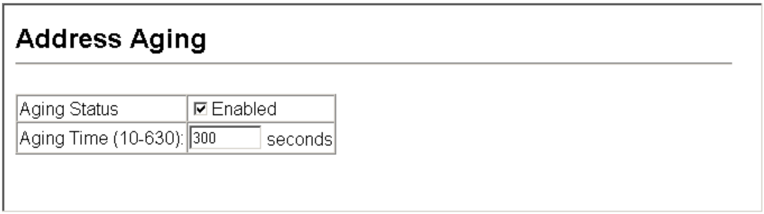


Figure 3-68. Setting the Aging Time

CLI – This example sets the aging time to 300 seconds.

```
Console(config)#mac-address-table aging-time 300                    4-138
Console(config)#
```

Spanning Tree Algorithm Configuration

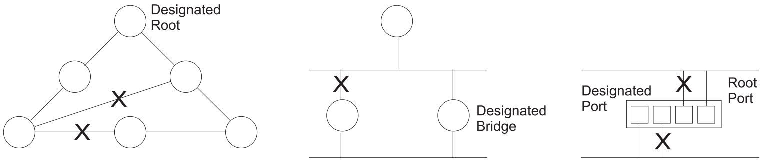
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

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

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. It selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device.

It then selects a port on the designated bridging device to communicate with each attached LAN or host device as a designated port. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



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

RSTP is designed as a general replacement for the slower, legacy STP. RSTP achieves must faster reconfiguration (i.e., around one tenth of the time required by STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

Displaying Global Settings

You can display a summary of the current bridge STA information that applies to the entire switch using the STA Information screen.

Field Attributes

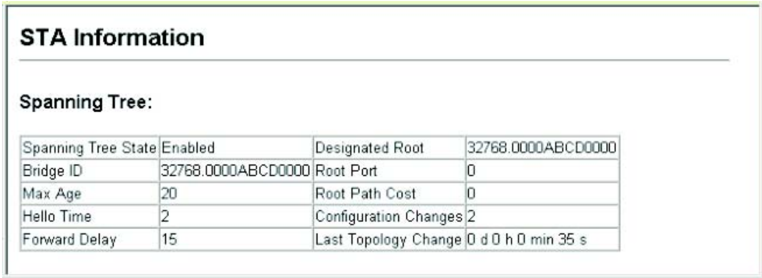
- **Spanning Tree State** – Shows if the switch is enabled to participate in an STA-compliant network.
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority and MAC address (where the address is taken from the switch system).
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

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

These additional parameters are only displayed for the CLI:

- **Spanning tree mode** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D)
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w)
- Priority – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- **Root Hello Time** – Interval (in seconds) at which this device transmits a configuration message.
- **Root Maximum Age** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)
- **Root Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- Transmission limit – The minimum interval between the transmission of consecutive RSTP BPDUs.
- Path Cost Method – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

Web – Click Spanning Tree, STA, Information.



STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0000ABCD0000
Bridge ID	32768.0000ABCD0000	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	2
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 35 s

Figure 3-69. Displaying the Spanning Tree Algorithm

CLI – This command displays global STA settings, followed by settings for each port.

```
Console#show spanning-tree                                              4-150
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode:                  RSTP
 Spanning tree enabled/disabled:        enabled
 Priority:                            32768
 Bridge Hello Time (sec.):            2
 Bridge Max Age (sec.):               20
 Bridge Forward Delay (sec.):         15
 Root Hello Time (sec.):              2
 Root Max Age (sec.):                 20
 Root Forward Delay (sec.):           15
 Designated Root:                     32768.0012CF0B0D00
 Current root port:                   0
 Current root cost:                   0
 Number of topology changes:          1
 Last topology changes time (sec.):2262
 Transmission limit:                  3
 Path Cost Method:                    long
.
.
.
```

Note: The current root port and current root cost display as zero when this device is not connected to the network.

Configuring Global Settings

Global settings apply to the entire switch.

Command Usage

- Spanning Tree Protocol
- Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. Rapid Spanning Tree Protocol

- RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
  - STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Command Attributes

Basic Configuration of Global Settings

- **Spanning Tree State** – Enables/disables STA on this switch. (Default: Enabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)
  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Root Device Configuration

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)
  - Default: 20
  - Minimum: The higher of 6 or [2 x (Hello Time + 1)].

- Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30

Configuration Settings for RSTP

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

Web – Click Spanning Tree, STA, Configration. Modify the required attributes, and click Apply.

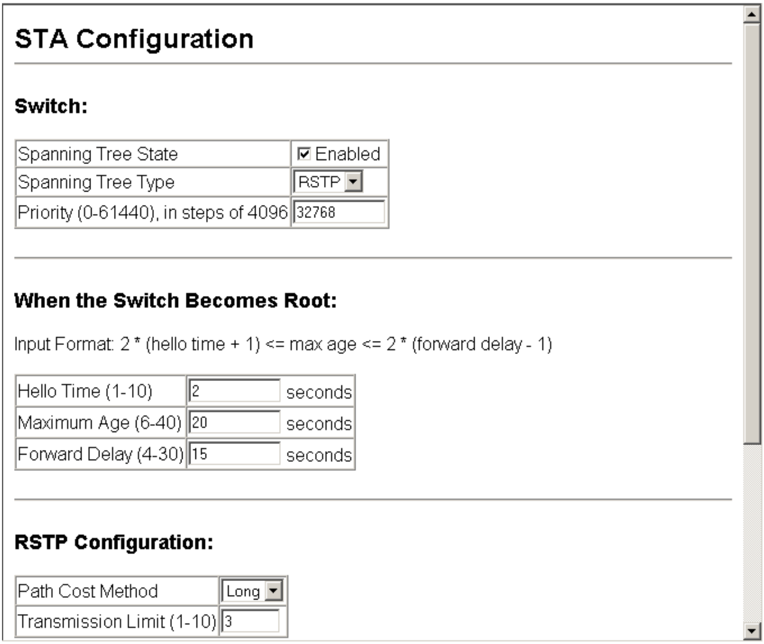


Figure 3-70. Configuring the Spanning Tree Algorithm

CLI – This example enables Spanning Tree Protocol and then configures the STA parameters.

```
Console(config)#spanning-tree                                    4-139
Console(config)#spanning-tree mode                               4-140
Console(config)#spanning-tree priority 40000                     4-143
Console(config)#spanning-tree hello-time 5                       4-142
Console(config)#spanning-tree max-age 38                         4-142
Console(config)#spanning-tree forward-time 20                    4-141
Console(config)#spanning-tree pathcost method long               4-144
Console(config)#spanning-tree transmission-limit 4               4-144
```

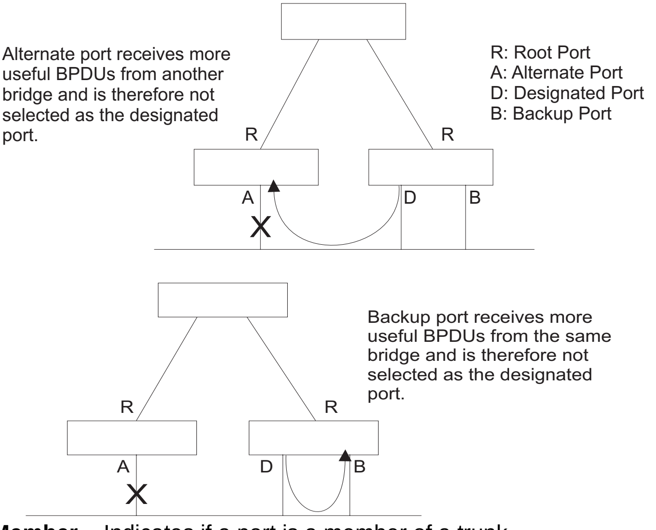
Displaying Interface Settings

The STA Port Information and STA Trunk Information pages display the current status of ports and trunks in the Spanning Tree.

Field Attributes

- **Spanning Tree** – Shows if STA has been enabled on this interface.
- **STA Status** – Displays current state of this port within the Spanning Tree.
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.
  - The rules defining port status are:
  - A port on a network segment with no other STA compliant bridging device is always forwarding.
  - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
  - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Path Cost** – Displays the parameter used by the STA to determine the best path between devices. Lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 3-121.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 3-121 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., **root** port), connecting a LAN

through the bridge to the root bridge (i.e., **designated** port)or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.



- **Trunk Member** – Indicates if a port is a member of a trunk. (STA Port Information only)

These additional parameters are only displayed for the CLI:

- **Admin status** – Shows if this interface is enabled.
- **Path cost** – The path cost for the IST. This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Priority** – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.
- **Designated root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Fast forwarding** – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.
- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices

such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.

Web – Click Spanning Tree, STA, Port Information or Trunk Information.

STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Discarding	0	0	32768.000012322321	128.1	2000000	Shared	Enabled	Disabled	
2	Enabled	Discarding	0	0	32768.000012322321	128.2	2000000	Shared	Enabled	Disabled	
3	Enabled	Forwarding	1	0	32768.000012322321	128.3	100000	Point-to-Point	Enabled	Designated	
4	Enabled	Discarding	0	0	32768.000012322321	128.4	2000000	Shared	Enabled	Disabled	
5	Enabled	Discarding	0	0	32768.000012322321	128.5	2000000	Shared	Enabled	Disabled	
6	Enabled	Discarding	0	0	32768.000012322321	128.6	2000000	Shared	Enabled	Disabled	
7	Enabled	Discarding	0	0	32768.000012322321	128.7	2000000	Shared	Enabled	Disabled	
8	Enabled	Discarding	0	0	32768.000012322321	128.8	2000000	Shared	Enabled	Disabled	
9	Enabled	Discarding	0	0	32768.000012322321	128.9	2000000	Shared	Enabled	Disabled	
10	Enabled	Discarding	0	0	32768.000012322321	128.10	2000000	Shared	Enabled	Disabled	
11	Enabled	Discarding	0	0	32768.000012322321	128.11	2000000	Shared	Enabled	Disabled	
12	Enabled	Discarding	0	0	32768.000012322321	128.12	2000000	Shared	Enabled	Disabled	

Figure 3-71. Displaying STA - Port Status Information

CLI – This example shows the STA attributes for port 5.

```
Console#show spanning-tree ethernet 1/5                              4-150
Eth  1/ 5 information
--------------------------------------------------------------
 Admin status         : enable
 Role                 : disable
 State                : discarding
 External path cost   : 10000
 Internal path cost   : 10000
 Priority             : 128
 Designated cost      : 200000
 Designated port      : 128.5
 Designated root      : 61440.0.0000E9313131
 Designated bridge    : 61440.0.0000E9313131
 Fast forwarding      : enable
 Forward transitions  : 0
 Admin edge port      : enable
 Oper edge port       : enable
 Admin Link type      : auto
 Oper Link type       : point-to-point
 Spanning Tree Status : enable
```

Configuring Interface Settings

You can configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding.

Command Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 3-118 for additional information.)
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk. (STA Port Configuration only)

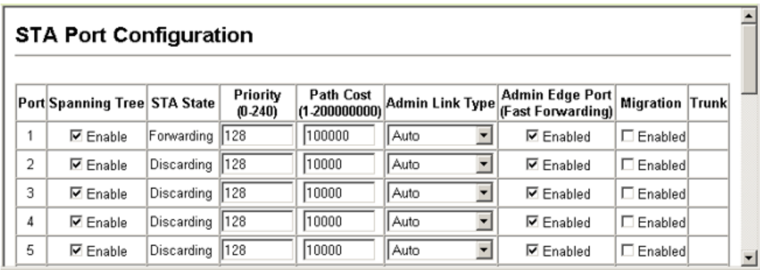
The following interface attributes can be configured:

- **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled).
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16
- **Admin Path Cost** – This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short, the maximum path cost is 65,535.
  - Range –Ethernet: 200,000-20,000,000
  - Fast Ethernet: 20,000-2,000,000
  - Gigabit Ethernet: 2,000-200,000
  - Default –Ethernet – Half duplex: 2,000,000; full duplex:
  - 1,000,000; trunk: 500,000
  - Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
  - Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000
- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.

- Shared – A connection to two or more bridges.
- Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)

- **Admin Edge Port** (Fast Forwarding) – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)
- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces.
  (Default: Disabled)

Web – Click Spanning Tree, STA, Port Configuration or Trunk Configuration. Modify the required attributes, then click Apply.



Port	Spanning Tree	STA State	Priority (0-240)	Path Cost (1-200000000)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	☑ Enable	Forwarding	128	100000	Auto	☑ Enabled	☐ Enabled	
2	☑ Enable	Discarding	128	10000	Auto	☑ Enabled	☐ Enabled	
3	☑ Enable	Discarding	128	10000	Auto	☑ Enabled	☐ Enabled	
4	☑ Enable	Discarding	128	10000	Auto	☑ Enabled	☐ Enabled	
5	☑ Enable	Discarding	128	10000	Auto	☑ Enabled	☐ Enabled	

Figure 3-72. Configuring Spanning Tree Algorithm per Port

CLI – This example sets STA attributes for port 7.

```
Console(config)#interface ethernet 1/7                          4-111
Console(config-if)#no no spanning-tree spanning-disabled        4-145
Console(config-if)#spanning-tree port-priority 0                4-146
Console(config-if)#spanning-tree cost 50                        4-145
Console(config-if)#spanning-tree link-type auto                 4-148
Console(config-if)#no spanning-tree edge-port                   4-147
Console(config-if)#spanning-tree protocol-migration             4-149
Console(config-if)#
```

VLAN Configuration

Overview

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

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

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

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

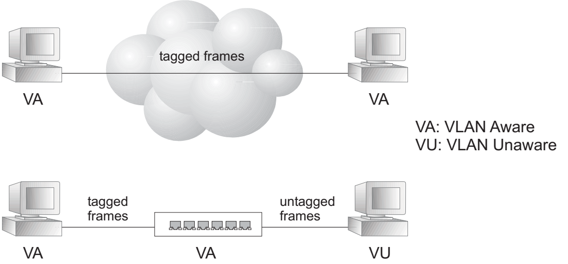
This switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

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

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



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

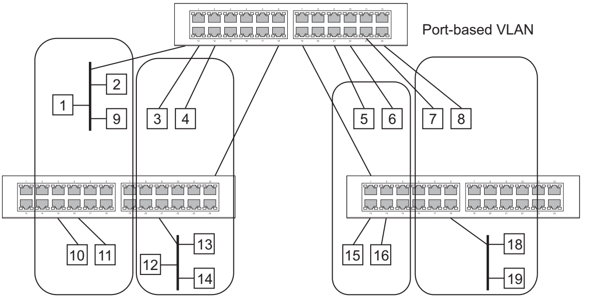
Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

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

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

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

Note: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in "Adding Static Members to VLANs (VLAN Index)" on page 3-129). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.



Forwarding Tagged/Untagged Frames

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

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

Displaying Basic VLAN Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Field Attributes

- **VLAN Version Number*** – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

* Web Only

Web – Click VLAN, 802.1Q VLAN, Basic Information.

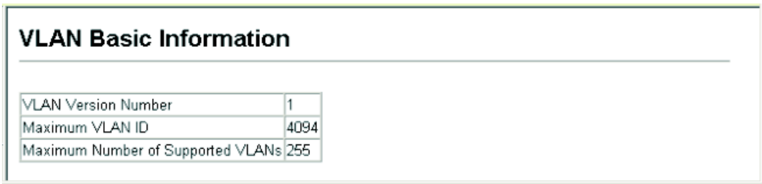


Figure 3-73. Displaying Basic VLAN Information

CLI – Enter the following command.

```
Console#show bridge-ext                                                    4-166
 Max support VLAN numbers:                256
 Max support VLAN ID:                     4093
 Extended multicast filtering services: No
 Static entry individual port:            Yes
 VLAN learning:                           IVL
 Configurable PVID tagging:               Yes
 Local VLAN capable:                      No
 Traffic classes:                         Enabled
 Global GVRP status:                      Disabled
 GMRP:                                    Disabled
Console#
```

Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes (Web)

- **VLAN ID** – ID of configured VLAN (1-4093).
- **Up Time at Creation** – Time this VLAN was created (i.e., System Up Time).

- **Status** – Shows how this VLAN was added to the switch.
  - **Dynamic GVRP**: Automatically learned via GVRP.
  - **Permanent**: Added as a static entry.
- Engress Ports – Shows the engress VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members.

Web – Click VLAN, 802.1Q VLAN, Current Table. Select any ID from the scroll-down list.

Figure 3-74. Displaying VLAN Information by Port Membership

Command Attributes (CLI)

- **VLAN** – ID of configured VLAN (1-4093, no leading zeroes).
- **Type** – Shows how this VLAN was added to the switch.
  - **Dynamic**: Automatically learned via GVRP.
  - **Static**: Added as a static entry.
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Ports / Channel groups** – Shows the VLAN interface members.

CLI – Current VLAN information can be displayed with the following command.

```
Console#show vlan id 1                                                    4-159
VLAN Type    Name        Status   Ports/Channel groups
---- ------- ----------- ------   ------------------------------------
1    Static  DefaultVlan  Active Eth1/1  Eth1/2  Eth1/3  Eth1/4  Eth1/5
                                 Eth1/6  Eth1/7  Eth1/8  Eth1/9  Eth1/10
                                 Eth1/11 Eth1/12 Eth1/13 Eth1/14 Eth1/15
                                 Eth1/16 Eth1/17 Eth1/18 Eth1/19 Eth1/20
                                 Eth1/21 Eth1/22 Eth1/23 Eth1/24
Console#
```

Creating VLANs

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- **New** – Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **VLAN Name** – Name of the VLAN (1 to 32 characters).
- **Status** (Web) – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **State** (CLI) – Enables or disables the specified VLAN.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Add** – Adds a new VLAN group to the current list.
- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Web – Click VLAN, 802.1Q VLAN, Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.

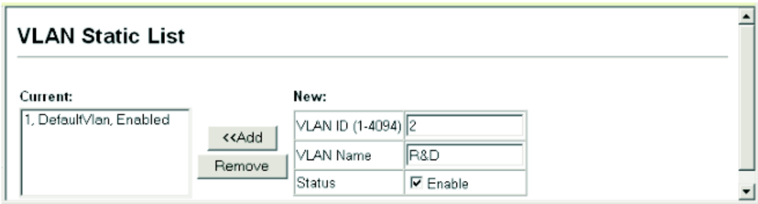


Figure 3-75. Creating Virtual LANs

CLI – This example creates a new VLAN.

```
Console(config)#vlan database                                        4-152
Console(config-vlan)#vlan 2 name R&D media ethernet state active   4-153
Console(config-vlan)#end
Console#show vlan                                                    4-159
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- ---------
----------------------------------
   1  Static      DefaultVlan    Active Eth1/1 Eth1/2 Eth1/3 Eth1/4 Eth1/
5
                                        Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9
Eth1/10
                                        Eth1/11 Eth1/12 Eth1/13 Eth1/14
Eth1/15
                                        Eth1/16 Eth1/17 Eth1/18 Eth1/19
Eth1/20
                                        Eth1/21 Eth1/22 Eth1/23 Eth1/24
   2  Static              R&D    Active
Console(config-vlan)#
```

Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

Notes: 1. You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index (page 3-131). However, note that this configuration page can only add ports to a VLAN as tagged members.

2. VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under “Configuring VLAN Behavior for Interfaces” on page 3-132.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4093, no leading zeroes).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **Port** – Port identifier.
- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface can only have one untagged VLAN, which must be the same as the Port VID. See “Configuring VLAN Behavior for Interfaces” on page 3-132 for configuring PVID.
  - **Forbidden**: Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see “Automatic VLAN Registration” on page 3-124.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
  - **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.

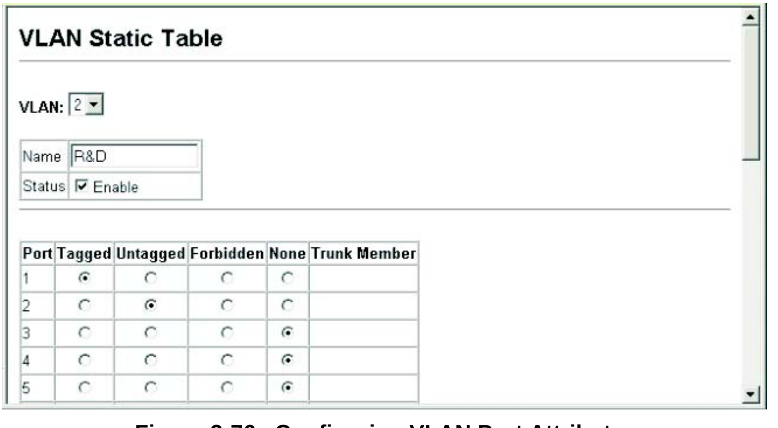


Figure 3-76. Configuring VLAN Port Attributes

CLI – The following example adds tagged and untagged ports to VLAN 2.

```
Console(config)#interface ethernet 1/1                                  4-111
Console(config-if)#switchport allowed vlan add 2 tagged                 4-157
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
```

Adding Static Members to VLANs (Port Index)

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface as a tagged member.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a tagged member.

Web – Open VLAN, 802.1Q VLAN, Static Membership. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.

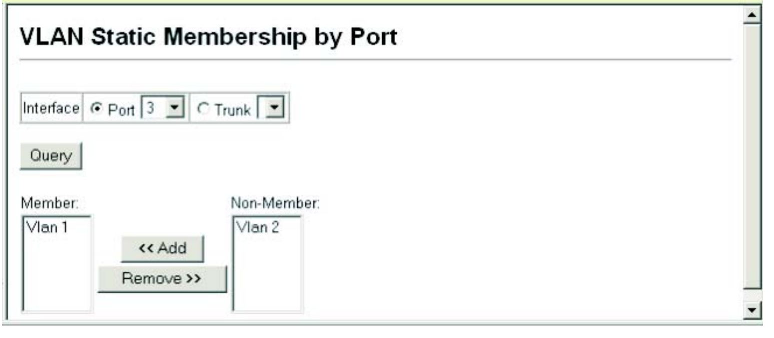


Figure 3-77. Assigning VLAN Port and Trunk Groups

CLI – This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/3                                  4-111
Console(config-if)#switchport allowed vlan add 1 tagged                 4-157
Console(config-if)#switchport allowed vlan remove 2
```

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, and ingress filtering.

Command Attributes

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)
- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, the PVID must be defined first, then the status of the VLAN can be configured as a tagged or untagged member.
- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)
- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. Ingress Filtering is always enabled. (Default: Enabled)
  - Ingress filtering only affects tagged frames.
  - If a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
  - Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.
- **Mode** – Indicates VLAN membership mode for an interface. (Default: Hybrid)
  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.
  - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Port Configuration or Trunk Configuration. Fill in the required settings for each interface, click Apply.

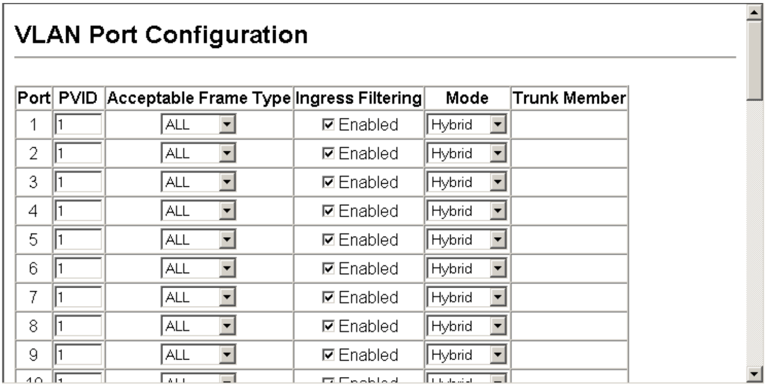


Figure 3-78. Configuring VLAN Ports

CLI – This example sets port 3 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, and then sets the switchport mode to hybrid.

```
Console(config)#interface ethernet 1/3                           4-111
Console(config-if)#switchport acceptable-frame-types tagged      4-155
Console(config-if)#switchport ingress-filtering                  4-156
Console(config-if)#switchport native vlan 3                      4-157
Console(config-if)#switchport gvrp                               4-166
Console(config-if)#switchport mode hybrid                        4-155
Console(config-if)#
```

Configuring Private VLANs

Private VLANs provide port-based security between ports within the assigned VLAN. This switch supports primary/secondary associated groups of private VLAN. A primary VLAN contains promiscuous ports that can communicate with all other ports in the private VLAN group, while a secondary (or community) VLAN contains community ports that can only communicate with other hosts within the secondary VLAN and with any of the promiscuous ports in the associated primary VLAN. In both cases, the promiscuous ports are designed to provide open access to an external network such as the Internet, while the community ports provide restricted access to local users.

Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be associated with each primary VLAN. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

To configure primary/secondary associated groups, follow these steps:

1. Use the Private VLAN Configuration menu to designate one or more community VLANs, and the primary VLAN that will channel traffic outside of the VLAN groups.
2. Use the Private VLAN Association menu to map the secondary (i.e., community) VLAN(s) to the primary VLAN.
3. Use the Private VLAN Port Configuration menu to set the port type to promiscuous (i.e., having access to all ports in the primary VLAN), or host (i.e., having access restricted to community VLAN members, and channeling all other traffic through promiscuous ports). Then assign any promiscuous ports to a primary VLAN and any host ports a community VLAN.

Displaying Current Private VLANs

The Private VLAN Information page displays information on the private VLANs configured on the switch, including primary and community VLANs, and their assigned interfaces.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4093), and VLAN type.
- **Primary VLAN** – The VLAN with which the selected VLAN ID is associated. A primary VLAN displays its own ID, and a community VLAN displays the associated primary VLAN.
- **Ports List** – The list of ports (and assigned port type) in the selected private VLAN.

Web – Click VLAN, Private VLAN, Information. Select the desired port from the VLAN ID drop-down menu.

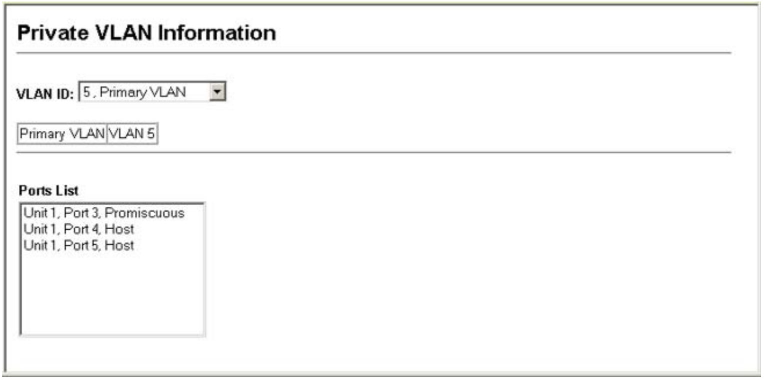


Figure 3-79. Private VLAN Information

CLI – This example shows the switch configured with primary VLAN 5 and secondary VLAN 6. Port 3 has been configured as a promiscuous port and mapped to VLAN 5, while ports 4 and 5 have been configured as a host ports and are associated with VLAN 6. This means that traffic for port 4 and 5 can only pass through port 3.

```
Console#show vlan private-vlan                                        4-153
Primary   Secondary       Type       Interfaces
--------  -----------  ----------  --------------------------------------
     5                 primary     Eth1/ 3
     5          6      community   Eth1/ 4 Eth1/ 5
```

Configuring Private VLANs

The Private VLAN Configuration page is used to create/remove primary, or community VLANs.

Command Attributes

- **VLAN ID** – ID of configured VLAN (2-4094).
- **Type** – There are three types of private VLANs:
  - **Primary** – Conveys traffic between promiscuous ports, and to their community ports within secondary (or community) VLANs.
  - **Community** – Conveys traffic between community ports, and to their promiscuous ports in the associated primary VLAN.
- **Current** - Displays a list of the currently configured VLANs.

Web – Click VLAN, Private VLAN, Configuration. Enter the VLAN ID number, select Primary, or Community type, then click Add. To remove a private VLAN from the switch, highlight an entry in the Current list box and then click Remove. Note that all member ports must be removed from the VLAN before it can be deleted.

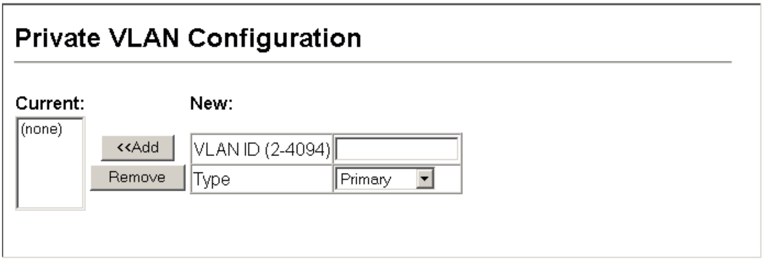


Figure 3-80. Private VLAN Configuration

CLI – This example configures VLAN 5 as a primary VLAN, and VLAN 6 as a community VLAN.

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 5 primary
Console(config-vlan)#private-vlan 6 community
Console(config-vlan)#
```

Associating VLANs

Each community VLAN must be associated with a primary VLAN.

Command Attributes

- **Primary VLAN ID** - ID of primary VLAN (1-4093).
- **Association** - Community VLANs associated with the selected primary VLAN.
- **Non-Association** - Community VLANs not associated with the selected VLAN.

Web – Click VLAN, Private VLAN, Association. Select the required primary VLAN from the scroll-down box, highlight one or more community VLANs in the Non-Association list box, and click Add to associate these entries with the selected primary VLAN. (A community VLAN can only be associated with one primary VLAN.)

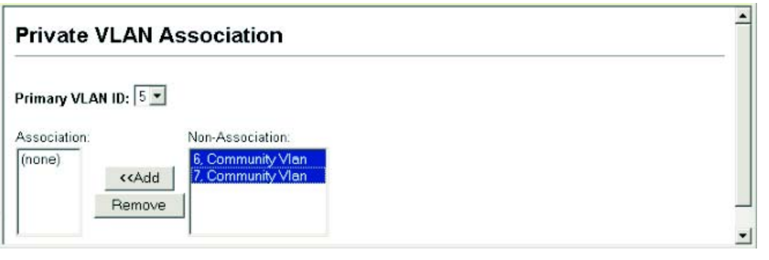


Figure 3-81. Private VLAN Association

CLI – This example associates community VLANs 6 and 7 with primary VLAN 5

```
Console(config)#vlan database                              4-152
Console(config-vlan)#private-vlan 5 association 6          4-162
Console(config-vlan)#private-vlan 5 association 7          4-162
Console(config)#
```

Displaying Private VLAN Interface Information

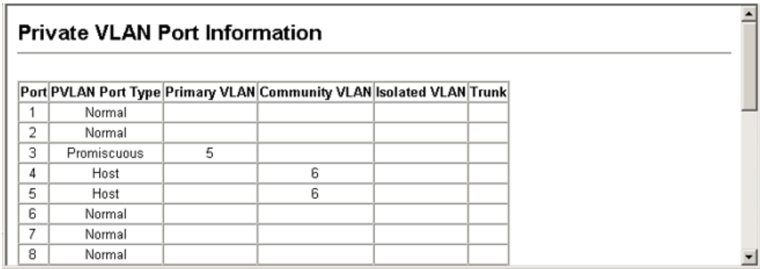
Use the Private VLAN Port Information and Private VLAN Trunk Information menus to display the interface associated with private VLANs.

Command Attributes

- **Port/Trunk** - The switch interface.
- **PVLAN Port Type** - Displays private VLAN port types.

  - **Normal** – The port is not configured in a private VLAN.
  - **Host** – The port is a community port and can only communicate with other ports in its own community VLAN, and with the designated promiscuous port(s).
  - **Promiscuous** – A promiscuous port can communicate with all the interfaces within a private VLAN.
- **Primary VLAN** - Conveys traffic between promiscuous ports, and between promiscuous ports and community ports within the associated secondary VLANs.
- **Community VLAN** – A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports.
- **Trunk** – The trunk identifier. (Port Information only)

Web – Click VLAN, Private VLAN, Port Information or Trunk Information.


Private VLAN Port Information

Port	PVLAN Port Type	Primary VLAN	Community VLAN	Isolated VLAN	Trunk
1	Normal				
2	Normal				
3	Promiscuous	5			
4	Host		6		
5	Host		6		
6	Normal				
7	Normal				
8	Normal				

Figure 3-82. Private VLAN Port Information

CLI – This example shows the switch configured with primary VLAN 5 and community VLAN 6. Port 3 has been configured as a promiscuous port and mapped to VLAN 5, while ports 4 and 5 have been configured as host ports and associated with VLAN 6. This means that traffic for port 4 and 5 can only pass through port 3.

```
Console#show vlan private-vlan                                         4-43
Primary   Secondary       Type       Interfaces
--------  -----------   ----------  ------------------------------
     5                  primary     Eth1/ 3
     5          6       community   Eth1/ 4 Eth1/ 5
Console#
```

Configuring Private VLAN Interfaces

Use the Private VLAN Port Configuration and Private VLAN Trunk Configuration menus to set the private VLAN interface type, and assign the interfaces to a private VLAN.

Command Attributes

- **Port/Trunk** - The switch interface.
- **PVLAN Port Type** - Sets private VLAN port types.
  - **Normal** – The port is not assigned in a private VLAN.
  - **Host** – The port is a community port. A community port can communicate with other ports in its own community VLAN and with designated promiscuous port(s).
  - **Promiscuous** – A promiscuous port can communicate with all the interfaces within a private VLAN.
- **Primary VLAN** - Conveys traffic between promiscuous ports, and between promiscuous ports and community ports within the associated secondary VLANs. If PVLAN type is “Promiscuous,” then specify the associated primary VLAN.
- **Community VLAN** – A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports. Set PVLAN Port Type to “Host,” and then specify the associated Community VLAN.
- **Trunk** – The trunk identifier. (Port Information only)

Web – Click VLAN, Private VLAN, Port Configuration or Trunk Configuration. Set the PVLAN Port Type for each port that will join a private VLAN. Assign promiscuous ports to a primary VLAN. Assign host ports to a community VLAN. After all the ports have been configured, click Apply.

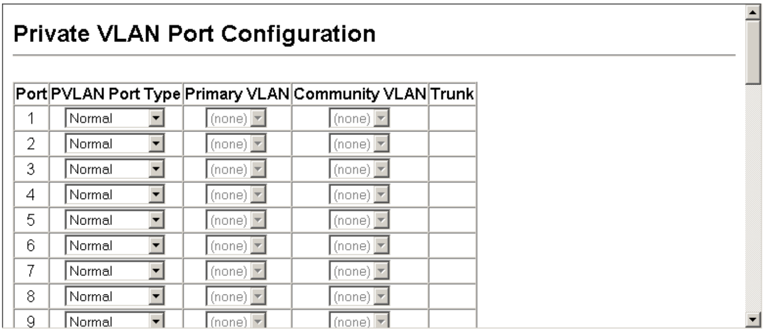


Figure 3-83. Private VLAN Port Configuration

CLI – This example shows the switch configured with primary VLAN 5 and secondary VLAN 6. Port 3 has been configured as a promiscuous port and mapped to VLAN 5, while ports 4 and 5 have been configured as a host ports and associated with VLAN 6. This means that traffic for port 4 and 5 can only pass through port 3.

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan promiscuous        4-155
Console(config-if)#switchport private-vlan mapping 5               4-164
Console(config-if)#exit
Console(config)#interface ethernet 1/4
Console(config-if)#switchport mode private-vlan host               4-162
Console(config-if)#switchport private-vlan host-association 6      4-163
Console(config-if)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#switchport mode private-vlan host
Console(config-if)#switchport private-vlan host-association 6
Console(config-if)#
```

Configuring Protocol VLANs

You can configure VLAN behavior to support multiple protocols to allow traffic to pass through different VLANS. When a packet is received at a port, its VLAN membership is determined by the protocol type of the packet.

Configuring Protocol VLAN Basic Settings

Use the Protocol VLAN Configuration menu to create or remove protocol VLANs.

Command Attributes

- **Protocol Group IP** - Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)
- **Frame Type** - Ethernet frame type.
- **Protocol Type** - The options for Ethernet frame type includes IP, ARP, or RARP.

Web – Click VLAN, Protocol VLAN, Configuration.

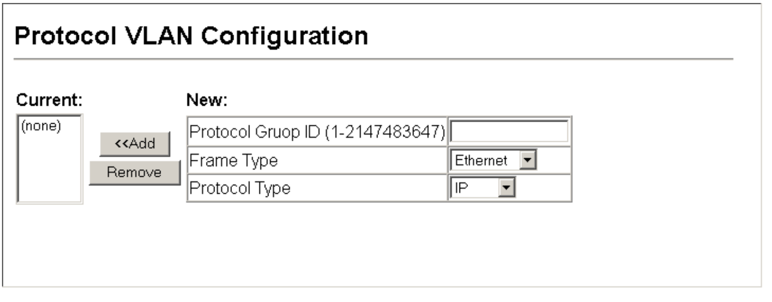


Figure 3-84. Protocol VLAN Configuration

Configuring Protocol VLAN System

Use the Protocol VLAN System Configuration menu to set the protocol VLAN settings for the switch.

Command Attributes

- **Protocol Group ID** - Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)
- **VLAN ID** - VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

Web – Click VLAN, Protocol VLAN, System Configuration.

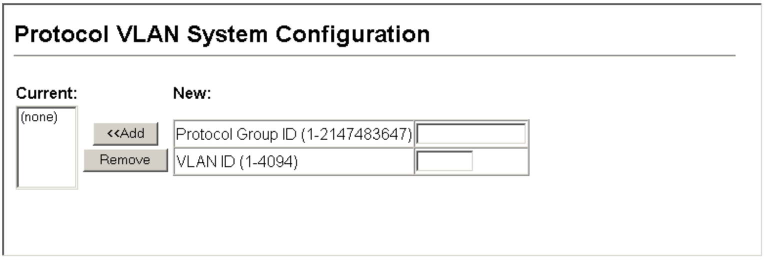


Figure 3-85. Protocol VLAN Port Configuration

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers. This information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Configuring Basic LLDP Time Information

Configures basic time parameters for LLDP configuration.

Command Attributes

- **LLDP** - Enable or disables LLDP.
- **Transmission Interval** - Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds)
- **Hold time Multiplier** - Configures the time-to-live (TTL) value sent in LLDP advertisements. (Range: 2-10 seconds)

- **Delay Interval** - Configures a delay time between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 0-8192 seconds)
- **Reinitialisation Delay** - Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. (Range: 0-10 seconds)
- **Notification Interval** - Configures the allowed interval for sending SNMP notifications about LLDP changes. (Range: 0-3600)

Web – Click LLDP, Configuration.

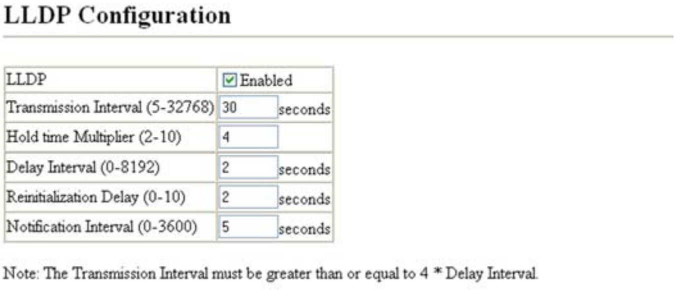


Figure 3-86. LLDP Configuration

CLI – This example shows the setting of the transmit interval to 60 seconds, the transmit delay to 10 seconds, the hold time to 10 seconds, the reinitialisation delay to 10 seconds, and the notifcation interval to 30 seconds.

```
Console(config)#lldp transmit- interval 60                          4-201
Console(config)#lldp transmit-delay 10                              4-201
Console(config)#lldp transmit-hold 10                               4-202
Console(config)#lldp reinit-delay 10                                4-202
Console(config)#lldp notification-interval 30                       4-203
Console(config)#
```

Configuring LLDP Port and Trunk Information

These commands enable LLDP transmit, receive, or transmit and receive mode on the specified port, whether to send SNMP notifications, and sets the TLV type.

Command Attributes

- **Port** - Specifies the port number.
- **LLDP** - Enables LLDP transmit (Tx only), receive (Rx only), or transmit and receive RxTx) mode on the specified port. Chosing ‘Disabled’ disables LLDP on the port.
- **SNMP Notification** - Enables the sending of SNMP trap messages about LLDP changes on the specified port.
- **TLV Type** - Configures the port to advertise the management address for the deivce, the port description, the system capabilities, the system description and the system name. Check each respective box to enable each feature.

- **Trunk** - Specifies if the port is a member of a trunk.

Web – Click LLDP, Port Configuration.

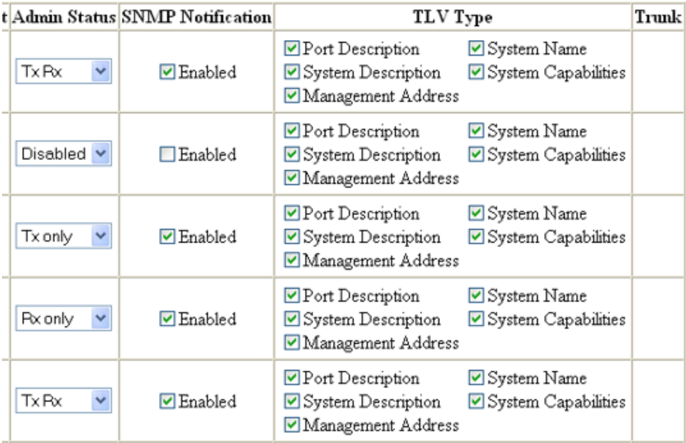


Figure 3-87. LLDP Port Configuration

CLI – This example shows the administration status of the specified port being set to transmit and recieve.

```
Console(config)#interface ge1/1
Console(config-if)#lldp transmit-and-receive                        4-204
Console(config-if)#
```

CLI – This example shows the enabling of SNMP trap notication messages on the specified port.

```
Console(config)#interface ge1/1
Console(config-if)#lldp notification                                4-207
Console(config-if)#
```

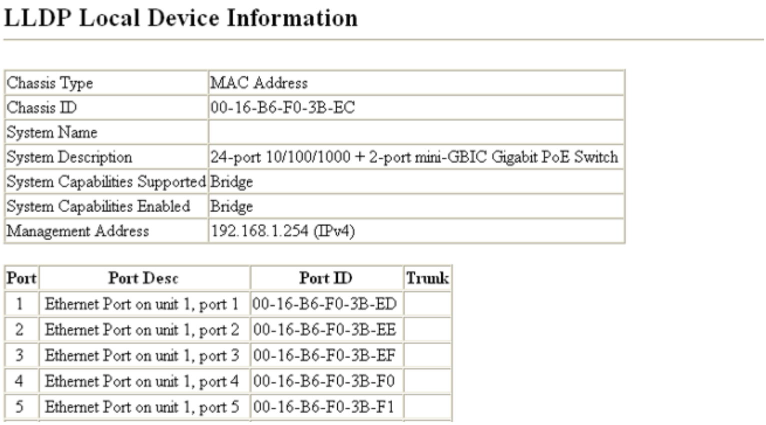
CLI – This example shows the enabling of basic TLV parameters to be broadcast about the specified port.

```
Console(config)#interface ge1/1
Console(config-if)#lldp basic-tlv management-address                4-204
Console(config-if)#lldp basic-tlv description                       4-205
Console(config-if)#lldp basic-tlv system-capabilities               4-206
Console(config-if)#lldp basic-tlv system-description                4-206
Console(config-if)#lldp basic-tlv system-name                       4-207
Console(config)#
```

Displaying LLDP Local and Remote Device Information

This displays information about the switch, such as its MAC address, chassis ID, management IP address, aswell as port information.

Web – Click LLDP, Local Information for local device information. Or click LLDP, Remote Port or Trunk Information for remote device port or trunk information.



LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	00-16-B6-F0-3B-EC
System Name	
System Description	24-port 10/100/1000 + 2-port mini-GBIC Gigabit PoE Switch
System Capabilities Supported	Bridge
System Capabilities Enabled	Bridge
Management Address	192.168.1.254 (IPv4)

Port	Port Desc	Port ID	Trunk
1	Ethernet Port on unit 1, port 1	00-16-B6-F0-3B-ED	
2	Ethernet Port on unit 1, port 2	00-16-B6-F0-3B-EE	
3	Ethernet Port on unit 1, port 3	00-16-B6-F0-3B-EF	
4	Ethernet Port on unit 1, port 4	00-16-B6-F0-3B-F0	
5	Ethernet Port on unit 1, port 5	00-16-B6-F0-3B-F1	

Figure 3-88. LLDP Local Device Information

Web – Click LLDP, Remote Information to specify the port or trunk associated with the device, then click Remote Port or Remote Trunk for remote device port or trunk information.

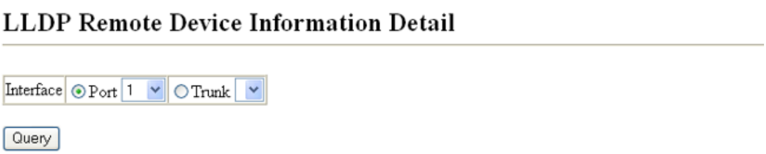


Figure 3-89. LLDP Remote Device Information

CLI – This example shows LLDP configuration settings for all ports.

```
Console#show lldp config                                          4-212
LLDP Global Configuation
LLDP Transmit interval : 30
LLDP Hold Time Multiplier : 4
LLDP Delay Interval : 2
LLDP Reinit Delay : 2
LLDP Notification Interval : 5

LLDP Port Configuration
Port AdminStatus NotificationEnabled
-------- + ---------- ------------------
ge1/1 Rx False
ge1/2 Rx False
ge1/3 Rx False
ge1/4 Rx False
... ge1/5 Rx False


switch#show lldp config detail
LLDP Port Configuration Detail
Port : ge1/1
Admin Status : Rx
...Notification Enabled : False

Console(config)#
```

CLI – This example shows LLDP global and interface-specific configuration settings for this device.

```
Console#show lldp info local-device                               4-213
LLDP Local System Information
Chassis Type : MAC Address
Chassis ID : 00-01-22-33-44-AB
System Description : ECN430
System Capabilities Support : Bridge, Router
System Capabilities Enable : Bridge, Router
Management Address : 0.0.0.0 (IPv4)
LLDP Port Information
Port | PortID Type PortID PortDesc
----- + --------------- ---------------- ----------------
ge1/1 MAC Address 00-01-22-33-44-AC ge1/1
ge1/2 MAC Address 00-01-22-33-44-AD ge1/2
ge1/3 MAC Address 00-01-22-33-44-AE ge1/3
ge1/4 MAC Address 00-01-22-33-44-AF ge1/4
... ge1/5 MAC Address 00-01-22-33-44-B0 ge1/5

Console#show lldp info local-device detail
LLDP Port Information Detail
Port : ge1/1
Port Type : MAC Address
Port ID : 00-01-22-33-44-AC
...P ort Desc : ge1/1

Console(config)#
```

CLI – This example shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

```
switch#show lldp info remote-device                                      4-214
LLDP Remote Devices Information
Interface | ChassisId PortId SysName
--------- + ---------------- ---------------- -----------
please provide sample data
switch#show lldp info remote-device detail
LLDP Remote Devices Information
please provide sample data
switch#

Console(config)#
```

CLI – This example shows statistical counters all LLDP-enabled interfaces.

```
switch#show lldp info statistics                                        4-215
LLDP Device Statistics
Neighbor Entries List Last Updated : 0 seconds
New Neighbor Entries Count : 0
Neighbor Entries Deleted Count : 0
Neighbor Entries Dropped Count : 0
Neighbor Entries Ageout Count : 0
Port | NumFramesRecvd NumFramesSent NumFramesDiscarded
----- + -------------- ------------ -----------------
1 | 0 0 0
2 | 0 0 0
3 | 0 0 0
4 | 0 0 0
... 5 | 0 0 0
switch#sh lldp info statistics detail
LLDP Port Statistics Detail
PortName : ge1/1
Frames Discarded : 0
Frames Invalid : 0
Frames Received : 0
Frames Sent : 0
TLVs Unrecognized : 0
TLVs Discarded : 0
... Ne ighbor Ageouts

Console(config)#
```

Class of Service Configuration

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port’s high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch’s priority queues.

Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Command Usage

- This switch provides eight priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

- **Default Priority*** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0 - 7, Default: 0)
- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

* CLI displays this information as "Priority for untagged traffic."

Web – Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.

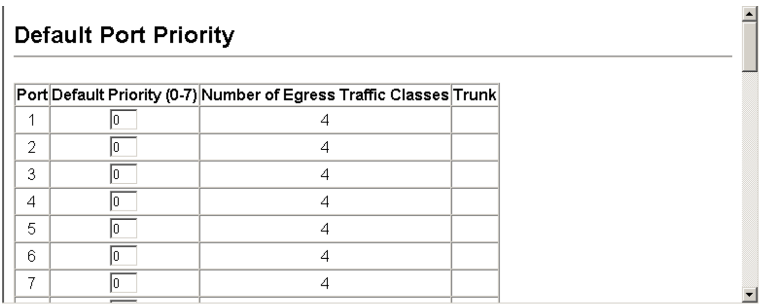


Figure 3-90. Port Priority Configuration

CLI – This example assigns a default priority of 5 to port 3.

```
Console(config)#interface ethernet 1/3                                      4-111
Console(config-if)#switchport priority default 5                           4-170
Console(config-if)#end
Console#show interfaces switchport ethernet 1/3                            4-119
Information of Eth 1/3
 Broadcast threshold:            Enabled, 500 packets/second
 LACP status:                    Disabled
 Ingress rate limit: enable, K bits per second: 25
 VLAN membership mode:           Hybrid
 Ingress rule:                   Enabled
 Acceptable frame type:          All frames
 Native VLAN:                    1
 Priority for untagged traffic: 5
 GVRP status:                    Disabled
 Allowed VLAN:                   1(u),
 Forbidden VLAN:
 Private-VLAN mode:              NONE
 Private-VLAN host-association: NONE
 Private-VLAN mapping:           NONE
Console#
```

Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict or Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Table 3-12 Egress Queue Priority Mapping

Queue	0	1	2	3
Priority	1,2	0,3	4,5	6,7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

Table 3-13 CoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter

Table 3-13 CoS Priority Levels

Priority Level	Traffic Type
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

- Interface – Select port or trunk identifier.
- **Priority** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **Traffic Class*** – Output queue buffer. (Range: 0-3, where 3 is the highest CoS priority queue)

* CLI shows Queue ID.

Web – Click Priority, Traffic Classes. Assign priorities to the traffic classes (i.e., output queues), then click Apply.

Figure 3-91. Configuring Class of Service

CLI – The following example shows how to change the CoS assignments to a one-to-one mapping.

```
Console(config)#interface ethernet 1/1                            4-111
Console(config-if)#queue cos-map 0 0                              4-172
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console(config)#exit
Console#show queue cos-map ethernet 1/1                           4-174
Information of Eth 1/1
 CoS Value :     0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 1 2 2 3 3
.
.
.
```

Note: Mapping specific values for CoS priorities is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Enabling CoS

Enable or disable Class of Service (CoS). Command Attributes.

Command Attributes

- **Traffic Classes** - Click to enable Class of Service. (Default: Enabled)

Web – Click Priority, Traffic Classes Status.

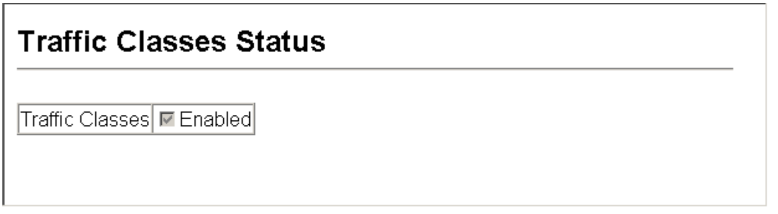


Figure 3-92. Enable Traffic Classes

Selecting the Queue Mode

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Command Attributes

- **WRR** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 through 7 respectively. (This is the default selection.)
- **Strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

Web – Click Priority, Queue Mode. Select Strict or WRR, then click Apply.

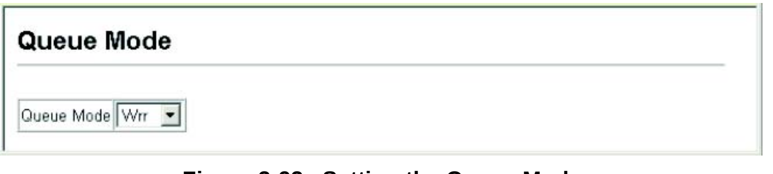


Figure 3-93. Setting the Queue Mode

CLI – The following sets the queue mode to strict priority service mode.

```
Console(config)#queue mode strict                                          4-173
Console(config)#exit
Console#show queue mode                                                    4-173

Queue mode: strict
Console#
```

Setting the Service Weight for Traffic Classes

This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in “Mapping CoS Values to Egress Queues” on page 3-147, the traffic classes are mapped to one of the four egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes

- **WRR Setting Table*** – Displays a list of weights for each traffic class (i.e., queue).

    * CLI shows Queue ID.

Web – Click Priority, Queue Scheduling. Highlight a traffic class (i.e., output queue), then click Apply.

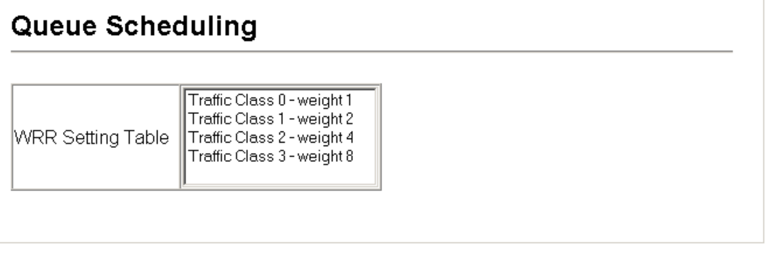


Figure 3-94. Configuring Queue Scheduling

CLI – The following example shows how to assign WRR weights to each of the priority queues.

```
Console(config)#queue bandwidth 1 2 4 8                                   4-172
Console(config)#exit
Console#show queue bandwidth                                              4-174
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
    0        1
    1        2
    2        3
    3        8
Information of Eth 1/2
 Queue ID  Weight
.
.
.
```

Mapping Layer 3/4 Priorities to CoS Values

This switch supports one method of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame using the number of the TCP port. When these service is enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP DSCP Priority, and then Default Port Priority.

Selecting IP DSCP Priority

The switch allows you to enable or disable IP DSCP priority.

Command Attributes

- **IP DSCP Priority Status – Enables the priority services**. Maps layer 3/4 priorities using Differentiated Services Code Point Mapping. **(Default Setting: Disabled)**

Web – Click Priority, IP DSCP Priority Status. Select IP DSCP, then click Apply.

Figure 3-95. IP DSCP Priority Status

Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP retains backward compatibility with the three precedence bits so that non-DSCP compliant will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 3-14 Mapping DSCP Priority

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

- **DSCP Priority Table –** Shows the DSCP Priority to CoS map.
- **Class of Service Value –** Maps a CoS value to the selected DSCP Priority value. Note that “0” represents low priority and “7” represent high priority.

Note: IP DSCP settings apply to all interfaces.

Web – Click Priority, IP DSCP Priority. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click Apply.

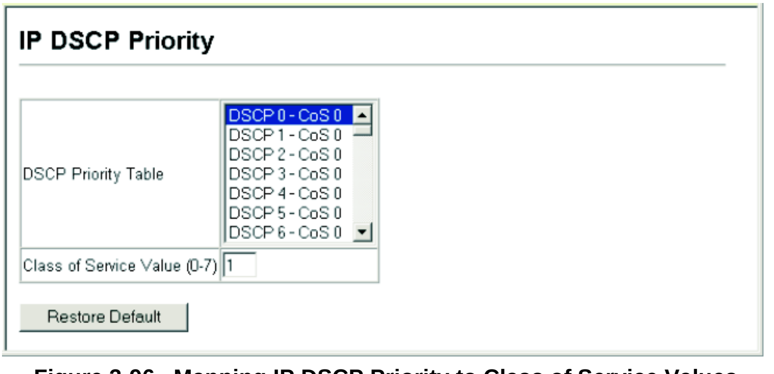


Figure 3-96. Mapping IP DSCP Priority to Class of Service Values

CLI – The following example globally enables DSCP Priority service on the switch, maps DSCP value 0 to CoS value 1 (on port 1), and then displays the DSCP Priority settings.

```
Console(config)#map ip dscp                                              4-175
Console(config)#interface ethernet 1/1                                   4-111
Console(config-if)#map ip dscp 1 cos 0                                   4-176
Console(config-if)#end
Console#show map ip dscp ethernet 1/1                                    4-177
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
.
.
.
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Note: Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Quality of Service

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

Notes: **1.** You can configure up to 16 rules per Class Map. You can also include multiple classes in a Policy Map.

2. You should create a Class Map before creating a Policy Map. Otherwise, you will not be able to select a Class Map from the Policy Rule Settings screen.

Configuring Quality of Service Parameters

To create a service policy for a specific category or ingress traffic, follow these steps:

1. Use the “Class Map” to designate a class name for a specific category of traffic.
2. Edit the rules for each class to specify a type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Use the “Policy Map” to designate a policy name for a specific manner in which ingress traffic will be handled.
4. Add one or more classes to the Policy Map. Assign policy rules to each class by “setting” the QoS value to be assigned to the matching traffic class. The policy rule can also be configured to monitor the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
5. Use the “Service Policy” to assign a policy map to a specific interface.

Configuring a Class Map

A class map is used for matching packets to a specified class.

Command Usage

- To configure a Class Map, follow these steps:
  - Open the Class Map page, and click Add Class.
  - When the Class Configuration page opens, fill in the “Class Name” field, and click Add.
  - When the Match Class Settings page opens, specify type of traffic for this class based on an access list, a DSCP or IP Precedence value, or a VLAN, and click the Add button next to the field for the selected traffic criteria. You can specify up to 16 items to match when assigning ingress traffic to a class map.
- The class map is used with a policy map to create a service policy for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.

Command Attributes

Class Map

- **Modify Name and Description** – Configures the name and a brief description of a class map. (Range: 1-16 characters for the name; 1-64 characters for the description)

- **Edit Rules** – Opens the “Match Class Settings” page for the selected class entry. Modify the criteria used to classify ingress traffic on this page.
- **Add Class** – Opens the “Class Configuration” page. Enter a class name and description on this page, and click Add to open the “Match Class Settings” page. Enter the criteria used to classify ingress traffic on this page.
- **Remove Class** – Removes the selected class.

Class Configuration

- **Class Name** – Name of the class map. (Range: 1-16 characters)
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- **Description** – A brief description of a class map.
(Range: 1-64 characters)
- **Add** – Adds the specified class.
- **Back** – Returns to previous page without making any changes.

Match Class Settings

- **Class Name** – List of the class maps.
- **ACL List** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- **IP DSCP** – A DSCP value. (Range: 0-63)
- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **VLAN** – A VLAN. (Range:1-4094)
- **Add** – Adds specified criteria to the class. Up to 16 items are permitted per class.
- **Remove** – Deletes the selected criteria from the class.

Web – Click QoS, DiffServ, then click Add Class to create a new class, or Edit Rules to change the rules of an existing class.

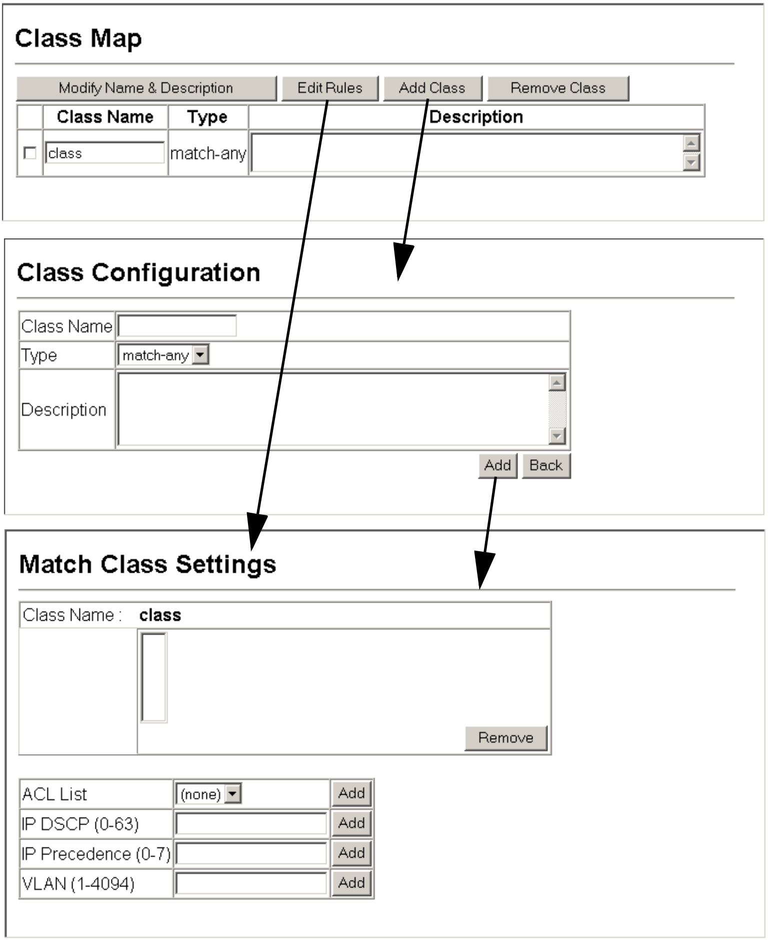


Figure 3-97. Configuring Class Maps

CLI – This example creates a class map call “rd-class,” and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd_class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

Creating QoS Policies

This function creates a policy map that can be attached to multiple interfaces.

Command Usage

- To configure a Policy Map, follow these steps:
  - Create a Class Map as described on 3-154.
  - Open the Policy Map page, and click Add Policy.
  - When the Policy Configuration page opens, fill in the “Policy Name” field, and click Add.
  - When the Policy Rule Settings page opens, select a class name from the scroll-down list (Class Name field). Configure a policy for traffic that matches criteria defined in this class by setting the quality of service that an IP packet will receive (in the Action field), defining the maximum throughput and burst rate (in the Meter field), and the action that results from a policy violation (in the Exceed field). Then finally click Add to register the new policy.
- A policy map can contain multiple class statements that can be applied to the same interface with the Service Policy Settings (page 3-153). You can configure up to 64 policers (i.e., meters or class maps) for each of the following access list types: MAC ACL, IP ACL (including Standard ACL and Extended ACL), IPv6 Standard ACL, and IPv6 Extended ACL. This limitation applies to each switch chip (ES4524D: ports 1-26, ES4548D: ports 1-25, ports 26-50). Also, note that the maximum number of classes that can be applied to a policy map is 16.

  Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the “Burst” field, and the average rate tokens are removed from the bucket is by specified by the “Rate” option.
- After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy to take effect.

Command Attributes

Policy Map

- **Modify Name and Description** – Configures the name and a brief description of a policy map. (Range: 1-16 characters for the name; 1-64 characters for the description)
- **Edit Classes** – Opens the “Policy Rule Settings” page for the selected class entry. Modify the criteria used to service ingress traffic on this page.
- **Add Policy** – Opens the “Policy Configuration” page. Enter a policy name and description on this page, and click Add to open the “Policy Rule Settings” page. Enter the criteria used to service ingress traffic on this page.
- **Remove Policy** – Deletes a specified policy.

Policy Configuration

- **Policy Name** – Name of the policy map. (Range: 1-16 characters)

- **Description** – A brief description of a policy map. (Range: 1-64 characters)
- **Add** – Adds the specified policy.
- **Back** – Returns to previous page without making any changes.

Policy Rule Settings

- Class Settings -

- **Class Name** – Name of class map.
- **Action** – Shows the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on 3-154).
- **Meter** – The maximum throughput and burst rate.
  - **Rate (kbps)** – Rate in kilobits per second.
  - **Burst (byte)** – Burst in bytes.
- **Exceed Action** – Specifies whether the traffic that exceeds the specified rate will be dropped or the DSCP service level will be reduced.
- **Remove Class** – Deletes a class.

- Policy Settings -

- Class Name – Name of class map.
- **Action** – Configures the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on page 3-147). (Range - CoS: 0-7, DSCP: 0-63, IP Precedence: 0-7, IPv6 DSCP: 0-63)
- **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.
  - **Rate (kbps)** – Rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
  - **Burst (byte)** – Burst in bytes. (Range: 64-1522)
- **Exceed** – Specifies whether the traffic that exceeds the specified rate or burst will be dropped or the DSCP service level will be reduced.
  - **Set** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)
  - **Drop** – Drops out of conformance traffic.
- **Add** – Adds specified criteria to the policy map.

Web – Click QoS, DiffServ, Policy Map to display the list of existing policy maps. To add a new policy map click Add Policy. To configure the policy rule settings click Edit Classes.

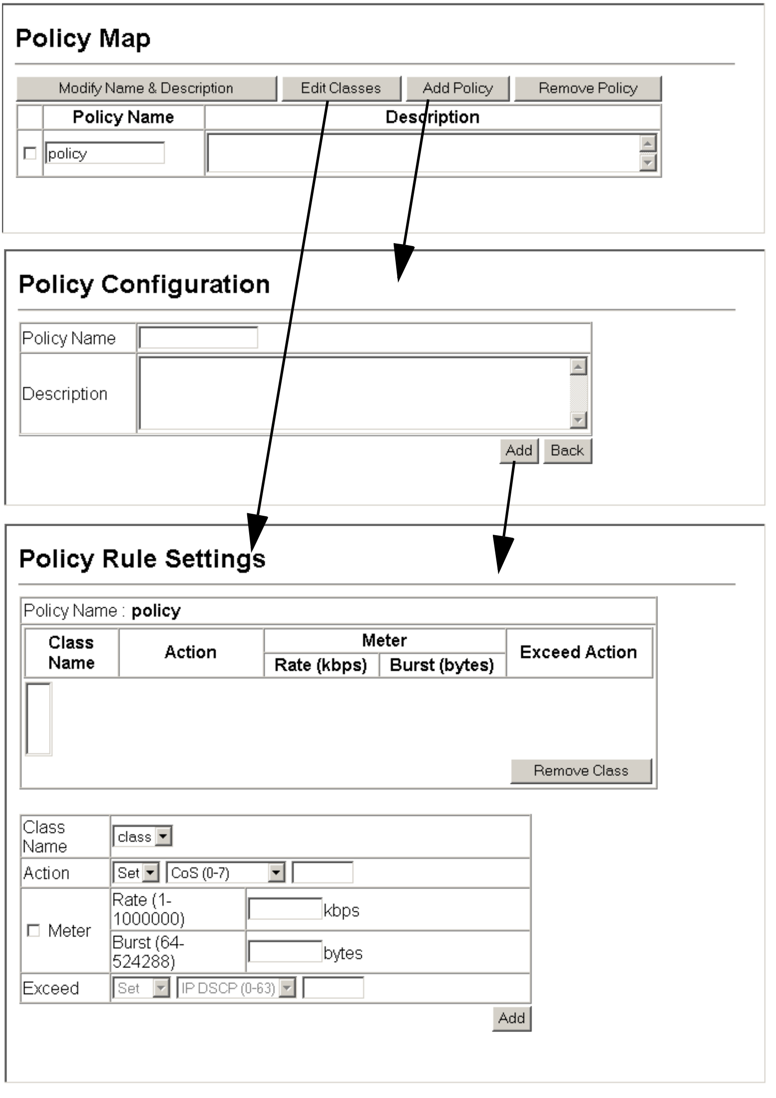


Figure 3-98. Configuring Policy Maps

CLI – This example creates a policy map called “rd-policy,” sets the average bandwidth the 1 Mbps, the burst rate to 1522 bps, and the response to reduce the DSCP value for violating packets to 0.

```
Console(config)#policy-map rd_policy#3
Console(config-pmap)#class rd_class#3
Console(config-pmap-c)#set ip dscp 4
Console(config-pmap-c)#police 100000 1522 exceed-action
  set ip dscp 0
Console(config-pmap-c)#
```

Attaching a Policy Map to Ingress Queues

This function binds a policy map to the ingress queue of a particular interface.

Command Usage

- You must first define a class map, then define a policy map, and finally bind the service policy to the required interface.
- You can only bind one policy map to an interface.
- The current firmware does not allow you to bind a policy map to an egress queue.

Command Attributes

- **Ports** – Specifies a port.
- **Ingress** – Applies the rule to ingress traffic.
- **Enabled** – Check this to enable a policy map on the specified port.
- **Policy Map** – Select the appropriate policy map from the scroll-down box.

Web – Click QoS, DiffServ, Service Policy. Check Enabled and choose a Policy Map for a port from the scroll-down box, then click Apply.

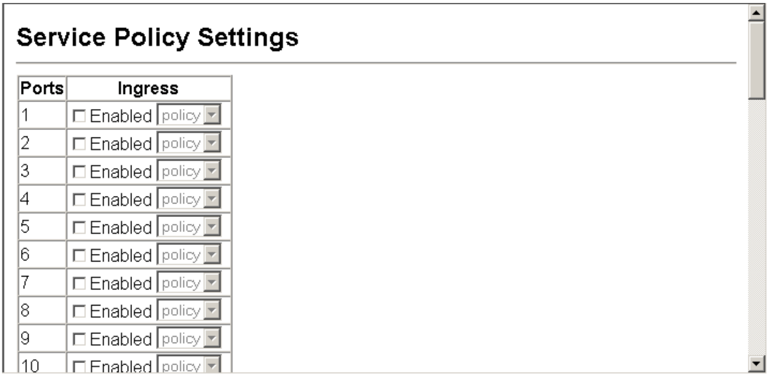
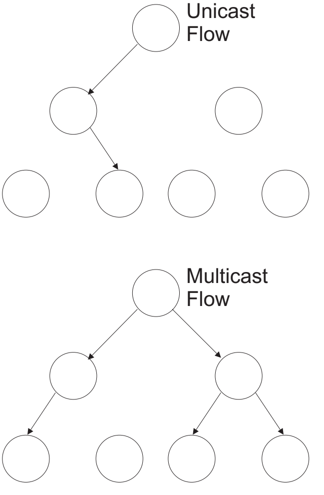


Figure 3-99. Service Policy Settings

CLI – This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/5
Console(config-if)#service-policy input rd_policy#3
Console(config-if)#
```

Multicast Filtering



Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. This procedure is called multicast filtering.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

This switch not only supports IP multicast filtering by passively monitoring IGMP query and report messages and multicast routing probe messages to register end-stations as multicast group members, but also supports the DVMRP and PIM-DM multicast routing protocols required to forward multicast traffic to other subnets (page 3-157 and 3-163).

IGMP Protocol

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately adjacent multicast router/switch. IGMP is a multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any adjacent multicast switch/router to ensure that it will continue to receive the multicast service.

Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Note that IGMP neither alters nor routes IP multicast packets. A multicast routing protocol must be used to deliver IP multicast packets across different subnetworks. Therefore, when DVMRP or PIM routing is enabled for a subnet on this switch, you also need to enable IGMP.

Layer 2 IGMP (Snooping and Query)

IGMP Snooping and Query — If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query (page 3-162) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic.

Static IGMP Router Interface — If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 3-165). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface — For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (page 3-167).

IGMP Query (Layer 2 or 3) – IGMP Query can only be enabled globally at Layer 2, but can be enabled for individual VLAN interfaces at Layer 3 (page 3-99). However, note that Layer 2 query is disabled if Layer 3 query is enabled.

Configuring IGMP Snooping and Query Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- **IGMP Snooping** — This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

- **IGMP Querier** — A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

- **IGMP Status** — When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Enabled)
- **Act as IGMP Querier** — When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Enabled)
- **IGMP Query Count** — Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10, Default: 2)
- **IGMP Query Interval** — Sets the frequency at which the switch sends IGMP host-query messages.
  (Range: 60-125 seconds, Default: 125)
- **IGMP Report Delay** — Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 5-25 seconds, Default: 10)
- **IGMP Query Timeout** — The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500 seconds, Default: 300)
- **IGMP Version** — Sets the protocol version for compatibility with other devices on the network. (Range: 1-2; Default: 2)

Notes:
1. All systems on the subnet must support the same version.
2. Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.

Web – Click IGMP Snooping, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)

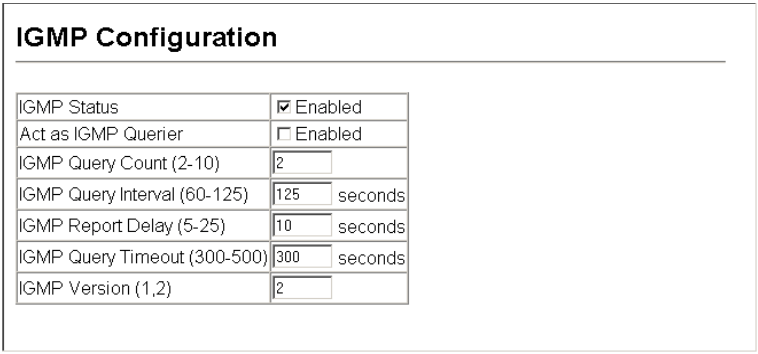


Figure 3-100. Configuring Internet Group Management Protocol

CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```
Console(config)#ip igmp snooping                                    4-178
Console(config)#ip igmp snooping querier                            4-182
Console(config)#ip igmp snooping query-count 10                     4-182
Console(config)#ip igmp snooping query-interval 100                 4-183
Console(config)#ip igmp snooping query-max-response-time 20         4-184
Console(config)#ip igmp snooping query-time-out 300                 4-185
Console(config)#ip igmp snooping version 2                          4-179
Console(config)#exit
Console#show ip igmp snooping                                       4-180
 Service status          : Enabled
 Querier status          : Enabled
 Query count             : 10
 Query interval          : 100 sec
 Query max response time : 20 sec
 Router port expire time: 300 sec
 IGMP snooping version   : Version 2
Console#
```

Displaying Interfaces Attached to a Multicast Router

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4093).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

Web – Click IGMP Snooping, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.

Figure 3-101. Mapping Multicast Switch Ports to VLANs

CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1                          4-186
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1           Eth 1/11 Static
```

Specifying Static Interfaces for a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP Snooping, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After you have finished adding interfaces to the list, click Apply.

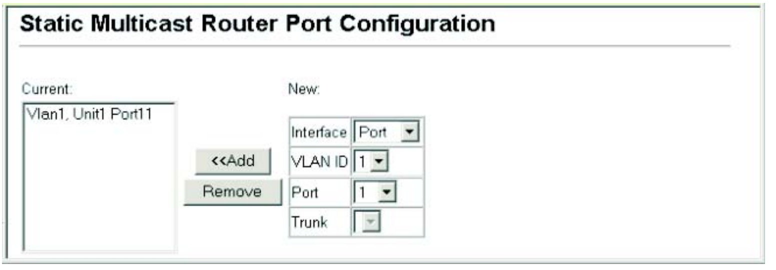


Figure 3-102. Static Multicast Router Port Configuration

CLI – This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11      4-185
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                       4-186
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1           Eth 1/11 Static
```

Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast service.

Command Attribute

- **VLAN ID** – Selects the VLAN for which to display port members.
- **Multicast IP Address** – The IP address for a specific multicast service.
- **Multicast Group Port List** – Shows the interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service.

Web – Click IGMP Snooping, IP Multicast Registration Table. Select a VLAN ID and the IP address for a multicast service from the scroll-down lists. The switch will display all the interfaces that are propagating this multicast service.

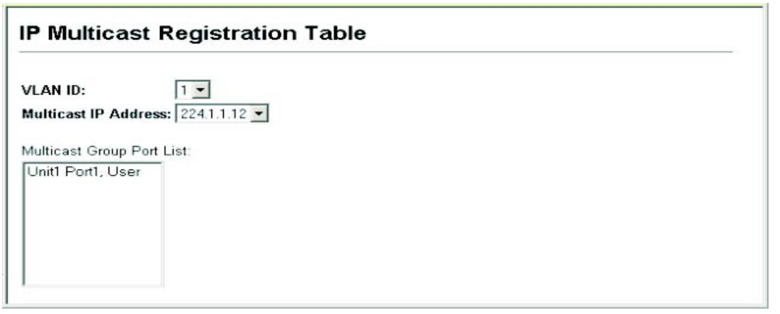


Figure 3-103. Displaying Port Members of Multicast Services

CLI – This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The Type field shows if this entry was learned dynamically or was statically configured.

```
Console#show bridge 1 multicast vlan 1                                  4-181
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

Assigning Ports to Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in "Configuring IGMP Snooping and Query Parameters" on page 3-162. For certain applications that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attribute

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch.
- **Multicast IP** – The IP address for a specific multicast service.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router/switch.

Web – Click IGMP Snooping, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and click Add. After you have completed adding ports to the member list, click Apply.

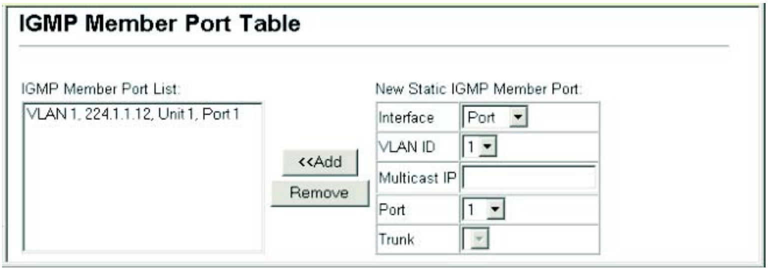


Figure 3-104. Specifying Multicast Port Membership

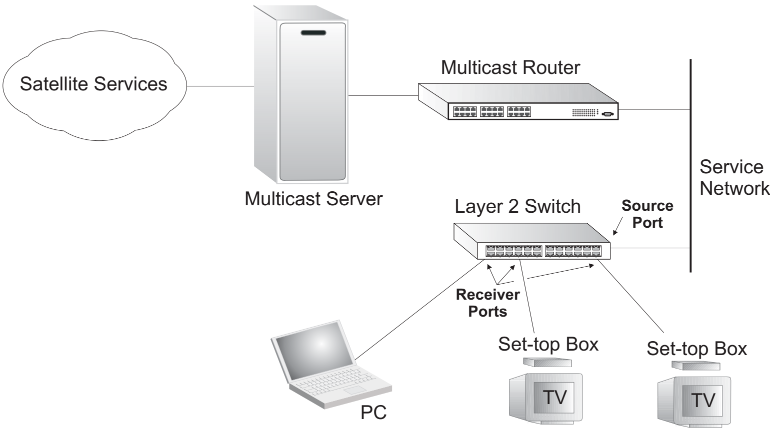
CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12
ethernet 1/12                                                      4-179
Console(config)#exit
Console#show mac-address-table multicast vlan 1                    4-181
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

Multicast VLAN Registration

Multicast VLAN Registration (MVR) is a protocol that controls access to a single network-wide VLAN most commonly used for transmitting multicast traffic (such as television channels or video-on-demand) across a service provider’s network. Any multicast traffic entering an MVR VLAN is sent to all attached subscribers. This protocol can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. This makes it possible to support common multicast services over a wide part of the network without having to use any multicast routing protocol.

MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).



General Configuration Guidelines for MVR

1. Enable MVR globally on the switch, select the MVR VLAN, and add the multicast groups that will stream traffic to attached hosts (see “Configuring Global MVR Settings” on page 3-169).

2. Set the interfaces that will join the MVR as source ports or receiver ports (see “Configuring MVR Interface Status” on page 3-172).

3. Enable IGMP Snooping to a allow a subscriber to dynamically join or leave an MVR group (see “Configuring IGMP Snooping and Query Parameters” on page 3-162). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

4. For multicast streams that will run for a long term and be associated with a stable set of hosts, you can statically bind the multicast group to the participating interfaces (see “Assigning Static Multicast Groups to Interfaces” on page 3-174).

Configuring Global MVR Settings

The global settings for Multicast VLAN Registration (MVR) include enabling or disabling MVR for the switch, selecting the VLAN that will serve as the sole channel for common multicast streams supported by the service provider, and assigning the multicast group address for each of these services to the MVR VLAN.

Command Attributes

- **MVR Status** – When MVR is enabled on both the switch, any multicast data associated an MVR group is sent from all designated source ports, and to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)

- **MVR Running Status** – Indicates whether or not all necessary conditions in the MVR environment are satisfied.
- **MVR VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR. (Range: 1-4093; Default: 1)
- **MVR Group IP** – IP address for an MVR multicast group. The IP address range of 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x. (Range: 224.0.1.0 - 239.255.255.255; Default: no groups are assigned to the MVR VLAN)
- **Count** – The number of contiguous MVR group addresses. (Range: 1-255; Default: 0)

Web – Click MVR, Configuration. Enable MVR globally on the switch, select the MVR VLAN, add the multicast groups that will stream traffic to attached hosts, and then click Apply.

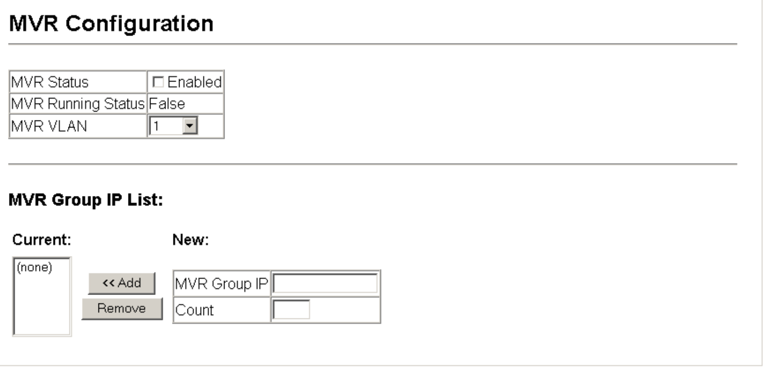


Figure 3-105. MVR Global Configuration

CLI – This example first enables IGMP snooping, enables MVR globally, and then configures a range of MVR group addresses.

```
Console(config)#ip igmp snooping                                      4-178
Console(config)#mvr                                                   4-194
Console(config)#mvr group 228.1.23.1 10                               4-194
Console(config)#
```

Displaying MVR Interface Status

You can display information about the interfaces attached to the MVR VLAN.

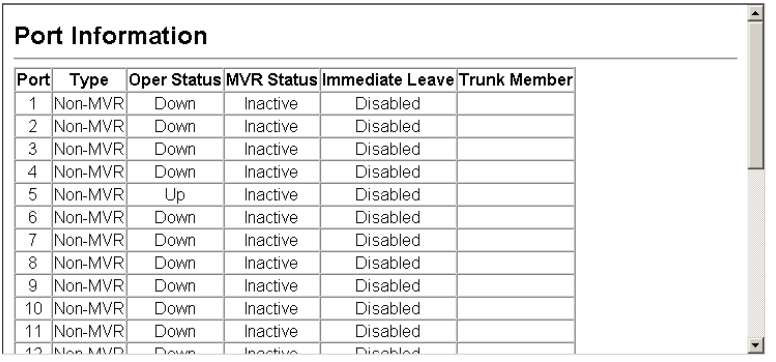
Field Attributes

- **Type** – Shows the MVR port type.
- **Oper Status** – Shows the link status.
- **MVR Status** – Shows the MVR status. MVR status for source ports is “ACTIVE” if MVR is globally enabled on the switch. MVR status for receiver ports is “ACTIVE”

only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.

- **Immediate Leave** – Shows if immediate leave is enabled or disabled.
- **Trunk Member** – Shows if port is a trunk member (Port Information only).

Web – Click MVR, Port or Trunk Information.



Port	Type	Oper Status	MVR Status	Immediate Leave	Trunk Member
1	Non-MVR	Down	Inactive	Disabled	
2	Non-MVR	Down	Inactive	Disabled	
3	Non-MVR	Down	Inactive	Disabled	
4	Non-MVR	Down	Inactive	Disabled	
5	Non-MVR	Up	Inactive	Disabled	
6	Non-MVR	Down	Inactive	Disabled	
7	Non-MVR	Down	Inactive	Disabled	
8	Non-MVR	Down	Inactive	Disabled	
9	Non-MVR	Down	Inactive	Disabled	
10	Non-MVR	Down	Inactive	Disabled	
11	Non-MVR	Down	Inactive	Disabled	

Figure 3-106. MVR Port Information

CLI – This example shows information about interfaces attached to the MVR VLAN.

```
Console#show mvr interface                                          4-197
Port    Type     Status        Immediate Leave
------- -------- ------------- ---------------
eth1/1  SOURCE   ACTIVE/UP     Disable
eth1/2  RECEIVER ACTIVE/UP     Disable
Console#
```

Displaying Port Members of Multicast Groups

You can display the multicast groups assigned to the MVR VLAN either through IGMP snooping or static configuration.

Field Attributes

- **Group IP** – Multicast groups assigned to the MVR VLAN.
- **Group Port List** – Shows the interfaces with subscribers for multicast services provided through the MVR VLAN.

Web – Click MVR, Group IP Information.

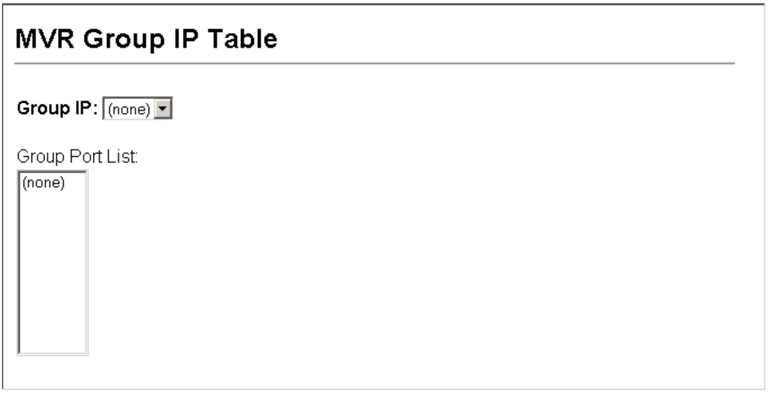


Figure 3-107. MVR Group IP Information

CLI – This example following shows information about the interfaces associated with multicast groups assigned to the MVR VLAN.

```
Console#show mvr interface                                             4-197
MVR Group IP     Status   Members
---------------- -------- -------
225.0.0.1        ACTIVE   eth1/1(d), eth1/2(s)
225.0.0.2        INACTIVE None
225.0.0.3        INACTIVE None
225.0.0.4        INACTIVE None
225.0.0.5        INACTIVE None
225.0.0.6        INACTIVE None
225.0.0.7        INACTIVE None
225.0.0.8        INACTIVE None
225.0.0.9        INACTIVE None
225.0.0.10       INACTIVE None
Console#
```

Configuring MVR Interface Status

Each interface that participates in the MVR VLAN must be configured as an MVR source port or receiver port. If only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

Command Usage

- One or more interfaces may be configured as MVR source ports.
- MVR receiver ports cannot be members of a trunk. Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN.
- IGMP snooping can be used to allow a source port or receiver port to dynamically join or leave multicast groups within the MVR VLAN using the standard rules for multicast filtering. Multicast groups can also be statically assigned to a source port

or receiver port (see “Assigning Static Multicast Groups to Interfaces” on page 3-174).

- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list. Using immediate leave can speed up leave\ latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface. Note that immediate leave does not apply to multicast groups which have been statically assigned to a port.

Command Attributes

- **MVR Type** – The following interface types are supported:
  - Source – An uplink port that can send and receive multicast data for the groups assigned to the MVR VLAN.
  - Receiver – A subscriber port that can receive multicast data sent through the MVR VLAN.
  - Non-MVR – An interface that does not participate in the MVR VLAN. (This is the default type.)
- **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group.
- **Trunk** – Shows if port is a trunk member (Port Configuration only).

Web – Click MVR, Port or Trunk Configuration.

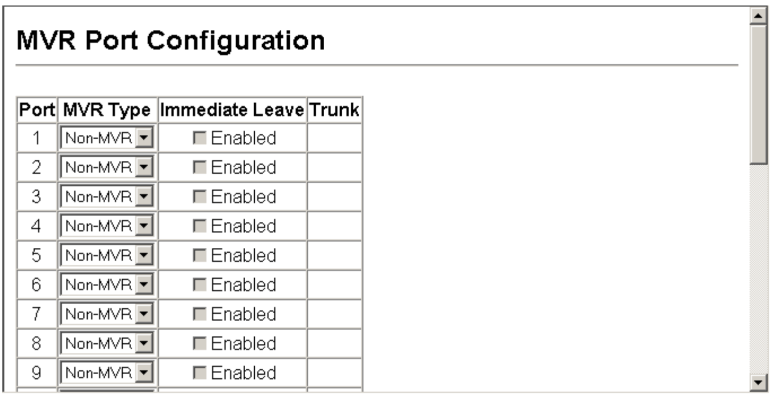


Figure 3-108. MVR Port Configuration

CLI – This example configures an MVR source port and receiver port, and then enables immediate leave on the receiver port.

```
Console(config)#interface ethernet 1/1
Console(config-if)#mvr type source                                    4-195
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#mvr type receiver                                  4-195
Console(config-if)#mvr immediate                                      4-195
Console(config-if)#
```

Assigning Static Multicast Groups to Interfaces

For multicast streams that will run for a long term and be associated with a stable set of hosts, you can statically bind the multicast group to the participating interfaces.

Command Usage

- Any multicast groups that use the MVR VLAN must be statically assigned to it under the MVR Configuration menu (see“Configuring Global MVR Settings” on page 3-169).
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

Command Attributes

- **Interface** – Indicates a port or trunk.
- **Member** – Shows the IP addresses for MVR multicast groups which have been statically assigned to the selected interface.
- **Non-Member** – Shows the IP addresses for all MVR multicast groups which have not been statically assigned to the selected interface.

Web – Click MVR, Group Member Configuration. Select a port or trunk from the “Interface” field, and click Query to display the assigned multicast groups. Select a multicast address from the displayed lists, and click the Add or Remove button to modify the Member list.

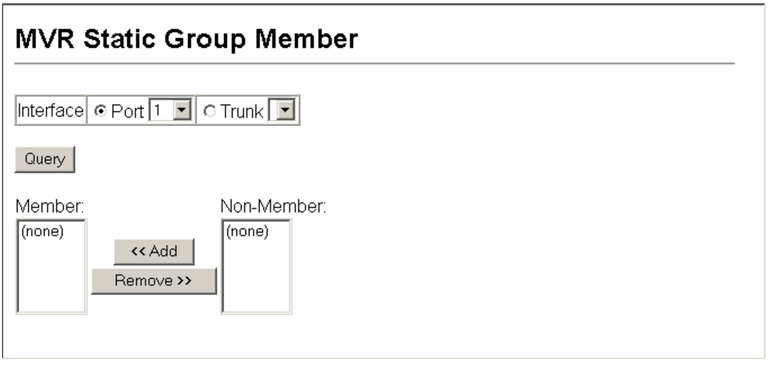


Figure 3-109. MVR Group Member Configuration

CLI – This example statically assigns a multicast group to a receiver port.

```
Console(config)#interface ethernet 1/2
Console(config-if)#mvr group 228.1.23.1                                   4-195
Console(config-if)#
```

DHCP Snooping

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

Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall. When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.

When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

Filtering rules are implemented as follows:

- If the global DHCP snooping is disabled, all DHCP packets are forwarded.
- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.
- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:
  - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
  - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
  - If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
  - If the DHCP packet is not a recognizable type, it is dropped.
- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

Additional considerations when the switch itself is a DHCP client – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

DHCP Snooping Configuration

Command Attributes

- **DHCP Snooping Status** – Enables or disables DHCP snooping globally.
- **DHCP Snooping MAC-Address Verification** – Enables or disables MAC address verification. DHCP packets will be dropped if the source MAC address in the Ethernet header of the packet is not same as the client’s hardware address in the DHCP packet.

Web – Click DHCP Snooping, Configuration.

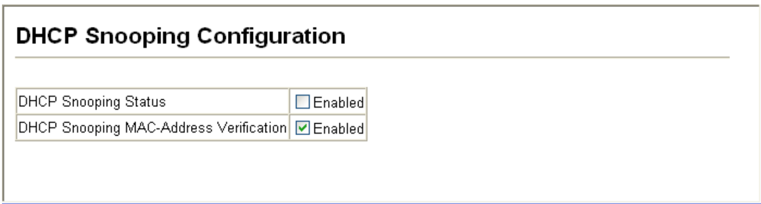


Figure 3-110. DHCP Snooping Configuration

CLI – This example first enables DHCP Snooping, and then enables DHCP Snooping MAC-Address Verification.

```
Console(config)#ip dhcp snooping                                      4-228
Console(config)#ip dhcp snooping verify mac-address                   4-231
Console(config)#
```

DHCP Snooping VLAN Configuration

Enables DHCP snooping on the specified VLAN.

Command Attributes

- **VLAN ID** – ID of a configured VLAN. (Range: 1-4093)
- **DHCP Snooping Status** – Enables or disables DHCP snooping for the selected VLAN. When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.

Web – Click DHCP Snooping, VLAN Configuration.

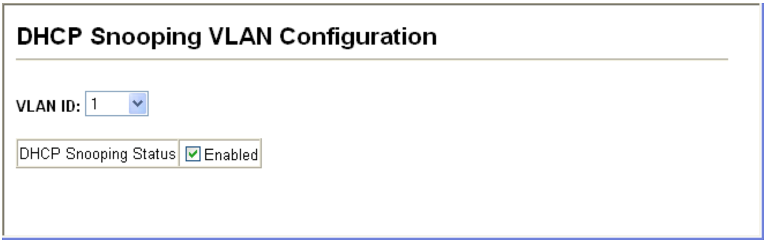


Figure 3-111. DHCP Snooping VLAN Configuration

CLI – This example first enables DHCP Snooping for VLAN 1.

```
Console(config)#ip dhcp snooping vlan 1                              4-230
Console(config)#
```

DHCP Snooping Information Option Configuration

DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. Known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients.

When the DHCP Snooping Information Option is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCP client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.

In some cases, the switch may receive DHCP packets from a client that already includes DHCP Option 82 information. The switch can be configured to set the action policy for these packets. Either the switch can discard the Option 82 information, keep the existing information, or replace it with the switch’s relay information.

Note: DHCP snooping must be enabled on the switch for the DHCP Option 82 information to be inserted into packets.

Command Attributes

- **DHCP Snooping Information Option Status** – Enables or disables DHCP Option 82 information relay.
- **DHCP Snooping Information Option Policy** – Sets the DHCP snooping information option policy for DHCP client packets that include Option 82 information.
  - **Replace** – Overwrites the DHCP client packet information with the switch’s relay information.
  - **Keep** – Retains the client’s DHCP information.

- **Drop** – Discards the Option 82 information in a packet and then floods it to the entire VLAN.

Web – Click DHCP Snooping, Information Option Configuration.

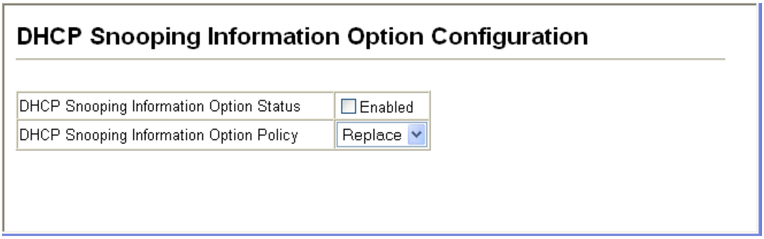


Figure 3-112. DHCP Snooping Information Option Configuration

CLI – This example enables DHCP Snooping Information Option, and sets the policy as replace.

```
Console(config)#ip dhcp snooping information option                 4-232
Console(config)#ip dhcp snooping information policy replace         4-233
Console(config)#
```

DHCP Snooping Port Configuration

Configures switch ports as trusted or untrusted. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

Command Attributes

- **Trust Status** – Enables or disables port as trusted.

Web – Click DHCP Snooping, Information Option Configuration.

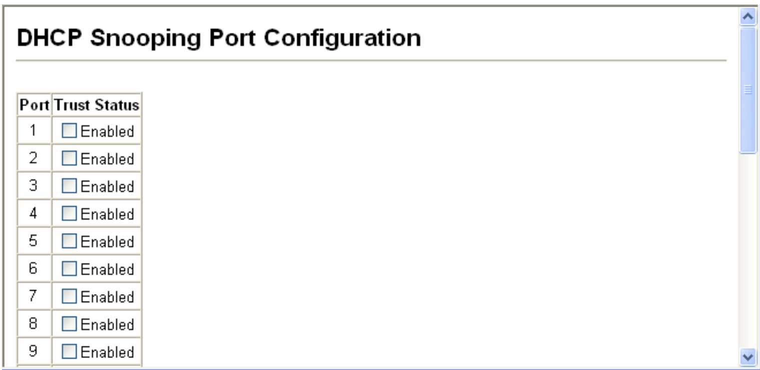


Figure 3-113. DHCP Snooping Port Configuration

CLI – This example shows how to enable the DHCP Snooping Trust Status for ports.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip dhcp snooping trust                              4-230
Console(config-if)#
```

DHCP Snooping Binding Information

Displays the DHCP snooping binding information.

Command Attributes

- **No.** – Entry number for DHCP snooping binding information.
- **Unit** – Stack unit.
- **Port** – Port number.
- **VLAN ID** – ID of a configured VLAN (Range: 1-4093)
- **MAC Address** – A valid unicast MAC address.
- **IP Address** – A valid unicast IP address.
- **IP Address Type** – Indicates an IPv4 or IPv6 address type.
- **Lease Time (Seconds)** – The time after which an entry is removed from the table.

Web – Click DHCP Snooping, DHCP Snooping Binding Information.

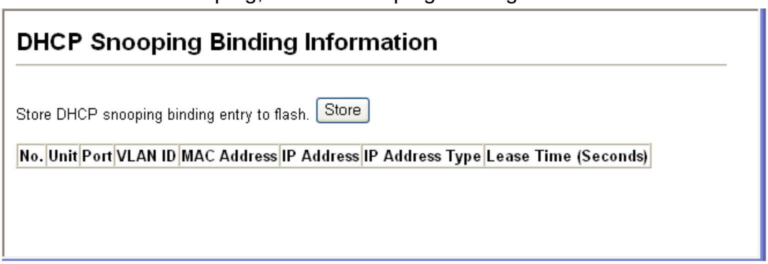


Figure 3-114. DHCP Snooping Binding Information

CLI – This example shows how to display the DHCP Snooping binding table entries.

```
Console#show ip dhcp snooping binding                                  4-234
MacAddress        IpAddress       Lease(sec) Type                 VLAN
Interface
----------------- --------------- ---------- -------------------- ----
---------
11-22-33-44-55-66 192.168.0.99             0 Dynamic                 1
Eth 1/5
Console#
```

IP Source Guard

IP Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or static and dynamic entries in the DHCP Snooping table when enabled (see "DHCP Snooping" on page 3-175). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands used to configure IP Source Guard.

IP Source Guard Port Configuration

IP Source Guard is used to filter traffic on an unsecure port which receives messages from outside the network or firewall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.

When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping or static addresses configured in the source guard binding table. An inbound packet's IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) are checked against the binding table. If no matching entry is found, the packet is dropped.

Command Attributes

- **Filter Type** – Configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. (Default: None)
  - **None** – Disables IP source guard filtering on the port.
  - **SIP** – Enables traffic filtering based on IP addresses stored in the binding table.
  - **SIP-MAC** – Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.

Web – Click IP Source Guard, Port Configuration.

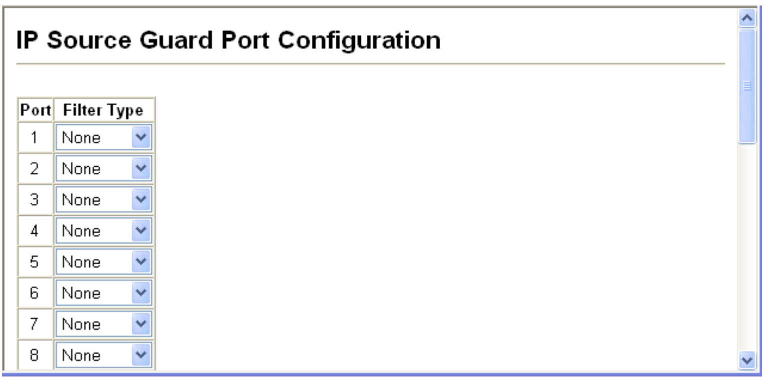


Figure 3-115. IP Source Guard Port Configuration

CLI – This example shows how to enable IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip                                   4-224
Console(config-if)#end
Console#show ip source-guard                                             4-227
Interface   Filter-type
---------   -----------
Eth 1/1     DISABLED
Eth 1/2     DISABLED
Eth 1/3     DISABLED
Eth 1/4     DISABLED
Eth 1/5     SIP
Eth 1/6     DISABLED
.
.
```

Static IP Source Guard Binding Configuration

Adds a static addresses to the source-guard binding table. Table entries include a MAC address, IP address, lease time, entry type (Static, Dynamic), VLAN identifier, and port identifier. All static entries are configured with an infinite lease time, which is indicated with a value of zero in the table.

Command Attributes

- **Static Binding Table Counts** – The total number of static entries in the table.
- **Current Static Binding Table** – The list of current static entries in the table.
- **Port** – Switch port number. (Range: 1-28)
- **VLAN ID** – ID of a configured VLAN (Range: 1-4093)
- **MAC Address** – A valid unicast MAC address.
- **IP Address** – A valid unicast IP address, including classful types A, B or C.

Web – Click IP Source Guard, Static Configuration.

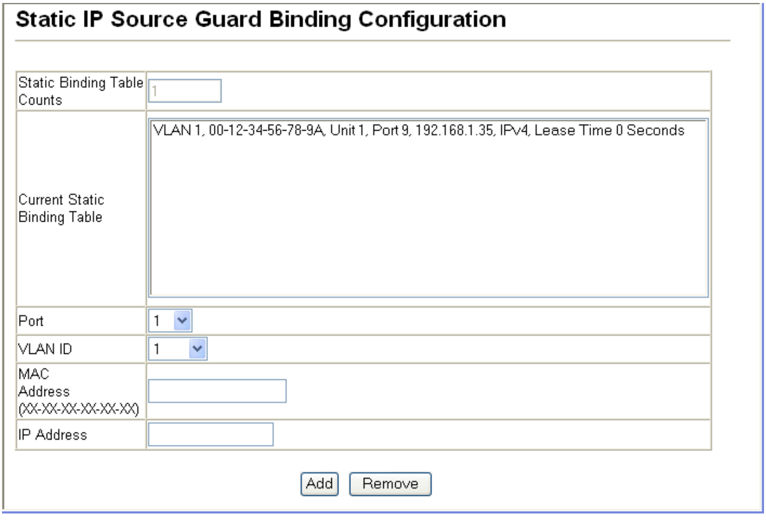


Figure 3-116. Static IP Source Guard Binding Configuration

CLI – This example shows how to configure a static source-guard binding on port 5.

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1
192.168.0.99 interface ethernet 1/5                                4-225
Console(config)#
```

Dynamic IP Source Guard Binding Information

Displays the source-guard binding table for a selected interface.

Command Attributes

- **Query by** – Select an interface to display the source-guard binding. (Options: Port, VLAN, MAC Address, or IP Address)
- **Dynamic Binding Table Counts** – Displays the number of IP addresses in the source-guard binding table.
- **Current Dynamic Binding Table** – Displays the IP addresses in the source-guard binding table.

Web – Click IP Source Guard, Dynamic Information.

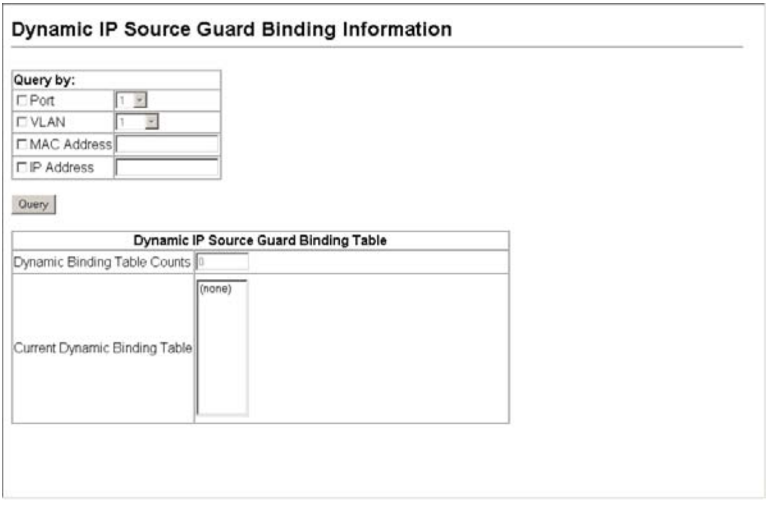


Figure 3-117. Dynamic IP Source Guard Binding Information

CLI – This example shows how to configure a static source-guard binding on port 5.

```
Console#show ip source-guard binding                                    4-227
MacAddress        IpAddress       Lease(sec) Type                   VLAN
Interface
----------------- --------------- ---------- --------------------- ----
--------
11-22-33-44-55-66 192.168.0.99             0 Static                   1 Eth 1/
5
Console#
```

Switch Clustering

Switch Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

A switch cluster has a “Commander” unit that is used to manage all other “Member” switches in the cluster. The management station uses Telnet to communicate directly with the Commander throught its IP address, and the Commander manages Member switches using cluster “internal” IP addresses. There can be up to 36 Member switches in one cluster. Cluster switches are limited to within a single IP subnet.

Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.

Note: Cluster Member switches can be managed through only using a Telnet connection to the Commander. From the Commander CLI prompt, use the “rcommand” command (see page 4-238) to connect to the Member switch.

Cluster Configuration

To create a switch cluster, first be sure that clustering is enabled on the switch (the default is enabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

Command Attributes

- **Cluster Status** – Enables or disables clustering on the switch.
- **Cluster Commander** – Enables or disables the switch as a cluster Commander.
- **Role** – Indicates the current role of the switch in the cluster; either Commander, Member, or Candidate.
- **Cluster IP Pool** – An “internal” IP address pool that is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.*x.x.member-ID*. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36. Note that you cannot change the cluster IP pool when the switch is currently in Commander mode. Commandoer mode must first be disabled.
- **Number of Members** – The current number of Member switches in the cluster.
- **Number of Candidates** – The current number of Candidate switches discovered in the network that are available to become Members.

Web – Click Cluster, Configuration.

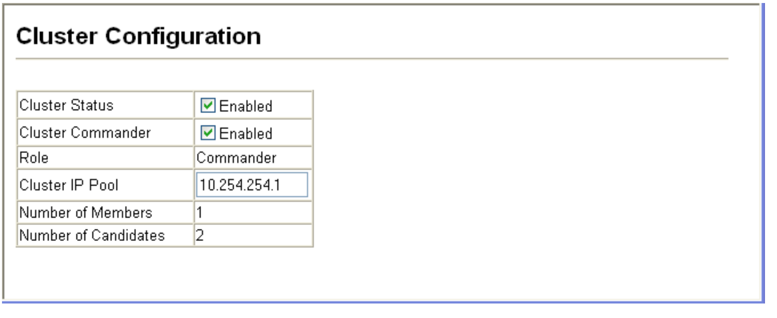


Figure 3-118. Cluster Configuration

CLI – This example first enables clustering on the switch, sets the switch as the cluster Commander, and then configures the cluster IP pool.

```
Console(config)#cluster                                    4-235
Console(config)#cluster commander                          4-236
Console(config)#cluster ip-pool 10.2.3.4                   4-236
Console(config)#
```

Cluster Member Configuration

Adds Candidate switches to the cluster as Members.

Command Attributes

- **Member ID** – Specify a Member ID number for the selected Candidate switch. (Range: 1-36)
- **MAC Address** – Select a discoverd switch MAC address from the Candidate Table, or enter a specific MAC address of a known switch.

Web – Click Cluster, Member Configuration.

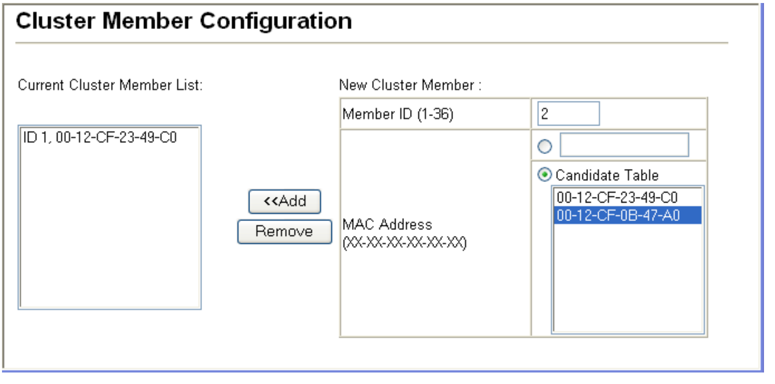


Figure 3-119. Cluster Member Configuration

CLI – This example creates a new cluster Member by specifying the Candidate switch MAC address and setting a Member ID.

```
Console(config)#cluster member mac-address 00-12-34-56-78-9a id 5   4-237
Console(config)#
```

Cluster Member Information

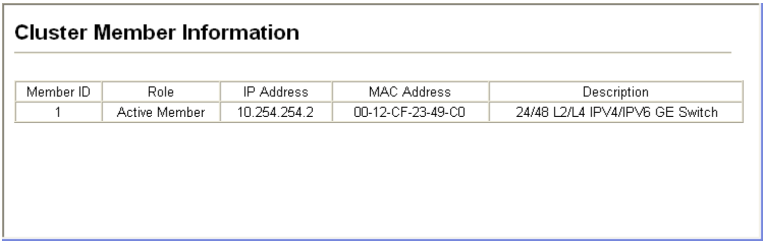
Displays current cluster Member switch information.

Command Attributes

- **Member ID** – The ID number of the Member switch. (Range: 1-36)
- **Role** – Indicates the current status of the switch in the cluster.
- **IP Address** – The internal cluster IP address assigned to the Member switch.
- **MAC Address** – The MAC address of the Member switch.

- **Description** – The system description string of the Member switch.

Web – Click Cluster, Member Information.



Cluster Member Information

Member ID	Role	IP Address	MAC Address	Description
1	Active Member	10.254.254.2	00-12-CF-23-49-C0	24/48 L2/L4 IPV4/IPV6 GE Switch

Figure 3-120. Cluster Member Information

CLI – This example shows information about cluster Member switches.

```
Console#show cluster members                                          4-239
Cluster Members:
ID:          1
Role:        Active member
IP Address:  10.254.254.2
MAC Address: 00-12-cf-23-49-c0
Description: 24/48 L2/L4 IPV4/IPV6 GE Switch
Console#
```

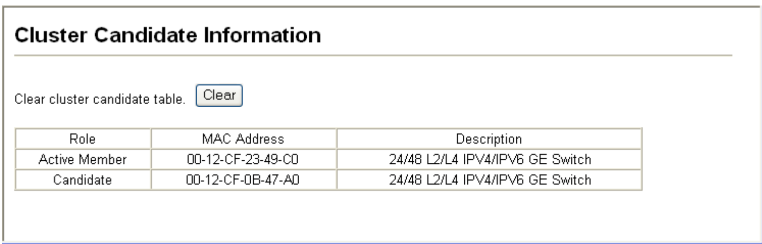
Cluster Candidate Information

Displays information about discovered switches in the network that are already cluster Members or are available to become cluster Members.

Command Attributes

- Clear – Click the Clear button to clear the cluster candidate table.
- **Role** – Indicates the current status of Candidate switches in the network.
- **MAC Address** – The MAC address of the Candidate switch.
- **Description** – The system description string of the Candidate switch.

Web – Click Cluster, Candidate Information.



Cluster Candidate Information

Clear cluster candidate table. Clear

Role	MAC Address	Description
Active Member	00-12-CF-23-49-C0	24/48 L2/L4 IPV4/IPV6 GE Switch
Candidate	00-12-CF-0B-47-A0	24/48 L2/L4 IPV4/IPV6 GE Switch

Figure 3-121. Cluster Candidate Information

CLI – This example shows information about cluster Candidate switches.

```
Console#show cluster candidates                                      4-239
Cluster Candidates:
Role            Mac               Description
--------------- -----------------
----------------------------------------
ACTIVE MEMBER   00-12-cf-23-49-c0 24/48 L2/L4 IPV4/IPV6 GE Switch
CANDIDATE       00-12-cf-0b-47-a0 24/48 L2/L4 IPV4/IPV6 GE Switch
Console#
```

UPnP

Universal Plug and Play (UPnP) is a set of computer network protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards.

Given an IP address, the first step in UPnP networking is discovery. When a device is added to the network, the UPnP discovery protocol allows that device to advertise its services to control points on the network. Similarly, when a control point is added to the network, the UPnP discovery protocol allows that control point to search for devices of interest on the network.

The next step in UPnP networking is description. After a control point has discovered a device, the control point still knows very little about the device. For the control point to learn more about the device and its capabilities, or to interact with the device, the control point must retrieve the device's description from the URL provided by the device in the discovery message.

After a control point has retrieved a description of the device, the control point can send actions to a device's service. To do this, a control point sends a suitable control message to the control URL for the service (provided in the device description).

The next step in UPnP networking is event notification, or "eventing". A UPnP description for a service includes a list of actions the service responds to and a list of variables that model the state of the service at run time. The service publishes updates when these variables change, and a control point may subscribe to receive this information. The service publishes updates by sending event messages.

The final step in UPnP networking is presentation. If a device has a URL for presentation, then the control point can retrieve a page from this URL, load the page into a web browser, and depending on the capabilities of the page, allow a user to control the device and/or view device status. The degree to which each of these can be accomplished depends on the specific capabilities of the presentation page and device.

UPnP Configuration

This page allows you to enable or disable UPnP, and to set time out values.

Command Attributes

- **UPNP Status** – Enables/disables UPnP on the device.
- **Advertising Duration** – This sets the duration of which a device will advertise its status to the control point. (Range: 60-86400 seconds; Default: 100 seconds)
- **TTL Value** – This sets the time-to-live (ttl) value for receiving of UPnP messages on the device.

Web – Click UPNP, Configuration and enter the desired variables

Figure 3-122. UPnP Configuration

CLI – This example enables UPnP, sets the device advertise duration to 200 seconds, the device ttl to 20 seconds, and displays information about basic UPnP configuration.

```
Console(config)#upnp device                                        4-217
Console(config)#upnp device advertise duration 200                 4-218
Console(config)#upnp device ttl 20                                 4-217
Console(config)#end
Console#sh upnp                                                    4-218
UPnP global settings:
 Status:                 Enabled
 Advertise duration:     200
 TTL:                    20
Console#
```

Chapter 4: Command Line Interface

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

Using the Command Line Interface

Accessing the CLI

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

Console Connection

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

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

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

```
User Access Verification
Username: admin
Password:
      CLI session with the SMC8124PL2 is opened.
      To end the CLI session, enter [Exit].
Console#
```

Telnet Connection

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

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

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

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

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

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

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

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

      CLI session with the SMC8124PL2 is opened.
      To end the CLI session, enter [Exit].

Console#
```

Note: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

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

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

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

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

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

Minimum Abbreviation

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

Command Completion

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

Getting Help on Commands

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

Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, Interface, Line, or VLAN Database). You can also display a list of valid keywords for a specific command. For example, the command "**show ?**" displays a list of possible show commands:

```
Console#show ?
  access-group        Access groups
  access-list         Access lists
  bridge-ext          Bridge extension information
  calendar            Date and time information
  class-map           Displays class maps
  cluster             Display cluster
  dot1x               802.1x content
  garp                GARP properties
  gvrp                GVRP interface information
  history             History information
  interfaces          Interface infor
  ip                  IP information
  lacp                LACP statistics
  line                TTY line information
  lldp                LLDP
  log                 Login records
  logging             Logging setting
  mac                 MAC access list
  mac-address-table   Configuration of the address table
  management          Show management information
  map                 Maps priority
  mvr                 Show mvr interface information
  policy-map          Displays policy maps
  port                Port characteristics
  power               Show power
  protocol-vlan       Protocol-VLAN information
  public-key          Public key information
  queue               Priority queue information
  radius-server       RADIUS server information
  running-config      Information on the running configuration
  snmp                Simple Network Management Protocol statistics
  sntp                Simple Network Time Protocol configuration
  spanning-tree       Spanning-tree configuration
  ssh                 Secure shell server connections
  startup-config      Startup system configuration
  system              System information
  tacacs-server       TACACS server settings
  upnp                UPnP settings
  users               Information about terminal lines
  version             System hardware and software versions
  vlan                Virtual LAN settings
Console#show
```

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

```
Console#show interfaces ?
  counters       Information of interfaces counters
  status         Information of interfaces status
  switchport     Information of interfaces switchport
Console#
```

Partial Keyword Lookup

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

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

Negating the Effect of Commands

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

Using Command History

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

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

Understanding Command Modes

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

Table 4-1. Command Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List Interface Line VLAN Database

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

Exec Commands

When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “Console>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password “admin.” The system will now display the “Console#” command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the **enable** command, followed by the privileged level password “super” (page 4-26).

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

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

      CLI session with the SMC8124PL2 is opened.
      To end the CLI session, enter [Exit].

Console#
```

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

      CLI session with the SMC8124PL2 is opened.
      To end the CLI session, enter [Exit].

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

Configuration Commands

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

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for packet filtering.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- VLAN Configuration - Includes the command to create VLAN groups.

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

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

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

Table 4-2. Configuration Commands

Mode	Command	Prompt	Page
Line	line {console | vty}	Console(config-line)#	4-9
Access Control List	access-list ip standard access-list ip extended	Console(config-std-acl)# Console(config-ext-acl)#	4-88
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)#	4-111
VLAN	vlan database	Console(config-vlan)	4-152

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

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

Command Line Processing

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

Table 4-3. Keystroke Commands

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.

Table 4-3. Keystroke Commands (Continued)

Keystroke	Function
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

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

Table 4-4. Command Group Index

Command Group	Description	Page
Line	Sets communication parameters for the serial port and Telnet, including baud rate and console time-out	4-9
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	4-19
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information	4-23
Flash/File	Manages code image or switch configuration files	4-64
Authentication	Configures logon access using local or remote authentication; also configures port security and IEEE 802.1X port access control	4-70
Access Control List	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)	4-88
SNMP	Activates authentication failure traps; configures community access strings, and trap managers; also configures IP address filtering	4-96
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	4-111
Broadcast	Configures broadcast storm control	4-121
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	4-122
Rate Limiting	Controls the maximum rate for traffic transmitted or received on a port	4-124
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	4-125
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	4-135

Table 4-4. Command Group Index (Continued)

Command Group	Description	Page
Spanning Tree	Configures Spanning Tree settings for the switch	4-139
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs	4-152
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for the bridge extension MIB	4-165
Priority	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for TCP/UDP traffic types, and DSCP	4-169
Multicast Filtering	Configures IGMP multicast filtering, query parameters, and specifies ports attached to a multicast router	4-178
LLDP	Configures LLDP settings.	4-199
UPNP	Configures UPnP settings.	
IP Interface	Configures IP address for the switch	4-219
IP Source Guard	Configures IP source guard security.	4-223
DHCP Snooping	Configures DHCP snooping	4-227
Switch Cluster	Configures switch clustering	4-235

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

ACL (Access Control List Configuration)

GC (Global Configuration)

IC (Interface Configuration)

IPC (IGMP Profile Configuration)

LC (Line Configuration)

NE (Normal Exec)

PE (Privileged Exec)

VC (VLAN Database Configuration)

Line Commands

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

Table 4-5. Line Command Syntax

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	4-10
login	Enables password checking at login	LC	4-11

Table 4-5. Line Command Syntax

Command	Function	Mode	Page
password	Specifies a password on a line	LC	4-12
timeout login response	Sets the interval that the system waits for a login attempt	LC	4-13
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	4-13
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	4-14
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command	LC	4-15
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC	4-15
parity*	Defines the generation of a parity bit	LC	4-16
speed*	Sets the terminal baud rate	LC	4-16
stopbits*	Sets the number of the stop bits transmitted per byte	LC	4-17
disconnect	Terminates a line connection	PE	4-17
show line	Displays a terminal line's parameters	NE, PE	4-18

*. These commands only apply to the serial port.

line

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

Syntax

line {**console** | **vty**}

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

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

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

Example

To enter console line mode, enter the following command:

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

Related Commands

show line (4-18)

show users (4-61)

login

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

Syntax

login [**local**]

no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

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

Example

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

Related Commands

username (4-25)

password (4-12)

password

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

Syntax

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

no password

- {**0** | **7**} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

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

Example

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

Related Commands

login (4-11)

password-thresh (4-14)

timeout login response

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

Syntax

timeout login response [*seconds*]
no timeout login response

seconds - Integer that specifies the timeout interval. (Range: 0 - 300 seconds; 0: disabled)

Default Setting

- CLI: Disabled (0 seconds)
- Telnet: 600 seconds

Command Mode

Line Configuration

Command Usage

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

Example

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

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

exec-timeout

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

Syntax

exec-timeout [*seconds*]

no exec-timeout

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

Default Setting

CLI: No timeout

Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

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

Example

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

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

password-thresh

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

Syntax

password-thresh [*threshold*]

no password-thresh

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

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.
- This command applies to both the local console and Telnet connections.

Example

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

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

Related Commands

silent-time (4-15)

silent-time

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

Syntax

silent-time [*seconds*]

no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Example

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

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

Related Commands

password-thresh (4-14)

databits

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

Syntax

databits {**7** | **8**}

no databits

- 7 - Seven data bits per character.
- 8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

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

Example

To specify 7 data bits, enter this command:

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

Related Commands

parity (4-16)

parity

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

Syntax

parity {**none** | **even** | **odd**}
no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

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

Example

To specify no parity, enter this command:

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

speed

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

Syntax

speed *bps*
no speed

bps - Baud rate in bits per second.
(Options: 9600, 19200, 38400, 57600, 115200 bps, or auto)

Default Setting

auto

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported. If you select the "auto" option, the switch will automatically detect the baud rate configured on the attached terminal, and adjust the speed accordingly.

Example

To specify 57600 bps, enter this command:

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

stopbits

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

Syntax

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

- 1 - One stop bit
- 2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

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

disconnect

Use this command to terminate an SSH, Telnet, or console connection.

Syntax

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection. (Range: 0-4)

Command Mode

Privileged Exec

Command Usage

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

Example

```
Console#disconnect 1
Console#
```

Related Commands

show ssh (4-40)

show users (4-61)

show line

This command displays the terminal line’s parameters.

Syntax

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

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

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
 Console configuration:
  Password threshold:  3 times
  Interactive timeout: Disabled
  Login timeout: Disabled
  Silent time:         Disabled
  Baudrate:            auto
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout: 300 sec
Console#
```

General Commands

Table 4-6. General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	4-19
disable	Returns to normal mode from privileged mode	PE	4-20
configure	Activates global configuration mode	PE	4-20
show history	Shows the command history buffer	NE, PE	4-21
reload	Restarts the system	PE	4-21
end	Returns to Privileged Exec mode	any config. mode	4-22
exit	Returns to the previous configuration mode, or exits the CLI	any	4-22
quit	Exits a CLI session	NE, PE	4-23
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

enable

This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. (See “Understanding Command Modes” on page 4-5.)

Syntax

enable [*level*]

level - Privilege level to log into the device.

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

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the **enable password** command on page 4-26.)
- The “#” character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

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

Related Commands

disable (4-20)

enable password (4-26)

disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. (See “Understanding Command Modes” on page 4-5.)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

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

Example

```
Console#disable
Console>
```

Related Commands

enable (4-19)

configure

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, and VLAN Database Configuration. (See “Understanding Command Modes” on page 4-5.)

Default Setting

None

Command Mode

Privileged Exec

Example

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

Related Commands

end (4-22)

show history

This command shows the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

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

Example

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

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

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

Console#
```

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

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

reload

This command restarts the system.

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

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

end

This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, and VLAN Database Configuration.

Example

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

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

exit

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

Default Setting

None

Command Mode

Any

Example

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

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

Press ENTER to start session
User Access Verification

Username:
```

quit

This command exits the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

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

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

System Management Commands

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

Table 4-7. System Management Commands

Command Group	Function	Page
Device Designation	Configures information that uniquely identifies this switch	4-24
User Access	Configures the basic user names and passwords for management access	4-25
IP Filter	Configures IP addresses that are allowed management access	4-27
Web Server	Enables management access via a web browser	4-29
Telnet Server	Enables management access via Telnet	4-32

Table 4-7. System Management Commands (Continued)

Command Group	Function	Page
Secure Shell	Provides secure replacement for Telnet	4-33
Event Logging	Controls logging of error messages	4-43
SMTP Alerts	Configures SMTP email alerts	4-49
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually	4-53
System Status	Displays system configuration, active managers, and version information	4-57
Frame Size	Enables support for jumbo frames	4-63

Device Designation Commands

Table 4-8. Device Designation Commands

Command	Function	Mode	Page
prompt	Customizes the prompt used in PE and NE mode	GC	4-24
hostname	Specifies the host name for the switch	GC	4-25
snmp-server contact	Sets the system contact string	GC	4-99
snmp-server location	Sets the system location string	GC	4-99

prompt

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

Syntax

prompt *string*

no prompt

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Example

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

hostname

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

Syntax

hostname *name*

no hostname

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

Default Setting

None

Command Mode

Global Configuration

Example

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

User Access Commands

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 4-9), user authentication via a remote authentication server (page 4-70), and host access authentication for specific ports (page 4-80).

Table 4-9. User Access Commands

Command	Function	Mode	Page
username	Establishes a user name-based authentication system at login	GC	4-25
enable password	Sets a password to control access to the Privileged Exec level	GC	4-26

username

This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **no password** |
password {**0** | **7**} *password*}

no username *name*

- *name* - The name of the user.
  (Maximum length: 8 characters, case sensitive. Maximum users: 16)
- **access-level** *level* - Specifies the user level.
- The device has two predefined privilege levels:
  0: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- **password** *password* - The authentication password for the user.
  (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The factory defaults for the user names and passwords are:

Table 4-10. Default Login Settings

username	access-level	password
guest admin	0 15	guest admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*
no enable password [**level** *level*]

- **level** *level* - Level 15 for Privileged Exec. (Levels 0-14 are not used.)
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.

- *password* - password for this privilege level. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default is level 15.
- The default password is “super”

Command Mode

Global Configuration

Command Usage

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the **enable** command (page 4-19).
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable (4-19)

authentication enable (4-71)

IP Filter Commands

Table 4-11. IP Filter Commands

Command	Function	Mode	Page
management	Configures IP addresses that are allowed management access	GC	4-27
show management	Displays the switch to be monitored or configured from a browser	PE	4-28

management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

Syntax

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**} *start-address* [*end-address*]

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.

- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.
- *start-address* - A single IP address, or the starting address of a range.
- *end-address* - The end address of a range.

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.

Command Mode

Privileged Exec

Example

```
Console#show management all-client
Management Ip Filter
 Http-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 Snmp-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 Telnet-Client:
   Start ip address      End ip address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```

Web Server Commands

Table 4-12. Web Server Command

Command	Function	Mode	Page
ip http port	Specifies the port to be used by the web browser interface	GC	4-29
ip http server	Allows the switch to be monitored or configured from a browser	GC	4-30
ip http secure-server	Enables HTTPS/SSL for encrypted communications	GC	4-30
ip http secure-port	Specifies the UDP port number for HTTPS/SSL	GC	4-31

ip http port

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server (4-30)

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

[**no**] **ip http server**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (4-29)

ip http secure-server

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

Syntax

[**no**] **ip http secure-server**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https**://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x or later versions.
- The following web browsers and operating systems currently support HTTPS:

Table 4-13. HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 4.76 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 3-56. Also refer to the **copy** command on page 4-64.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port (4-31)

copy tftp https-certificate (4-64)

ip http secure-port

This command specifies the UDP port number used for HTTPS/SSL connection to the switch's web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*
no ip http secure-port

port_number – The UDP port used for HTTPS/SSL. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://***device***:***port_number*

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server (4-30)

Telnet Server Commands

Table 4-14. Telnet Server Commands

Command	Function	Mode	Page
ip telnet server	Allows the switch to be monitored or configured from Telnet	GC	4-32
ip telnet port	Specifies the port to be used by the Telnet interface	GC	4-32

ip telnet server

This command allows this device to be monitored or configured from Telnet. Use the **no** form to disable this function.

Syntax

[**no**] **ip telnet server**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet server
Console(config)#
```

ip telnet server port

This command specifies the TCP port number used by the Telnet interface. Use the **no** form to use the default port.

Syntax

[**no**] **ip telnet port** [*port-number*]

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

23

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet port 123
Console(config)#
```

Secure Shell Commands

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When a client contacts the switch via the SSH protocol, the switch uses a public-key that the client must match along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

This section describes the commands used to configure the SSH server. However, note that you also need to install an SSH client on the management station when using this protocol to configure the switch.

Note: The switch supports both SSH Version 1.5 and 2.0.

Table 4-15. Secure Shell Commands

Command	Function	Mode	Page
ip ssh server	Enables the SSH server on the switch	GC	4-35
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC	4-36
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC	4-37
ip ssh server-key size	Sets the SSH server key size	GC	4-37
copy tftp public-key	Copies the user’s public key from a TFTP server to the switch	PE	4-64
delete public-key	Deletes the public key for the specified user	PE	4-38

Table 4-15. Secure Shell Commands (Continued)

Command	Function	Mode	Page
ip ssh crypto host-key generate	Generates the host key	PE	4-38
ip ssh crypto zeroize	Clear the host key from RAM	PE	4-39
ip ssh save host-key	Saves the host key from RAM to flash memory	PE	4-39
disconnect	Terminates a line connection	PE	4-17
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	4-40
show ssh	Displays the status of current SSH sessions	PE	4-40
show public-key	Shows the public key for the specified user or for the host	PE	4-41
show users	Shows SSH users, including privilege level and public key type	PE	4-61

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the **authentication login** command on page 4-70. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the **ip ssh crypto host-key generate** command to create a host public/private key pair.

2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

3. 10.1.0.54 1024 35
   15684995401867669259333946775054617325313674890836547254
   15020245593199868544358361651999923329781766065830956
   10825913212890233 76546801726272571413428762941301196195566782
   595664104869574278881462065
   1941746772984865468615717739390164779355942303577413098022737
   087794545240839717526463580581767167095748047761117

4. Import Client's Public Key to the Switch – Use the **copy tftp public-key** command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the username command as described on page 4-25.)

The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA Version 1 key:

5. 1024 35
   134108168560989392104094492015542534763164192187295892114317388 0
   05553616163105177594083868631109291232226828519254374603100937
   187721199696317813662774141689851320491172048303392543241016379
   975923714490119380060902539484084827178194372288402533115952134
   861022902978982721353267131629432532818915045306393916643
   steve@192.168.1.19

6. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

7. Enable SSH Service – Use the **ip ssh server** command to enable the SSH server on the switch.

8. Configure Challenge-Response Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can gain access. The following exchanges take place during this process:

9. The client sends its public key to the switch.

10. The switch compares the client's public key to those stored in memory.

11. If a match is found, the switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.

12. The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.

13. The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

ip ssh server

This command enables the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

Syntax

[no] ip ssh server

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- You must generate the host key before enabling the SSH server.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

ip ssh crypto host-key generate (4-38)

show ssh (4-40)

ip ssh timeout

This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout *seconds*
no ip ssh timeout

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

exec-timeout (4-13)

show ip ssh (4-40)

ip ssh authentication-retries

This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

ip ssh authentication-retries *count*
no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (4-40)

ip ssh server-key size

This command sets the SSH server key size. Use the **no** form to restore the default setting.

Syntax

ip ssh server-key size *key-size*
no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

Default Setting

768 bits

Command Mode

Global Configuration

Command Usage

- The server key is a private key that is never shared outside the switch.
- The host key is shared with the SSH client, and is fixed at 1024 bits.

Example

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

delete public-key

This command deletes the specified user's public key.

Syntax

delete public-key *username* [**dsa** | **rsa**]

- *username* – Name of an SSH user. (Range: 1-8 characters)
- **dsa** – DSA public key type.
- **rsa** – RSA public key type.

Default Setting

Deletes both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

This command generates the host key pair (i.e., public and private).

Syntax

ip ssh crypto host-key generate [**dsa** | **rsa**]

- **dsa** – DSA (Version 2) key type.
- **rsa** – RSA (Version 1) key type.

Default Setting

Generates both the DSA and RSA key pairs.

Command Mode

Privileged Exec

Command Usage

- This command stores the host key pair in memory (i.e., RAM). Use the **ip ssh save host-key** command to save the host key pair to flash memory.

- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#
```

Related Commands

ip ssh crypto zeroize (4-39)

ip ssh save host-key (4-39)

ip ssh crypto zeroize

This command clears the host key from memory (i.e. RAM).

Syntax

ip ssh crypto zeroize [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Clears both the DSA and RSA key.

Command Mode

Privileged Exec

Command Usage

- This command clears the host key from volatile memory (RAM). Use the **no ip ssh save host-key** command to clear the host key from flash memory.
- The SSH server must be disabled before you can execute this command.

Example

```
Console#ip ssh crypto zeroize dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (4-38)

ip ssh save host-key (4-39)

no ip ssh server (4-35)

ip ssh save host-key

This command saves the host key from RAM to flash memory.

Syntax

ip ssh save host-key [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Saves both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#ip ssh save host-key dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (4-38)

show ip ssh

This command displays the connection settings used when authenticating client access to the SSH server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
SSH Enabled - version 1.99
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```

show ssh

This command displays the current SSH server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Connection Version State                Username Encryption
  0          2.0   Session-Started      admin    ctos aes128-cbc-hmac-md5
                                                 stoc aes128-cbc-hmac-md5
Console#
```

Table 4-16. show ssh - display description

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.
Encryption	The encryption method is automatically negotiated between the client and server. Options for SSHv1.5 include: DES, 3DES Options for SSHv2.0 can include different algorithms for the client-to-server (ctos) and server-to-client (stoc): aes128-cbc-hmac-sha1 aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1 3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1 aes128-cbc-hmac-md5 aes192-cbc-hmac-md5 aes256-cbc-hmac-md5 3des-cbc-hmac-md5 blowfish-cbc-hmac-md5 Terminology: DES – Data Encryption Standard (56-bit key) 3DES – Triple-DES (Uses three iterations of DES, 112-bit key) aes – Advanced Encryption Standard (160 or 224-bit key) blowfish – Blowfish (32-448 bit key) cbc – cypher-block chaining sha1 – Secure Hash Algorithm 1 (160-bit hashes) md5 – Message Digest algorithm number 5 (128-bit hashes)

show public-key

This command shows the public key for the specified user or for the host.

Syntax

show public-key [**user** [*username*]| **host**]

username – Name of an SSH user. (Range: 1-8 characters)

Default Setting

Shows all public keys.

Command Mode

Privileged Exec

Command Usage

- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

```
Console#show public-key host
Host:
RSA:
1024 65537
156849954018676692593339467750546173253136748908365472541502024559
199868544358361651999923329781766065830958610825913212890233765468017262
257141342876294130119619556678259566410486957427888146206519417467729848
546861571773939016477935594230357741309802273708779454524083971752646358
58176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv
JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjw
bvwrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
w0W
Console#
```

Event Logging Commands

Table 4-17. Event Logging Commands

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	4-43
logging history	Limits syslog messages saved to switch memory based on severity	GC	4-44
logging host	Adds a syslog server host IP address that will receive logging messages	GC	4-45
logging facility	Sets the facility type for remote logging of syslog messages	GC	4-45
logging trap	Limits syslog messages saved to a remote server based on severity	GC	4-46
clear logging	Clears messages from the logging buffer	PE	4-46
show logging	Displays the state of logging	PE	4-47
show log	Displays log messages	PE	4-48

logging on

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

Syntax

[**no**] **logging on**

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory. You can use the **logging history** command to control the type of error messages that are stored.

Example

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

Related Commands

logging history (4-44)
clear logging (4-46)

logging history

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

Syntax

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

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- *level* - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Table 4-18. Logging Levels

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

** There are only Level 2, 5 and 6 error messages for the current firmware release.*

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

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

Example

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

logging host

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

Syntax

[**no**] **logging host** *host_ip_address*

host_ip_address - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- By using this command more than once you can build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

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

logging facility

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

Syntax

[**no**] **logging facility** *type*

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

Default Setting

23

Command Mode

Global Configuration

Command Usage

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

Example

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

logging trap

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

Syntax

logging trap [*level*]

no logging trap

level - One of the level arguments listed below. Messages sent include the selected level up through level 0. (Refer to the table on page 4-44.)

Default Setting

- Disabled
- Level 7 - 0

Command Mode

Global Configuration

Command Usage

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

Example

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

clear logging

This command clears messages from the log buffer.

Syntax

clear logging [**flash** | **ram**]

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

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear logging
Console#
```

Related Commands

show log (4-48)

show logging

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

Syntax

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

- **flash** - Displays settings for storing event messages in flash memory (i.e., permanent memory).
- **ram** - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).
- **sendmail** - Displays settings for the SMTP event handler (page 4-52).
- **trap** - Displays settings for the trap function.

Default Setting

None

Command Mode

Privileged Exec

Example

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

```
Console#show logging flash
Syslog logging:           Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:           Enabled
History logging in RAM: level debugging
Console#
```

Table 4-19. show logging flash/ram - display description

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

The following example displays settings for the trap function.

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type:        Debugging messages
REMOTELOG server IP address: 1.2.3.4
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#
```

Table 4-20. show logging trap - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
REMOTELOG status	Shows if remote logging has been enabled via the **logging trap** command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the **logging facility** command.
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the **logging trap** command.
REMOTELOG server IP address	The address of syslog servers as specified in the **logging host** command.

Related Commands

show logging sendmail (4-52)

show log

This command displays the log messages stored in local memory.

Syntax

show log {**flash** | **ram**}

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

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows the event message stored in RAM.

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

SMTP Alert Commands

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

Table 4-21. SMTP Alert Commands

Command	Function	Mode	Page
logging sendmail host	Specifies SMTP servers that will be sent alert messages	GC	4-49
logging sendmail level	Sets the severity threshold used to trigger alert messages	GC	4-50
logging sendmail source-email	Sets the email address used for “From” field of alert messages	GC	4-51
logging sendmail destination-email	Specifies the email recipients of alert messages	GC	4-51
logging sendmail	Enables SMTP event handling	GC	4-52
show logging sendmail	Displays SMTP event handler settings	NE, PE	4-52

logging sendmail host

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

Syntax

[**no**] **logging sendmail host** *ip_address*

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

logging sendmail level

This command sets the severity threshold used to trigger alert messages.

Syntax

logging sendmail level *level*

level - One of the system message levels (page 4-44). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

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

Example

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

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

logging sendmail source-email

This command sets the email address used for the “From” field in alert messages.

Syntax

logging sendmail source-email email-address

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

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

logging sendmail destination-email

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

Syntax

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

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

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

logging sendmail

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

Syntax

[**no**] **logging sendmail**

Default Setting

Enabled

Command Mode

Global Configuration

Example

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

show logging sendmail

This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show logging sendmail
SMTP servers
-----------------------------------------------
192.168.1.19
SMTP minimum severity level: 7

SMTP destination email addresses
-----------------------------------------------
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enabled
Console#
```

Time Commands

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

Table 4-22. Time Commands

Command	Function	Mode	Page
sntp client	Accepts time from specified time servers	GC	4-53
sntp server	Specifies one or more time servers	GC	4-53
sntp poll	Sets the interval at which the client polls for time	GC	4-55
show sntp	Shows current SNTP configuration settings	NE, PE	4-55
clock timezone	Sets the time zone for the switch's internal clock	GC	4-56
calendar set	Sets the system date and time	PE	4-56
show calendar	Displays the current date and time setting	NE, PE	4-57

sntp client

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

Syntax

[**no**] **sntp client**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (e.g., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **sntp servers** command. It issues time synchronization requests based on the interval set via the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time:  Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

Related Commands

sntp client (4-53)

sntp poll (4-55)

show sntp (4-55)

sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

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

ip - IP address of an time server (NTP or SNTP).

(Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

Related Commands

Related Commands (4-54)

sntp poll (4-55)

show sntp (4-55)

sntp poll

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

Syntax

sntp poll *seconds*

no sntp poll

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

Default Setting

16 seconds

Command Mode

Global Configuration

Example

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

Related Commands

Related Commands (4-54)

show sntp

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

Command Mode

Normal Exec, Privileged Exec

Command Usage

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

Example

```
Console#show sntp
Current time:  Dec 23 05:13:28 2002
Poll interval: 16
Current mode:  unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

clock timezone

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

Syntax

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

- *name* - Name of timezone, usually an acronym. (Range: 1-29 characters)
- *hours* - Number of hours before/after UTC. (Range: 1-13 hours)
- *minutes* - Number of minutes before/after UTC. (Range: 0-59 minutes)
- **before-utc** - Sets the local time zone before (east) of UTC.
- **after-utc** - Sets the local time zone after (west) of UTC.

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

Related Commands

show sntp (4-55)

calendar set

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

Syntax

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

- *hour* - Hour in 24-hour format. (Range: 0 - 23)
- *min* - Minute. (Range: 0 - 59)
- *sec* - Second. (Range: 0 - 59)
- *day* - Day of month. (Range: 1 - 31)
- *month* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**
- *year* - Year (4-digit). (Range: 2001 - 2101)

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2002.

```
Console#calendar set 15 12 34 1 February 2002
Console#
```

show calendar

This command displays the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show calendar
 15:12:34 February 1 2002
Console#
```

System Status Commands

Table 4-23. System Status Commands

Command	Function	Mode	Page
show running-config	Displays the configuration data currently in use	PE	4-59
show system	Displays system information	NE, PE	4-60
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE	4-61
show version	Displays version information for the system	NE, PE	4-62

show startup-config

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

Default Setting

None

Command Mode

Privileged Exec

Command Usage

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

Example

```
Console#show startup-config
building startup-config, please wait.....
!
!
username admin access-level 15
username admin password 0 admin
!
username guest access-level 0
username guest password 0 guest
!
enable password level 15 0 super
!
snmp-server community public ro
snmp-server community private rw
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
interface vlan 1
 ip address dhcp
!
line console
!
line vty
!
end

Console#
```

Related Commands

show running-config (4-59)

show running-config

This command displays the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by “!” symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)

- VLAN configuration settings for each interface
- IP address configured for the switch
- Spanning tree settings
- Any configured settings for the console port and Telnet

Example

```
Console#show running-config
building running-config, please wait.....
!
phymap 00-30-f1-df-9c-a0 00-00-00-00-00-00 00-00-00-00-00-00
00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
00-00-00-00-00-00
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
snmp-server community public ro
snmp-server community private rw
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
.
.
.
interface vlan 1
 IP address 192.168.1.51 255.255.255.0
 IP address DHCP
!
no map IP DSCP
!
line console
!
line vty
!
end
Console#
```

show system

This command displays system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to “Displaying System Information” on page 3-10.
- The POST results should all display “PASS.” If any POST test indicates “FAIL,” contact your distributor for assistance.

Example

```
Console#show system
System description: SMC Networks SMC8124PL2
System OID string: 1.3.6.1.4.1.259.6.10.94
System Information
 System Up Time:           0 days, 0 hours, 7 minutes, and 22.65 seconds
 System Name:              [NONE]
 System Location:          [NONE]
 System Contact:           [NONE]
 MAC Address (Unit1):      00-00-35-28-00-03
 Web Server:               Enabled
 Web Server Port:          80
 Web Secure Server:        Enabled
 Web Secure Server Port:   443
 Telnet Server:            Enable
 Telnet Server Port:       23
 Jumbo Frame:              Disabled

 POST Result:
DUMMY Test 1 ................. PASS
UART Loopback Test ........... PASS
DRAM Test .................... PASS
Timer Test ................... PASS

Done All Pass.
Console#
```

show users

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

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

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

Example

```
Console#show users
 Username accounts:
  Username Privilege Public-Key
  -------- --------- ----------
     admin        15       None
     guest         0       None
     steve        15        RSA

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
  0   console    admin           0:14:14
* 1     VTY 0    admin           0:00:00    192.168.1.19
  2     SSH 1    steve           0:00:06    192.168.1.19

 Web online users:
  Line        Remote IP addr Username Idle time (h:m:s).
  ----------- -------------- -------- ------------------
 1      HTTP   192.168.1.19    admin           0:00:00

Console#
```

show version

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

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See “Displaying Switch Hardware/Software Versions” on page 3-11 for detailed information on the items displayed by this command.

Example

```
Console#show version
Unit 1
 Serial Number:
 Hardware Version:
 EPLD Version:             0.01
 Number of Ports:          28
 Main Power Status:        Up
 Redundant Power Status:   Not present

Agent (Master)
 Unit ID:                  1
 Loader Version:           1.0.0.0
 Boot ROM Version:         1.0.0.3
 Operation Code Version:   1.0.0.8

Console#
```

Frame Size Commands

Table 4-24. Frame Size Commands

Command	Function	Mode	Page
jumbo frame	Enables support for jumbo frames	GC	4-63

jumbo frame

This command enables support for jumbo frames. Use the **no** form to disable it.

Syntax

[**no**] **jumbo frame**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

- Enabling jumbo frames will limit the maximum threshold for broadcast storm control to 64 packets per second. (See the **broadcast packet-rate** command on page 4-121.)
- The current setting for jumbo frames can be displayed with the **show system** command (page 4-60).

Example

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

Flash/File Commands

These commands are used to manage the system code or configuration files.

Table 4-25. Flash/File Commands

Command	Function	Mode	Page
copy	Copies a code image or a switch configuration to or from flash memory or a TFTP server	PE	4-64
delete	Deletes a file or code image	PE	4-67
dir	Displays a list of files in flash memory	PE	4-67
whichboot	Displays the files booted	PE	4-68
boot system	Specifies the file or image used to start up the system	GC	4-69

copy

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

Syntax

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

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

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

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

copy unit file

- **file** - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.

- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **https-certificate** - Keyword that allows you to copy the HTTPS secure site certificate.
- **public-key** - Keyword that allows you to copy a SSH key from a TFTP server. (“Secure Shell Commands” on page 4-33)
- **unit** - Keyword that allows you to copy to/from a specific unit in the stack.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- Due to the size limit of the flash memory, the switch supports only two operation code files.
- The maximum number of user-defined configuration files depends on available memory.
- You can use “Factory_Default_Config.cfg” as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.
- The Boot ROM and Loader cannot be uploaded or downloaded from the TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.
- For information on specifying an https-certificate, see “Replacing the Default Secure-site Certificate” on page 3-56. For information on configuring the switch to use HTTPS/SSL for a secure connection, see “ip http server” on page 4-30.

Example

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

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

Console#
```

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

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

Console#
```

The following example shows how to download a configuration file:

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

\Write to FLASH finish.
Success.

Console#
```

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

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

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

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

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

Console#
```

delete

This command deletes a file or image.

Syntax

delete [*unit*:] *filename*

filename - Name of the configuration file or image name.
unit - Stack unit. (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.
- “Factory_Default_Config.cfg” cannot be deleted.
- A colon (:) is required after the specified unit number.

Example

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

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (4-67)

delete public-key (4-38)

dir

This command displays a list of files in flash memory.

Syntax

dir [*unit*:] [**boot-rom** | **config** | **opcode** [:*filename*]]

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file.
- **config** - Switch configuration file.
- **opcode** - Run-time operation code image file.
- *filename* - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.
- *unit* - Stack unit. (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.
- A colon (:) is required after the specified unit number.
- File information is shown below:

Table 4-26. File Directory Information

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

The following example shows how to display all file information.

```
Console#dir
                       file name      file type startup size (byte)
-------------------------------- -------------- ------- -----------
 Unit1:
                       diag_0060 Boot-Rom image       Y      111360
                       run_01642 Operation Code       N     1074304
                        run_0200 Operation Code       Y     1083008
      Factory_Default_Config.cfg    Config File       N        2574
                         startup    Config File       Y        2710
-------------------------------------------------------------------
                                        Total free space:         0
Console#
```

whichboot

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

Syntax

whichboot [*unit*]

unit - Stack unit. (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

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

```
Console#whichboot
                        file name                file type startup size
(byte)
 -------------------------------- ----------------------- -------
-----------
Unit1:
                        diag_0060          Boot-Rom image       Y
111360
                         run_0200          Operation Code       Y
1083008
                          startup             Config File       Y
2710
Console#
```

boot system

This command specifies the image used to start up the system.

Syntax

boot system [*unit*:] {**boot-rom**| **config** | **opcode**}: *filename*

The type of file or image to set as a default includes:

- **boot-rom*** - Boot ROM.
- **config*** - Configuration file.
- **opcode*** - Run-time operation code.
- *filename* - Name of the configuration file or image name.
- *unit** - Stack unit. (Range: 1-8)

* The colon (:) is required.

Default Setting

None

Command Mode

Global Configuration

Command Usage

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

Example

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

Related Commands

dir (4-67)
whichboot (4-68)

Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. You can also enable port-based authentication for network client access using IEEE 802.1X.

Table 4-27. Authentication Commands

Command Group	Function	Page
Authentication Sequence	Defines logon authentication method and precedence	4-70
RADIUS Client	Configures settings for authentication via a RADIUS server	4-72
TACACS+ Client	Configures settings for authentication via a TACACS+ server	4-76
Port Security	Configures secure addresses for a port	4-78
Port Authentication	Configures host authentication on specific ports using 802.1X	4-80

Authentication Sequence

Table 4-28. Authentication Sequence

Command	Function	Mode	Page
authentication login	Defines logon authentication method and precedence	GC	4-70
authentication enable	Defines the authentication method and precedence for command mode change	GC	4-71

authentication login

This command defines the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[**local**] [**radius**] [**tacacs**]}
no authentication login

- **local** - Use local password.
- **radius** - Use RADIUS server password.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

username - for setting the local user names and passwords (4-25)

authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the **enable** command (see page 4-19). Use the **no** form to restore the default.

Syntax

authentication enable {[**local**] [**radius**] [**tacacs**]}
no authentication enable

- **local** - Use local password only.
- **radius** - Use RADIUS server password only.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication enable radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication enable radius
Console(config)#
```

Related Commands

enable password - sets password for changing command modes (4-26)

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 4-29. RADIUS Client Commands

Command	Function	Mode	Page
radius-server host	Specifies the RADIUS server	GC	4-72
radius-server port	Sets the RADIUS server network port	GC	4-73
radius-server key	Sets the RADIUS encryption key	GC	4-74
radius-server retransmit	Sets the number of retries	GC	4-74
radius-server timeout	Sets the interval between sending authentication requests	GC	4-75
show radius-server	Shows the current RADIUS settings	PE	4-75

radius-server host

This command specifies primary and backup RADIUS servers and authentication parameters that apply to each server. Use the **no** form to restore the default values.

Syntax

radius-server host *host_ip_address*
no radius-server host

[**no**] **radius-server** *index* **host** {*host_ip_address* | *host_alias*}
[**auth-port** *auth_port*] [**timeout** *timeout*] [**retransmit** *retransmit*] [**key** *key*]

- *index* - Allows you to specific up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.
- *host_ip_address* - IP address of server.
- *host_alias* - Symbolic name of server. (Maximum length: 20 characters)
- *port_number* - RADIUS server UDP port used for authentication messages. (Range: 1-65535)
- *timeout* - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)
- *retransmit* - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)
- *key* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

- **auth-port** - 1812
- **timeout** - 5 seconds
- **retransmit** - 2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10
retransmit 5 key green
Console(config)#
```

radius-server port

This command sets the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

radius-server key

This command sets the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*
no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server

Remote RADIUS server configuration:

Global settings:
 Communication key with RADIUS server:
 Server port number:                   1812
 Retransmit times:                     2
 Request timeout:                      5

Console#
```

TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 4-30. TACACS+ Client Commands

Command	Function	Mode	Page
tacacs-server host	Specifies the TACACS+ server	GC	4-76
tacacs-server port	Specifies the TACACS+ server network port	GC	4-76
tacacs-server key	Sets the TACACS+ encryption key	GC	4-77
show tacacs-server	Shows the current TACACS+ settings	GC	4-77

tacacs-server host

This command specifies the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address - IP address of a TACACS+ server.

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server port

This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port_number*
no tacacs-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server key

This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server key *key_string*
no tacacs-server key

key_string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string.
(Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

show tacacs-server

This command displays the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address:                       10.11.12.13
 Communication key with TACACS server: *****
 Server port number:                      30
Console#
```

Port Security Commands

These commands can be used to enable port security on a port. When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Table 4-31. Port Security Commands

Command	Function	Mode	Page
port security	Configures a secure port	IC	4-78
mac-address-table static	Maps a static address to a port in a VLAN	GC	4-135
show mac-address-table	Displays entries in the bridge-forwarding database	PE	4-137

port security

This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**}
| **max-mac-count** *address-count*]

no port security [**action** | **max-mac-count**]

- **action** - Response to take when port security is violated.
  - **shutdown** - Disable port only.
  - **trap** - Issue SNMP trap message only.
  - **trap-and-shutdown** - Issue SNMP trap message and disable port.
- max-mac-count
  - *address-count* - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

Default Setting

Status: Disabled

Action: None

Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If you enable port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- First use the **port security max-mac-count** command to set the number of addresses, and then use the **port security** command to enable security on the port.
- Use the **no port security max-mac-count** command to disable port security and reset the maximum number of addresses to the default.
- You can also manually add secure addresses with the **mac-address-table static** command.
- A secure port has the following restrictions:
  - Cannot use port monitoring.
  - Cannot be a multi-VLAN port.
  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.
- If a port is disabled due to a security violation, it must be manually re-enabled using the **no shutdown** command.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

Related Commands

shutdown (4-116)

mac-address-table static (4-135)

show mac-address-table (4-137)

802.1X Port Authentication

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Table 4-32. 802.1X Port Authentication Commands

Command	Function	Mode	Page
dot1x system-auth-control	Enables dot1x globally on the switch.	GC	4-80
dot1x default	Resets all dot1x parameters to their default values	GC	4-81
dot1x max-req	Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session	IC	4-81
dot1x port-control	Sets dot1x mode for a port interface	IC	4-81
dot1x operation-mode	Allows single or multiple hosts on a dot1x port	IC	4-82
dot1x re-authenticate	Forces re-authentication on specific ports	PE	4-83
dot1x re-authentication	Enables re-authentication for all ports	IC	4-83
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	IC	4-83
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	IC	4-84
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	IC	4-84
show dot1x	Shows all dot1x related information	PE	4-85

dot1x system-auth-control

This command enables IEEE 802.1X port authentication globally on the switch. Use the **no** form to restore the default.

Syntax

[no] dot1x system-auth-control

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dot1x system-auth-control
Console(config)#
```

dot1x default

This command sets all configurable dot1x global and port settings to their default values.

Syntax

dot1x default

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*

no dot1x max-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

dot1x port-control

This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}
no dot1x port-control

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x operation-mode

This command allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

Syntax

dot1x operation-mode {**single-host** | **multi-host** [**max-count** *count*]}
no dot1x operation-mode [**multi-host max-count**]

- **single-host** – Allows only a single host to connect to this port.
- **multi-host** – Allows multiple host to connect to this port.
- **max-count** – Keyword for the maximum number of hosts.
  - *count* – The maximum number of hosts that can connect to a port. (Range: 1-1024; Default: 5)

Default

Single-host

Command Mode

Interface Configuration

Command Usage

- The “max-count” parameter specified by this command is only effective if the dot1x mode is set to “auto” by the dot1x port-control command (page 4-105).
- In “multi-host” mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)

Command Mode

Privileged Exec

Example

```
Console#dot1x re-authenticate
Console#
```

dot1x re-authentication

This command enables periodic re-authentication globally for all ports. Use the **no** form to disable re-authentication.

Syntax

[**no**] **dot1x re-authentication**

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

dot1x timeout quiet-period

This command sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

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

Default

60 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

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

Default

3600 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

dot1x timeout tx-period

This command sets the time that the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

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

Default

30 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

- **statistics** - Displays dot1x status for each port.
- interface
- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- *Global 802.1X Parameters* – Shows whether or not 802.1X port authentication is globally enabled on the switch.
- *802.1X Port Summary* – Displays the port access control parameters for each interface that has enabled 802.1X, including the following items:
  - Status– Administrative state for port access control.
  - Operation Mode–Allows single or multiple hosts (page 4-82).
  - Mode– Dot1x port control mode (page 4-81).
  - Authorized– Authorization status (yes or n/a - not authorized).
- *802.1X Port Details* – Displays the port access control parameters for each interface, including the following items:
  - reauth-enabled – Periodic re-authentication (page 4-83).
  - reauth-period – Time after which a connected client must be re-authenticated (page 4-84).
  - quiet-period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 4-83).
  - tx-period – Time a port waits during authentication session before re-transmitting EAP packet (page 4-84).
  - supplicant-timeout – Supplicant timeout.
  - server-timeout – Server timeout.
  - reauth-max – Maximum number of reauthentication attempts.
  - max-req – Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the

authentication session (page 4-81).
  - Status – Authorization status (authorized or not).
  - Operation Mode – Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.
  - Max Count – The maximum number of hosts allowed to access this port (page 4-82).
  - Port-control –Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized (page 4-81).
  - Supplicant – MAC address of authorized client.
  - Current Identifier – The integer (0-255) used by the Authenticator to identify the current authentication session.
- *Authenticator State Machine*
  - State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
  - Reauth Count – Number of times connecting state is re-entered.
- *Backend State Machine*
  - State – Current state (including request, response, success, fail, timeout, idle, initialize).
  - Request Count – Number of EAP Request packets sent to the Supplicant without receiving a response.
  - Identifier(Server) – Identifier packet received from the Authentication Server.
- *Reauthentication State Machine*
  - State – Current state (including initialize, reauthenticate).

Example

```
Console#show dot1x
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status        Operation Mode   Mode                Authorized
1/1        disabled      Single-Host      ForceAuthorized     n/a
1/2        disabled      Single-Host      ForceAuthorized     n/a
.
.
.
1/25       disabled      Single-Host      ForceAuthorized     yes
1/26       enabled       Single-Host      Auto                yes


802.1X Port Details

802.1X is enabled on port 1/1
.
.
.
802.1X is enabled on port 26
reauth-enabled:       Enable
reauth-period:        3600
quiet-period:         60
tx-period:            30
supplicant-timeout:   30
server-timeout:       10
reauth-max:           2
max-req:              2
Status                Authorized
Operation mode        Multi-Host
Max count             5
Port-control          Auto
Supplicant            00-e0-29-94-34-65
Current Identifier    3
Authenticator State Machine
State               Authenticated
Reauth Count        0

Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  2

Reauthentication State Machine
State               Initialize

Console#
```

Access Control List Commands

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, and then bind the list to a specific port.

Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

There are three filtering modes:

- Standard IP ACL mode (STD-ACL) filters packets based on the source IP address.
- Extended IP ACL mode (EXT-ACL) filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the TCP protocol is specified, then you can also filter packets based on the TCP control code.

The following restrictions apply to ACLs:

- Each ACL can have up to 60 rules.
- This switch supports ACLs for ingress filtering only. However, you can only bind one IP ACL to any port for ingress filtering. In other words, only one ACL can be bound to an interface - Ingress IP ACL.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Ingress IP ACL for ingress ports.
2. Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
3. If no explicit rule is matched, the implicit default is permit all.

Table 4-33. Access Control List Commands

Command Groups	Function	Page
IP ACLs	Configure ACLs based on IP addresses, TCP/UDP port number, protocol type, and TCP control code	4-89
ACL Information	Display ACLs and associated rules; shows ACLs assigned to each port	4-95

IP ACLs

Table 4-34. IP ACL Commands

Command	Function	Mode	Page
access-list ip	Creates an IP ACL and enters configuration mode for standard or extended IP ACLs	GC	4-89
permit, deny	Filters packets matching a specified source IP address	STD-ACL	4-90
permit, deny	Filters packets meeting the specified criteria, including source and destination IP address, TCP/UDP port number, protocol type, and TCP control code	EXT-ACL	4-91
show ip access-list	Displays the rules for configured IP ACLs	PE	4-92
ip access-group	Adds a port to an IP ACL	IC	4-92
show ip access-group	Shows port assignments for IP ACLs	PE	4-92
map access-list ip	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC	4-93
show map access-list ip	Shows CoS value mapped to an access list for an interface	PE	4-94

access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IP ACLs. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list ip** {**standard** | **extended**} *acl_name*

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An egress ACL must contain all deny rules.
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

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

Related Commands

permit, deny 4-90

ip access-group (4-92)

show ip access-list (4-92)

permit, **deny** (Standard ACL)

This command adds a rule to a Standard IP ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit** | **deny**} {**any** | *source bitmask* | **host** *source*}

- **any** – Any source IP address.
- *source* – Source IP address.
- *bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.

Default Setting

None

Command Mode

Standard ACL

Command Usage

- New rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Related Commands

access-list ip (4-89)

permit, **deny** (Extended ACL)

This command adds a rule to an Extended IP ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit** | **deny**} [*protocol-number* | **udp**]
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | host *destination*}
[**source-port** *sport* [*end*]] [**destination-port** *dport* [*end*]]

[**no**] {**permit** | **deny**} **tcp**
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**source-port** *sport* [*end*]] [**destination-port** *dport* [*end*]]

- *protocol-number* – A specific protocol number. (Range: 0-255)
- *source* – Source IP address.
- *destination* – Destination IP address.
- *address-bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.
- *sport* – Protocol[3] source port number. (Range: 0-65535)
- *dport* – Protocol destination port number. (Range: 0-65535)
- *end* – Upper bound of the protocol port range. (Range: 0-65535)

Default Setting

None

Command Mode

Extended ACL

Command Usage

- All new rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

3. Includes TCP, UDP or other protocol types.

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
destination-port 80
Console(config-ext-acl)#
```

Related Commands

access-list ip (4-89)

show ip access-list

This command displays the rules for configured IP ACLs.

Syntax

show ip access-list {**standard** | **extended**} [*acl_name*]

- **standard** – Specifies a standard IP ACL.
- **extended** – Specifies an extended IP ACL.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
Console#
```

Related Commands

permit, deny 4-90

ip access-group (4-92)

ip access-group

This command binds a port to an IP ACL. Use the **no** form to remove the port.

Syntax

[**no**] **ip access-group** *acl_name* {**in** | **out**}

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

- **in** – Indicates that this list applies to ingress packets.
- **out** – Indicates that this list applies to egress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- You must configure a mask for an ACL rule before you can bind it to a port.

Example

```
Console(config)#int eth 1/25
Console(config-if)#ip access-group standard david in
Console(config-if)#
```

Related Commands

show ip access-list (4-92)

show ip access-group

This command shows the ports assigned to IP ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/25
 IP standard access-list david
Console#
```

Related Commands

ip access-group (4-92)

map access-list ip

This command sets the output queue for packets matching an ACL rule. The specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. Use the **no** form to remove the CoS mapping.

Syntax

[**no**] **map access-list ip** *acl_name* **cos** *cos-value*

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- *cos-value* – CoS value. (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- You must configure an ACL mask before you can map CoS values to the rule.
- A packet matching a rule within the specified ACL is mapped to one of the output queues as shown in the following table. For information on mapping the CoS values to output queues, see **queue cos-map** on 4-172.

Table 4-35. Egress Queue Priority Mapping

Priority	0	1	2	3	4	5	6	7
Queue	1	2	0	3	4	5	6	7

Example

```
Console(config)#interface ethernet 1/25
Console(config-if)#map access-list ip bill cos 0
Console(config-if)#
```

Related Commands

queue cos-map (4-172)

show map access-list ip (4-94)

show map access-list ip

This command shows the CoS value mapped to an IP ACL for the current interface. (The CoS value determines the output queue for packets matching an ACL rule.)

Syntax

show map access-list ip [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)

Command Mode

Privileged Exec

Example

```
Console#show map access-list ip
Access-list to COS of Eth 1/24
 Access-list ALS1 cos 0
Console#
```

Related Commands

map access-list ip (4-93)

ACL Information

Table 4-36. ACL Information

Command	Function	Mode	Page
show access-list	Shows all ACLs and associated rules	PE	4-95
show access-group	Shows the ACLs assigned to each port	PE	4-95

show access-list

This command shows all ACLs and associated rules, as well as all the user-defined masks.

Command Mode

Privileged Exec

Command Usage

Once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask.

Example

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 0.0.15.255
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
IP access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

show access-group

This command shows the port assignments of ACLs.

Command Mode

Privileged Executive

Example

```
Console#show access-group
Interface ethernet 1/25
 IP standard access-list david
 IP access-list jerry
Console#
```

SNMP Commands

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 4-37. SNMP Commands

Command	Function	Mode	Page
snmp-server	Enables the SNMPv3 server	GC	4-96
show snmp	Displays the status of SNMP communications	NE, PE	4-97
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	4-98
snmp-server contact	Sets the system contact string	GC	4-99
snmp-server location	Sets the system location string	GC	4-99
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	4-100
snmp-server enable traps	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC	4-102
snmp-server engine-id	Sets the SNMPv3 engine ID	GC	4-103
show snmp engine-id	Shows the SNMPv3 engine ID	PE	4-104
snmp-server view	Adds an SNMPv3 view	GC	4-105
show snmp view	Shows the SNMPv3 views	PE	4-105
snmp-server group	Adds an SNMPv3 group, mapping users to views	GC	4-106
show snmp group	Shows the SNMPv3 groups	PE	4-107
snmp-server user	Adds a user to an SNMPv3 group	GC	4-109
show snmp user	Shows the SNMPv3 users	PE	4-110

snmp-server

This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

Syntax

[**no**] **snmp-server**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server
Console(config)#
```

show snmp

This command can be used to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the snmp-server enable traps command.

Example

```
Console#show snmp

SNMP Agent: enabled

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read-write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
   0 Trap PDUs

SNMP logging: disabled
Console#
```

snmp-server community

This command defines the SNMP v1 and v2c community access string. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro**|**rw**]

no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.

- private - Read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*

no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location (4-99)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*

no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact (4-99)

snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *host-addr* [**inform** [**retry** *retries* | **timeout** *seconds*]] *community-string* [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} [**udp-port** *port*]}

no snmp-server host *host-addr*

- *host-addr* - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 recipient destination IP address entries)
- **inform** - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
  - *retries* - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
  - *seconds* - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
- *community-string* - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)
- **version** - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)
  - **auth** | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See “Simple Network Management Protocol” on page 3-34 for further information about these authentication and encryption options.
- *port* - Host UDP port to use. (Range: 1-65535; Default: 162)

Default Setting

- Host Address: None
- Notification Type: Traps
- SNMP Version: 1

- UDP Port: 162

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.
- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.
- To send an inform to a SNMPv2c host, complete these steps:

1. Enable the SNMP agent (page 4-96).
2. Allow the switch to send SNMP traps; i.e., notifications (page 4-102).
3. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
4. Create a view with the required notification messages (page 4-105).
5. Create a group that includes the required notify view (page 4-106).

- To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent (page 4-96).
2. Allow the switch to send SNMP traps; i.e., notifications (page 4-102).
3. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
4. Create a view with the required notification messages (page 4-105).
5. Create a group that includes the required notify view (page 4-106).

6. Specify a remote engine ID where the user resides (page 4-103).
7. Then configure a remote user (page 4-109).

- The switch can send SNMP version 1, 2c, or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 notifications.
- If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. If you use the V3 “auth” or “priv” options, the user name must first be defined with the **snmp-server user** command. Otherwise, the authentication password and/or privacy password will not exist, and the switch will not authorize SNMP access for the host. However, if you specify a V3 host with the “noauth” option, an SNMP user account will be generated, and the switch will authorize SNMP access for the host.

Example

```
Console(config)#snmp-server host 10.1.19.23 inform retries 10 timeout 30
batman version 2c udp-port 162
Console(config)#
```

Related Commands

snmp-server enable traps (4-102)

snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

[**no**] **snmp-server enable traps** [**authentication** | **link-up-down**]

- **authentication** - Keyword to issue authentication failure notifications.
- **link-up-down** - Keyword to issue link-up or link-down notifications.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.
- The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the **snmp-server group** command (page 4-106).

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (4-100)

snmp-server engine-id

This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

Syntax

snmp-server engine-id {**local** | **remote** {*ip-address*}} *engineid-string*

no snmp-server engine-id {**local** | **remote** {**address**}}

- **local** - Specifies the SNMP engine on this switch.
- **remote** - Specifies an SNMP engine on a remote device.
- *ip-address* - The Internet address of the remote device.
- *engineid-string* - String identifying the engine ID. (Range: 1-26 hexadecimal characters)

Default Setting

A unique engine ID is automatically generated by the switch based on its MAC address.

Command Mode

Global Configuration

Command Usage

- An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
- A remote engine ID is required when using SNMPv3 informs. (See **snmp-server host** on page 4-100.) The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. SNMP passwords are localized using the engine ID of the

authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

- Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value "1234" is equivalent to "1234" followed by 22 zeroes.
- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engineID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users (page 4-109).

Example

```
Console(config)#snmp-server engineID local 12345
Console(config)#snmp-server engineID remote 54321 192.168.1.19
Console(config)#
```

Related Commands

snmp-server host (4-100)

show snmp engine-id

This command shows the SNMP engine ID.

Command Mode

Privileged Exec

Example

This example shows the default engine ID.

```
Console#show snmp engine-id
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                                          IP address
80000000030004e2b316c54321                                  192.168.1.19
Console#
```

Table 4-38. show snmp engine-id - display description

Field	Description
Local SNMP engineID	String identifying the local engine ID.
Local SNMP engineBoots	The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.
Remote SNMP engineID	String identifying an engine ID on a remote device.
IP address	IP address of the device containing the corresponding remote SNMP engine.

snmp-server view

This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

Syntax

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name*

- *view-name* - Name of an SNMP view. (Range: 1-64 characters)
- *oid-tree* - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)
- **included** - Defines an included view.
- **excluded** - Defines an excluded view.

Default Setting

defaultview (includes access to the entire MIB tree)

Command Mode

Global Configuration

Command Usage

- Views are used in the **snmp-server group** command to restrict user access to specified portions of the MIB tree.
- The predefined view “defaultview” includes access to the entire MIB tree.

Examples

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included
Console(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included
Console(config)#
```

show snmp view

This command shows information on the SNMP views.

Command Mode

Privileged Exec

Example

```
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: nonvolatile
Row Status: active

Console#
```

Table 4-39. show snmp view - display description

Field	Description
View Name	Name of an SNMP view.
Subtree OID	A branch in the MIB tree.
View Type	Indicates if the view is included or excluded.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.

snmp-server group

This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

Syntax

snmp-server group *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]

no snmp-server group *groupname*

- *groupname* - Name of an SNMP group. (Range: 1-32 characters)
- **v1** | **v2c** | **v3** - Use SNMP version 1, 2c or 3.
  - **auth** | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See “Simple Network Management Protocol” on page 3-34 for further information about these authentication and encryption options.
- *readview* - Defines the view for read access. (1-64 characters)
- *writeview* - Defines the view for write access. (1-64 characters)
- *notifyview* - Defines the view for notifications. (1-64 characters)

Default Setting

- Default groups: public[4] (read only), private[5] (read/write)

4. No view is defined.
5. Maps to the defaultview.

- *readview* - Every object belonging to the Internet OID space (1.3.6.1).
- *writeview* - Nothing is defined.
- *notifyview* - Nothing is defined.

Command Mode

Global Configuration

Command Usage

- A group sets the access policy for the assigned users.
- When authentication is selected, the MD5 or SHA algorithm is used as specified in the **snmp-server user** command.
- When privacy is selected, the DES 56-bit algorithm is used for data encryption
- For additional information on the notification messages supported by this switch, see "Supported Notification Messages" on page 3-45. Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the **snmp-server enable traps** command (page 4-102).

Example

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

show snmp group

Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

Command Mode

Privileged Exec

Example

```
Console#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: nonvolatile
Row Status: active

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#
```

Table 4-40. show snmp group - display description

Field	Description
groupname	Name of an SNMP group.
security model	The SNMP version.
readview	The associated read view.
writeview	The associated write view.
notifyview	The associated notify view.
storage-type	The storage type for this entry.
Row Status	The row status of this entry.

snmp-server user

This command adds a user to an SNMP group, restricting the user to a specific SNMP Read and a Write View. Use the **no** form to remove a user from an SNMP group.

Syntax

snmp-server user *username groupname* [**remote** *ip-address*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote**}

- *username* - Name of user connecting to the SNMP agent. (Range: 1-32 characters)
- *groupname* - Name of an SNMP group to which the user is assigned. (Range: 1-32 characters)
- **remote** - Specifies an SNMP engine on a remote device.
- *ip-address* - The Internet address of the remote device.
- **v1** | **v2c** | **v3** - Use SNMP version 1, 2c or 3.
- **encrypted** - Accepts the password as encrypted input.
- **auth** - Uses SNMPv3 with authentication.
- **md5** | **sha** - Uses MD5 or SHA authentication.
- *auth-password* - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)
- **priv des56** - Uses SNMPv3 with 56-bit DES data encryption.
- *priv-password* - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the **snmp-server engine-id** command before using this configuration command.
- Before you configure a remote user, use the **snmp-server engine-id** command (page 4-103) to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.

- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent’s SNMP engine ID before you can send proxy requests or informs to it.

Example

```
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace
priv des56 einstien
Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3
auth md5 greenpeace priv des56 einstien
Console(config)#
```

show snmp user

This command shows information on SNMP users.

Command Mode

Privileged Exec

Example

```
Console#show snmp user
EngineId: 01000000000000000000000000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Table 4-41. show snmp user - display description

Field	Description
EngineId	String identifying the engine ID.
User Name	Name of user connecting to the SNMP agent.
Authentication Protocol	The authentication protocol used with SNMPv3.
Privacy Protocol	The privacy protocol used with SNMPv3.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.
SNMP remote user	A user associated with an SNMP engine on a remote device.

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Table 4-42. Interface Commands

Command	Function	Mode	Page
interface	Configures an interface type and enters interface configuration mode	GC	4-111
description	Adds a description to an interface configuration	IC	4-112
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC	4-112
negotiation	Enables autonegotiation of a given interface	IC	4-113
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC	4-114
flowcontrol	Enables flow control on a given interface	IC	4-115
shutdown	Disables an interface	IC	4-116
clear counters	Clears statistics on an interface	PE	4-116
show interfaces status	Displays status for the specified interface	NE, PE	4-117
show interfaces counters	Displays statistics for the specified interfaces	NE, PE	4-118
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-119

interface

This command configures an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

Syntax

interface *interface*
no interface port-channel *channel-id*

- *interface*
  - **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)
- **port-channel** *channel-id* (Range: 1-8)
- **vlan** *vlan-id* (Range: 1-4093)

Default Setting

None

Command Mode

Global Configuration

Example

To specify port 24, enter the following command:

```
Console(config)#interface ethernet 1/24
Console(config-if)#
```

description

This command adds a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*
no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example adds a description to port 24.

```
Console(config)#interface ethernet 1/24
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

This command configures the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {1000full | 100full | 100half | 10full | 10half}
no speed-duplex

- **1000full** - Forces 1000 Mbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is

1000full for Gigabit Ethernet ports.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (4-113)

capabilities (4-114)

negotiation

This command enables autonegotiation for a given interface. Use the **no** form to disable autonegotiation.

Syntax

[**no**] **negotiation**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.
- If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

capabilities (4 -114)

speed-duplex (4-112)

capabilities

This command advertises the port capabilities of a given interface during autonegotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

[**no**] **capabilities** {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

- **1000full** - Supports 1000 Mbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation
- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (*The current switch ASIC only supports symmetric pause frames.*)

Default Setting

- 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
- 1000BASE-SX/LX/LH: 1000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When auto-negotiation is enabled with the **negotiation** command, the switch will negotiate the best settings for a link based on the **capabilites** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

negotiation (4-113)

speed-duplex (4-112)

flowcontrol (4-115)

flowcontrol

This command enables flow control. Use the **no** form to disable flow control.

Syntax

[**no**] **flowcontrol**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.
- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (4-113)

capabilities (flowcontrol, symmetric) (4-114)

shutdown

This command disables an interface. To restart a disabled interface, use the **no** form.

Syntax

[**no**] **shutdown**

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

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

clear counters

This command clears statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Always unit 1)

- *port* - Port number. (Range: 1-28)
- **port-channel** *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces status

This command displays the status for an interface.

Syntax

show interfaces status [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)
- **port-channel** *channel-id* (Range: 1-8)
- **vlan** *vlan-id* (Range: 1-4093)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see “Displaying Connection Status” on page 3-81.

Example

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
 Basic information:
  Port type:                1000T
  Mac address:              00-30-F1-D4-73-A5
 Configuration:
  Name:
  Port admin:               Up
  Speed-duplex:             Auto
  Capabilities:             10half, 10full, 100half, 100full, 1000full
  Broadcast storm:          Enabled
  Broadcast storm limit:    500 packets/second
  Flow control:             Disabled
  LACP:                     Disabled
  Port security:            Disabled
  Max MAC count:            0
  Port security action:     None
  Media type:               None
Current status:
  Link status:              Up
  Port operation status:    Up
  Operation speed-duplex:   1000full
  Flow control type:        None
Console#show interfaces status vlan 1
 Information of VLAN 1
 MAC address:               00-00-AB-CD-00-00
Console#
```

show interfaces counters

This command displays interface statistics.

Syntax

show interfaces counters [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)
- **port-channel** *channel-id* (Range: 1-8)

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see “Showing Port Statistics” on page 3-99.

Example

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/7
 Iftable stats:
  Octets input: 30658, Octets output: 196550
  Unicast input: 6, Unicast output: 5
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 3064
  Broadcast input: 262, Broadcast output: 1
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 227208, Packets: 3338
  Broadcast pkts: 263, Multi-cast pkts: 3064
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
  Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets:0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)
- **port-channel** *channel-id* (Range: 1-8)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 24.

```
Console#show interfaces switchport ethernet 1/24
 Broadcast threshold:           Enabled, 500 packets/second
 LACP status:                   Enabled
 Ingress rate limit:            disable, Level: 30
 VLAN membership mode:          Hybrid
 Ingress rule:                  Enabled
 Acceptable frame type:         All frames
 Native VLAN:                   1
 Priority for untagged traffic: 0
 Gvrp status:                   Disabled
 Allowed Vlan:                  1(u),
 Forbidden Vlan:
 Private-VLAN mode:             NONE
 Private-VLAN host-association: NONE
 Private-VLAN mapping:          NONE
Console#
```

Table 4-43. show interfaces switchport - display description

Field	Description
Broadcast threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 4-121).
LACP status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 4-127).
Ingress rate limit	Shows if rate limiting is enabled, and the current rate limit. (page 4-124).
VLAN membership mode	Indicates membership mode as Trunk or Hybrid (page 4-155).
Ingress rule	Shows if ingress filtering is enabled or disabled (page 4-156). Note: Ingress filtering is always enabled.
Acceptable frame type	Shows if acceptable VLAN frames include all types or tagged frames only (page 4-155).
Native VLAN	Indicates the default Port VLAN ID (page 4-157).
Priority for untagged traffic	Indicates the default priority for untagged frames (page 4-169).
GVRP status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 4-166).
Allowed VLAN	Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged (page 4-157).
Forbidden VLAN	Shows the VLANs this interface can not dynamically join via GVRP (page 4-158).
Private VLAN mode	Shows the private VLAN mode as host, promiscuous,or none.
Private VLAN host-association	Shows the secondary (or community) VLAN with which this port is associated.
Private VLAN mapping	Shows the primary VLAN mapping for a promiscuous port.

Broadcast Commands

This section describes how to configure broadcast storm control for the switch.

Table 4-44. Broadcast Commands

Command	Function	Mode	Page
broadcast packet-rate	Configures the global threshold level	GC	4-121
switchport broadcast	Enables broadcast storm control for an interface	IC	4-121
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-119

broadcast packet-rate

This command configures the global broadcast storm control threshold level.

Syntax

broadcast packet-rate *rate*

rate - Threshold level as a rate; i.e., packets per second. (Range: 240 - 1488100)

Default Setting

500 packets per second

Command Mode

Global Configuration

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- The specified threshold value applies to all ports on the switch.

Example

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#broadcast packet-rate 600
```

switchport broadcast

This command enables broadcast storm control on an interface. Use the **no** form to disable broadcast storm control on an interface.

Syntax

[**no**] **switchport broadcast**

Default Setting

Enabled

Command Mode

Interface Configuration

Example

The following shows how to disable broadcast storm control on an interface:

```
Console(config-if)#no switchport broadcast
```

Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

Table 4-45. Mirror Port Commands

Command	Function	Mode	Page
port monitor	Configures a mirror session	IC	4-122
show port monitor	Shows the configuration for a mirror port	PE	4-123

port monitor

This command configures a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface* - **ethernet** *unit*/*port* (source port)
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- The mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- You can create multiple mirror sessions, but all sessions must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.

Example

The following example configures the switch to mirror all packets from port 6 to 11.

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

This command displays mirror information.

Syntax

show port monitor [*interface*]

- *interface* - **ethernet** *unit*/*port* (source port)
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 11.

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/1
 Source port(monitored port)  :Eth1/6
 Mode                         :RX/TX
Console#
```

Rate Limit Commands

This function allows the network manager to control the maximum rate for traffic received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Table 4-46. Rate Limit Commands

Command	Function	Mode	Page
rate-limit	Configures the maximum input or output rate for a port	IC	4-124

rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

Syntax

rate-limit {**input**} [*rate*]

no rate-limit {**input**}

- **input** – Input rate
- *rate* – Percentage

Default Setting

100 percent

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 600
Console(config-if)#
```

Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 4-47. Link Aggregation Commands

Command	Function	Mode	Page
Manual Configuration Commands			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	4-111
channel-group	Adds a port to a trunk	IC (Ethernet)	4-126
Dynamic Configuration Commands			
lacp	Configures LACP for the current interface	IC (Ethernet)	4-127
lacp system-priority	Configures a port's LACP system priority	IC (Ethernet)	4-128
lacp admin-key	Configures a port's administration key	IC (Ethernet)	4-129
lacp admin-key	Configures a port channel's administration key	IC (Port Channel)	4-130
lacp port-priority	Configures a port's LACP port priority	IC (Ethernet)	4-131
Trunk Status Display Commands			
show interfaces status port-channel	Shows trunk information	NE, PE	4-117
show lacp	Shows LACP information	PE	4-131

Guidelines for Creating Trunks

- General Guidelines –
- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to 8 ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including

communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.
- Dynamically Creating a Port Channel –
- Ports assigned to a common port channel must meet the following criteria:
- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.
- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

channel-group

This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*
no channel-group

channel-id - Trunk index (Range: 1-8)

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 11.

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#
```

lacp

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

[no] lacp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The ports on both ends of an LACP trunk must be configured for full duplex, and auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 10-12. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/10
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type:              1000T
  Mac address:            00-30-F1-D4-73-A4
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full, 1000full
  Flow control:           Disabled
  Port security:          Disabled
  Max MAC count:          0
 Current status:
  Created by:             Lacp
  Link status:            Up
  Operation speed-duplex: 1000full
  Flow control type:      None
  Member Ports:           Eth1/10, Eth1/11, Eth1/12,
Console#
```

lacp system-priority

This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **system-priority** *priority*

no lacp {actor | partner} system-priority

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **admin-key** *key*

[no] lacp {actor | partner} admin-key

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *key* - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel admin key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.

- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

Syntax

lacp admin-key *key*

[no] lacp admin-key

key - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Port Channel)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

Example

```
Console(config)#interface port channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp port-priority

This command configures LACP port priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **port-priority** *priority*

no lacp {actor | partner} port-priority

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - LACP port priority is used to select a backup link. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

show lacp

This command displays LACP information.

Syntax

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sys-id**}

- *port-channel* - Local identifier for a link aggregation group. (Range: 1-6)
- **counters** - Statistics for LACP protocol messages.
- **internal** - Configuration settings and operational state for local side.
- **neighbors** - Configuration settings and operational state for remote side.
- **sys-id** - Summary of system priority and MAC address for all channel groups.

Default Setting

Port Channel: all

Command Mode

Privileged Exec

Example

```
Console#show lacp 1 counters
Channel group : 1
-------------------------------------------------------------------
Eth 1/ 2
-------------------------------------------------------------------
  LACPDUs Sent:          10
  LACPDUs Receive:       5
  Marker Sent:           0
  Marker Receive:        0
  LACPDUs Unknown Pkts: 0
  LACPDUs Illegal Pkts: 0
.
.
.
```

Table 4-48. show lacp counters - display description

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```
Console#show lacp internal
Channel group : 1
-------------------------------------------------------------------
Oper Key:  3
Admin Key: 0
Eth 1/ 2
-------------------------------------------------------------------
  LACPDUs Internal:      30 sec
  LACP System Priority: 32768
  LACP Port Priority:   32768
  Admin Key:            3
  Oper Key:             3
  Admin State: defaulted, aggregation, long timeout, LACP-activity
  Oper State:           distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
.
.
.
```

Table 4-49. show lacp internal - display description

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor’s state parameters: Expired – The actor’s receive machine is in the expired state. Defaulted – The actor’s receive machine is using defaulted operational partner information, administratively configured for the partner. Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

```
Console#show lacp 1 neighbors
Channel group 1 neighbors
-------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------
  Partner Admin System ID:   32768, 00-00-00-00-00-00
  Partner Oper System ID:    32768, 00-01-F4-78-AE-C0
  Partner Admin Port Number: 2
  Partner Oper Port Number:  2
  Port Admin Priority:       32768
  Port Oper Priority:        32768
  Admin Key:                 0
  Oper Key:                  3
  Admin State:               defaulted, distributing, collecting,
                             synchronization, long timeout,
  Oper State:                distributing, collecting,
                             synchronization, aggregation,
                             long timeout, LACP-activity
.
.
.
```

Table 4-50. show lacp neighbors - display description

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

```
Console#show lacp 1 sysid
Channel group    System Priority    System MAC Address
-------------------------------------------------------------------
           1              32768      00-30-F1-8F-2C-A7
           2              32768      00-30-F1-8F-2C-A7
           3              32768      00-30-F1-8F-2C-A7
           4              32768      00-30-F1-8F-2C-A7
           5              32768      00-30-F1-8F-2C-A7
           6              32768      00-30-F1-8F-2C-A7
           7              32768      00-30-F1-D4-73-A0
           8              32768      00-30-F1-D4-73-A0
           9              32768      00-30-F1-D4-73-A0
          10              32768      00-30-F1-D4-73-A0
          11              32768      00-30-F1-D4-73-A0
          12              32768      00-30-F1-D4-73-A0
.
.
.
```

Table 4-51. show lacp sysid - display description

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Table 4-52. Address Table Commands

Command	Function	Mode	Page
mac-address-table static	Maps a static address to a port in a VLAN	GC	4-135
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE	4-136
show mac-address-table	Displays entries in the bridge-forwarding database	PE	4-137
mac-address-table aging-time	Sets the aging time of the address table	GC	4-138
show mac-address-table aging-time	Shows the aging time for the address table	PE	4-138

mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface*
vlan *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
  - **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)
  - **port-channel** *channel-id* (Range: 1-8)
- *vlan-id* - VLAN ID (Range: 1-4093)
- *action*
  - **delete-on-reset** - Assignment lasts until the switch is reset.
  - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

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

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* - MAC address.
- *mask* - Bits to match in the address.
- *interface*
  - **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Always unit 1)
  - *port* - Port number. (Range: 1-28)
  - **port-channel** *channel-id* (Range: 1-8)
- *vlan-id* - VLAN ID (Range: 1-4093)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learned - Dynamic address entries
  - Permanent - Static entry
  - Delete-on-reset - Static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit “0” means to match a bit and “1” means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means “any.”

- The maximum number of address entries is 8191.

Example

```
Console#show mac-address-table
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-00-00-00-00-17    1 Learned
  Eth 1/ 1 00-E0-29-94-34-DE    1 Delete-on-reset
Console#
```

mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds - Aging time. (Range: 10-1000000 seconds; 0 to disable aging)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

This command shows the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Table 4-53. Spanning Tree Commands

Command	Function	Mode	Page
spanning-tree	Enables the spanning tree protocol	GC	4-139
spanning-tree mode	Configures STP, or RSTP mode	GC	4-140
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC	4-141
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC	4-142
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC	4-142
spanning-tree priority	Configures the spanning tree bridge priority	GC	4-143
spanning-tree pathcost method	Configures the path cost method for RSTP	GC	4-144
spanning-tree transmission-limit	Configures the transmission limit for RSTP	GC	4-144
spanning-tree spanning-disabled	Disables spanning tree for an interface	IC	4-145
spanning-tree cost	Configures the spanning tree path cost of an interface	IC	4-145
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC	4-146
spanning-tree edge-port	Enables fast forwarding for edge ports	IC	4-147
spanning-tree portfast	Sets an interface to fast forwarding	IC	4-148
spanning-tree link-type	Configures the link type for RSTP	IC	4-148
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE	4-149
show spanning-tree	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), or a selected interface.	PE	4-150

spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

[**no**] **spanning-tree**

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch.

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree mode

This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {**stp** | **rstp**}
no spanning-tree mode

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- Spanning Tree Protocol
- Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members.
- Rapid Spanning Tree Protocol
- RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
- STP Mode – If the switch receives an 802.1D BPDU after a port’s migration

delay timer expires, the switch assumes that it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

- RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Example

The following example configures the switch to use Rapid Spanning Tree.

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*
no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)

The minimum value is the higher of 4 or [(max-age / 2) +1].

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*
no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).
The maximum value is the lower of 10 or [(max-age / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

Related Commands

spanning-tree forward-time (4-141)

spanning-tree max-age (4-142)

spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)

The minimum value is the higher of 6 or [2 x (hello-time + 1)].

The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

Related Commands

spanning-tree forward-time (4-141)

spanning-tree hello-time (4-142)

spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge. (Range: 0 - 65535)

(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000. This method is based on the IEEE 802.1w Rapid Spanning Tree Protocol.
- **short** - Specifies 16-bit based values that range from 1-65535. This method is based on the IEEE 802.1 Spanning Tree Protocol.

Default Setting

Long method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 4-145) takes precedence over port priority (page 4-146).

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the **no** form to reenable the spanning tree algorithm for the specified interface.

Syntax

[**no**] **spanning-tree spanning-disabled**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

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

spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree cost *cost*
no spanning-tree cost *cost*

cost - The path cost for the port. (Range: 1-200,000,000))
The recommended range is:

- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

Default Setting

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000

- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the spanning-tree pathcost method (page 4-144) is set to short, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree port-priority

This command configures the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*
no spanning-tree port-priority *priority*

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands

spanning-tree cost (4-145)

spanning-tree edge-port

This command specifies an interface as an edge port. Use the **no** form to restore the default.

Syntax

[**no**] **spanning-tree edge-port**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the **spanning-tree portfast**.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast (4-148)

spanning-tree portfast

This command sets an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

[**no**] **spanning-tree portfast**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)
- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#Spanning-tree portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port (4-147)

spanning-tree link-type

This command configures the link type for Rapid Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.

- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

- *interface*
  - **ethernet** *unit/port*
  - unit - Stack unit. (Always unit 1)
  - port - Port number. (Range: 1-28)
  - **port-channel** *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console#spanning-tree protocol-migration eth 1/5
Console#
```

show spanning-tree

This command shows the configuration for the common spanning tree (CST).

Syntax

show spanning-tree [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - unit - Stack unit. (Always unit 1)
    - port - Port number. (Range: 1-28)
  - **port-channel** *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- For a description of the items displayed under “Spanning-tree information,” see “Configuring Global Settings” on page 3-114. For a description of the items displayed for specific interfaces, see “Displaying Interface Settings” on page 3-118.

Example

```
Console#show spanning-tree
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode:                  RSTP
 Spanning tree enabled/disabled:      enabled
 Instance:                            0
 VLANs configuration:                 1-4093
 Priority:                            32768
 Bridge Hello Time (sec.):            2
 Bridge Max Age (sec.):               20
 Bridge Forward Delay (sec.):         15
 Root Hello Time (sec.):              2
 Root Max Age (sec.):                 20
 Root Forward Delay (sec.):           15
 Max hops:                            20
 Remaining hops:                      20
 Designated Root:                     32768.0.0000E8AAAA00
 Current root port:                   1
 Current root cost:                   10000
 Number of topology changes:          1
 Last topology changes time (sec.):21561
 Transmission limit:                  3
 Path Cost Method:                    long
---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
 Admin status:                enabled
 Role:                        root
 State:                       forwarding
 External admin path cost:  10000
 Internal admin path cost:  10000
 External oper path cost:   10000
 Internal oper path cost:   10000
 Priority:                    128
 Designated cost:             0
 Designated port:             128.1
 Designated root:             32768.0.0000E8AAAA00
 Designated bridge:           32768.0.0000E8AAAA00
 Fast forwarding:             disabled
 Forward transitions:         1
 Admin edge port:             disabled
 Oper edge port:              disabled
 Admin Link type:             auto
 Oper Link type:              point-to-point
 Spanning Tree Status:        enabled
.
.
.
Console#
```

VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Table 4-54. VLAN Commands

Command Groups	Function	Page
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state	4-152
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP	4-154
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses	4-159
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports	4-160

Editing VLAN Groups

Table 4-55. Editing VLAN Groups

Command	Function	Mode	Page
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC	4-152
vlan	Configures a VLAN, including VID, name and state	VC	4-153

vlan database

This command enters VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the **show running-config** command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

show vlan (4-159)

vlan

This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of configured VLAN. (Range: 1-4093, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
- **state** - Keyword to be followed by the VLAN state.
  - **active** - VLAN is operational.
  - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- **no vlan** *vlan-id* deletes the VLAN.
- **no vlan** *vlan-id* **name** removes the VLAN name.
- **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan (4-159)

Configuring VLAN Interfaces

Table 4-56. Configuring VLAN Interfaces

Command	Function	Mode	Page
interface vlan	Enters interface configuration mode for a specified VLAN	IC	4-154
switchport mode	Configures VLAN membership mode for an interface	IC	4-155
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	4-155
switchport ingress-filtering	Enables ingress filtering on an interface	IC	4-156
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	4-157
switchport allowed vlan	Configures the VLANs associated with an interface	IC	4-157
switchport gvrp	Enables GVRP for an interface	IC	4-166
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	4-158
switchport priority default	Sets a port priority for incoming untagged frames	IC	*4-170*

interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown (4-116)

switchport mode

This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {**hybrid** | **access**}
no switchport mode

- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- **access** - Specifies an access VLAN inferface. The port transmits and receives untagged frames only.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

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

Related Commands

switchport acceptable-frame-types (4-155)

switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** - The port accepts all frames, tagged or untagged.
- **tagged** - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

switchport mode (4-155)

switchport ingress-filtering

This command enables ingress filtering for an interface.

Note: Although the ingress filtering command is available, the switch has ingress filtering permanently set to enable. Therefore, trying to disable the filtering with the "no switchport ingress-filtering” command will produce this error message: “Note: Failed to ingress-filtering on ethernet interface !”

Syntax

switchport ingress-filtering

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.
- With ingress filtering enabled, a port will discard received frames tagged for VLANs for it which it is not a member.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

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

switchport native vlan

This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port.
(Range: 1-4093, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Setting the native VLAN for a port can only be performed when the port is a member of the VLAN and the VLAN is untagged. The “no switchport native vlan” command will set the native VLAN of the port to untagged VLAN 1.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

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

switchport allowed vlan

This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

Note: Each port can only have one untagged VLAN. If a second VLAN is defined for a port as untagged, the other VLAN that had untagged status will automatically be changed to tagged. Setting a VLAN untagged will also change the native VLAN of the port to this VLAN.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}

no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no

spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4093).

Default Setting

- All ports are assigned to VLAN 1 by default
- The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- The interface can be added to a VLAN as an untagged member regardless of connected devices to this interface. The default setting is untagged VLAN 1. Note that each port can only have one untagged VLAN. If a second VLAN is defined for a port as untagged, the other VLAN that had untagged status will automatically be changed to tagged. Setting a VLAN untagged will also change the native VLAN of the port to this VLAN.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport forbidden vlan

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

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}
no switchport forbidden vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no

spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4093).

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

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

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

Displaying VLAN Information

Table 4-57. Displaying VLAN Information

Command	Function	Mode	Page
show vlan	Shows VLAN information	NE, PE	4-159
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	4-117
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	4-119

show vlan

This command shows VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
- *vlan-id* - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
- *vlan-name* - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1.

```
Console#show vlan id 1

VLAN ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channels:  Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                     Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                     Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                     Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                       Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S)
Console#
```

Configuring Private VLANs

Private VLANs provide port-based security between ports within the assigned VLAN. This switch supports primary/secondary associated groups of private VLAN. A primary VLAN contains promiscuous ports that can communicate with all other ports in the private VLAN group, while a secondary (or community) VLAN contains community ports that can only communicate with other hosts within the secondary VLAN and with any of the promiscuous ports in the associated primary VLAN. In both cases, the promiscuous ports are designed to provide open access to an external network such as the Internet, while the community ports provide restricted access to local users.

Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be associated with each primary VLAN. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

Table 4-58. Private VLAN Commands

Command	Function	Mode	Page
Edit Private VLAN Groups			
private-vlan	Adds or deletes primary or community VLANs	VC	4-161
private-vlan association	Associates a community VLAN with a primary VLAN	VC	*4-162*
Configure Private VLAN Interfaces			
switchport mode private-vlan	Sets an interface to host mode or promiscuous mode	IC	*4-162*
switchport private-vlan host-association	Associates an interface with a secondary VLAN	IC	*4-163*
switchport private-vlan mapping	Maps an interface to a primary VLAN	IC	*4-164*
Display Private VLAN Information			
show vlan private-vlan	Shows private VLAN information	NE, PE	4-164

To configure primary/secondary associated groups, follow these steps:

1. Use the private-vlan command to designate one or more community VLANs and the primary VLAN that will channel traffic outside of the community groups.
2. Use the private-vlan association command to map the community VLAN(s) to the primary VLAN.
3. Use the switchport mode private-vlan command to configure ports as promiscuous (i.e., having access to all ports in the primary VLAN) or host (i.e., community port).
4. Use the switchport private-vlan host-association command to assign a port to a secondary VLAN.
5. Use the switchport private-vlan mapping command to assign a port to a primary VLAN.
6. Use the show vlan private-vlan command to verify your configuration settings.

private-vlan

Use this command to create a primary or community VLAN. Use the **no** form to remove the specified private VLAN.

Syntax

private-vlan *vlan-id* {**community | primary**}
no private-vlan *vlan-id*

- *vlan-id* - ID of private VLAN. (Range: 1-4093, no leading zeroes).
- **community** – A VLAN in which traffic is restricted to host memebers in the same VLAN and to promiscuous ports in the associate primary VLAN.
- **primary** – A VLAN which can contain one or more community VLANs, and serves to channel traffic between community VLANs and other locations.

Default Setting

None

Command Mode

VLAN Configuration

Command Usage

- Private VLANs are used to restrict traffic to ports within the same community VLAN, and channel traffic passing outside the community through promiscuous ports. When using community VLANs, they must be mapped to an associated “primary” VLAN that contains promiscuous ports.
- Port membership for private VLANs is static. Once a port has been assigned to a private VLAN, it cannot be dynamically moved to another VLAN via GVRP.
- Private VLAN ports cannot be set to trunked mode. (See “switchport mode” on

page 4-155.)

Example

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 community
Console(config)#
```

private vlan association

Use this command to associate a primary VLAN with a secondary (i.e., community) VLAN. Use the no form to remove all associations for the specified primary VLAN.

Syntax

private-vlan *primary-vlan-id* **association** {*primary-vlan-id* | **add** *secondary-vlan-id* | **remove** *secondary-vlan-id*}

no private-vlan *primary-vlan-id* **association**

- *primary-vlan-id* - ID of primary VLAN. (Range: 1-4093, no leading zeroes).
- *secondary-vlan-id* - ID of secondary (i.e, community) VLAN. (Range: 1-4093, no leading zeroes).

Default Setting

None

Command Mode

VLAN Configuration

Command Usage

Secondary VLANs provide security for group members. The associated primary VLAN provides a common interface for access to other network resources within the primary VLAN (e.g., servers configured with promiscuous ports) and to resources outside of the primary VLAN (via promiscuous ports).

Example

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

switchport mode private-vlan

Use this command to set the private VLAN mode for an interface. Use the **no** form to restore the default setting.

Syntax

switchport mode private-vlan{**host** | **promiscuous**}
no switchport mode private-vlan

- **host** – This port type can subsequently be assigned to a community VLAN.
- **promiscuous** – This port type can communicate with all other promiscuous

ports in the same primary VLAN, as well as with all the ports in the associated secondary VLANs.

Default Setting

Normal VLAN

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To assign a promiscuous port to a primary VLAN, use the **switchport private-vlan mapping** command. To assign a host port to a community VLAN, use the **private-vlan host association** command.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config-if)#
```

switchport private-vlan host-association

Use this command to associate an interface with a secondary VLAN. Use the **no** form to remove this association.

Syntax

switchport private-vlan host-association *secondary-vlan-id*
no switchport private-vlan host-association

secondary-vlan-id - ID of secondary (i.e., community) VLAN. (Range: 1-4093, no leading zeroes).

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

All ports assigned to a secondary (i.e., community) VLAN can pass traffic between group members, but must communicate with resources outside of the group via promiscuous ports in the associated primary VLAN.

Example

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config-if)#
```

switchport private-vlan mapping

Use this command to map an interface to a primary VLAN. Use the **no** form to remove this mapping.

Syntax

switchport private-vlan mapping *primary-vlan-id*
no switchport private-vlan mapping

primary-vlan-id - ID of primary VLAN. (Range: 1-4093, no leading zeroes).

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Promiscuous ports assigned to a primary VLAN can communicate with any other promiscuous ports in the same VLAN, and with the group members within any associated secondary VLANs.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
Console(config-if)#
```

show vlan private-vlan

Use this command to show the private VLAN configuration settings on this switch.

Syntax

show vlan private-vlan mapping [**community** | **primary**]

- **community** – Displays all community VLANs, along with their associated primary VLAN and assigned host interfaces.
- **primary** – Displays all primary VLANs, along with any assigned promiscuous interfaces.

Default Setting

None

Command Mode

Privileged Executive

Example

```
Console#show vlan private-vlan
Primary   Secondary       Type       Interfaces
--------  -----------  ----------  ------------------------------
     5                 primary     Eth1/ 3
     5         6       community   Eth1/ 4 Eth1/ 5
Console#
```

GVRP and Bridge Extension Commands

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

Table 4-59. GVRP and Bridge Extension Commands

Command	Function	Mode	Page
bridge-ext gvrp	Enables GVRP globally for the switch	GC	4-165
show bridge-ext	Shows the global bridge extension configuration	PE	4-166
switchport gvrp	Enables GVRP for an interface	IC	4-166
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	4-158
show gvrp configuration	Displays GVRP configuration for the selected interface	NE, PE	4-167
garp timer	Sets the GARP timer for the selected function	IC	4-167
show garp timer	Shows the GARP timer for the selected function	NE, PE	4-168

bridge-ext gvrp

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

Syntax

[no] bridge-ext gvrp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

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

Example

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

show bridge-ext

This command shows the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Displaying Basic VLAN Information” on page 3-126 and “Displaying Bridge Extension Capabilities” on page 3-12 for a description of the displayed items.

Example

```
Console#show bridge-ext
 Max support VLAN numbers:                256
 Max support VLAN ID:                     4093
 Extended multicast filtering services:  No
 Static entry individual port:            Yes
 VLAN learning:                           IVL
 Configurable PVID tagging:               Yes
 Local VLAN capable:                      No
 Traffic classes:                         Enabled
 Global GVRP status:                      Disabled
 GMRP:                                    Disabled
Console#
```

switchport gvrp

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

Syntax

[no] switchport gvrp

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

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

show gvrp configuration

This command shows if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

- **ethernet** *unit*/*port*
  - unit - Stack unit. (Always unit 1)
  - port - Port number. (Range: 1-28)
- **port-channel** *channel-id* (Range: 1-8)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 Gvrp configuration: Enabled
Console#
```

garp timer

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

Syntax

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

- {**join** | **leave** | **leaveall**} - Which timer to set.
- *timer_value* - Value of timer.
  Ranges:
  join: 20-1000 centiseconds
  leave: 60-3000 centiseconds
  leaveall: 500-18000 centiseconds

Default Setting

- join: 20 centiseconds

- leave: 60 centiseconds
- leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

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

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

Example

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

Related Commands

show garp timer (4-168)

show garp timer

This command shows the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

- **ethernet** *unit*/*port*
  - unit - Stack unit. (Always unit 1)
  - port - Port number. (Range: 1-28)
- **port-channel** *channel-id* (Range: 1-8)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer: 20 centiseconds
 Leave timer: 60 centiseconds
 Leaveall timer: 1000 centiseconds
Console#
```

Related Commands

garp timer (4-167)

Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Table 4-60. Priority Commands

Command Groups	Function	Page
Priority (Layer 2)	Configures default priority for untagged frames, sets queue weights, and maps class of service tags to hardware queues	4-170
Priority (Layer 3 and 4)	Maps IP DSCP tags to class of service values	4-175

Priority Commands (Layer 2)

Table 4-61. Priority Commands (Layer 2)

Command	Function	Mode	Page
queue mode	Sets the queue mode to strict priority or Weighted Round-Robin (WRR)	GC	4-170
switchport priority default	Sets a port priority for incoming untagged frames	IC	*4-170*
queue bandwidth	Assigns round-robin weights to the priority queues	GC	4-172
queue cos map	Assigns class-of-service values to the priority queues	IC	4-172
show queue mode	Shows the current queue mode	PE	4-173
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	4-174
show queue cos-map	Shows the class-of-service map	PE	4-174
show interfaces switchport	Displays the administrative and operational status of an interface	PE	4-119

queue mode

This command sets the queue mode to strict priority or Weighted Round-Robin (WRR) for the class of service (CoS) priority queues. Use the **no** form to restore the default value.

Syntax

queue mode {**strict** | **wrr**}
no queue mode

- **strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 - 7 respectively.

Default Setting

Weighted Round Robin

Command Mode

Global Configuration

Command Usage

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Example

The following example sets the queue mode to strict priority service mode.

```
Console(config)#queue mode strict
Console(config)#
```

switchport priority default

This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- This switch provides eight priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the **show queue bandwidth** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

queue bandwidth

This command assigns weighted round-robin (WRR) weights to the eight class of service (CoS) priority queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight1...weight4*
no queue bandwidth

weight1...weight4 - The ratio of weights for queues 0 - 3 determines the weights used by the WRR scheduler. (Range: 1 - 15)

Default Setting

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

WRR controls bandwidth sharing at the egress port by defining scheduling weights.

Example

This example shows how to assign WRR weights to each of the priority queues for port 5.

```
Console#configure
Console(config)#int eth 1/5
Console(config-if)#queue bandwidth 1 3 5 7 9 11 13 15
Console(config-if)#
```

Related Commands

show queue bandwidth (4-174)

queue cos-map

This command assigns class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 7). Use the **no** form set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The ID of the priority queue.
- Ranges are 0 to 7, where 7 is the highest priority queue.
- *cos1 .. cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using eight priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown below.

Table 4-62. Default CoS Priority Levels

Queue	0	1	2	3	4	5	6	7
Priority	2	0	1	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- CoS values assigned at the ingress port are also used at the egress port.
- This command sets the CoS priority for all interfaces.

Example

The following example shows how to change the CoS assignments to a one-to-one mapping.

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Console#
```

Related Commands

show queue cos-map (4-174)

show queue mode

This command shows the current queue mode.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#sh queue mode

Wrr status: Enabled
Console#
```

show queue bandwidth

This command displays the weighted round-robin (WRR) bandwidth allocation for the eight priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
    0        1
    1        2
    2        4
    3        6
    4        8
    5        10
    6        12
    7        14
.
.
.
```

show queue cos-map

This command shows the class of service priority map.

Syntax

show queue cos-map [*interface*]

interface

- **ethernet** *unit*/*port*
  - unit - Stack unit. (Always unit 1)
  - port - Port number. (Range: 1-28)
- **port-channel** *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value     : 0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```

Priority Commands (Layer 3 and 4)

Table 4-63. Priority Commands (Layer 3 and 4)

Command	Function	Mode	Page
map ip dscp	Enables IP DSCP class of service mapping	GC	4-175
map ip dscp	Maps IP DSCP value to a class of service	IC	4-176
map access-list ip	Sets the CoS value and corresponding output queue for packets matching an ACL rule	IC	4-93
show map ip dscp	Shows the IP DSCP map	PE	4-177
show map access-list ip	Shows CoS value mapped to an access list for an interface	PE	4-94

map ip dscp (Global Configuration)

This command enables IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

[no] map ip dscp

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP DSCP, and default switchport priority.

Example

The following example shows how to enable IP DSCP mapping globally.

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

This command sets IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

Syntax

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

- *dscp-value* - 8-bit DSCP value. (Range: 0-255)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 4-64. Mapping IP DSCP to CoS Values

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0.

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

show map ip dscp

This command shows the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

interface

- **ethernet** *unit*/*port*
  - unit - Stack unit. (Always unit 1)
  - port - Port number. (Range: 1-28)
- **port-channel** *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port       DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
.
.
.
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Related Commands

map ip dscp (Global Configuration) (4-175)

map ip dscp (Interface Configuration) (4-176)

Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Table 4-65. Multicast Filtering Commands

Command Groups	Function	Page
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, displays current snooping and query settings, and displays the multicast service and group members	4-178
IGMP Query	Configures IGMP query parameters for multicast filtering at Layer 2	4-182
Static Multicast Routing	Configures static multicast router ports	4-185

IGMP Snooping Commands

Table 4-66. IGMP Snooping Commands

Command	Function	Mode	Page
ip igmp snooping	Enables IGMP snooping	GC	4-178
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	*4-179*
ip igmp snooping version	Configures the IGMP version for snooping	GC	4-179
ip igmp snooping immediate-leave	Enables IGMP immediate leave for a VLAN interface.	IC	4-180
show ip igmp snooping	Shows the IGMP snooping and query configuration	PE	4-180
show mac-address-table multicast	Shows the IGMP snooping MAC multicast list	PE	*4-181*

ip igmp snooping

This command enables IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping**

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

This command adds a port to a multicast group. Use the **no** form to remove the port.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **static** *ip-address interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *ip-address* - IP address for multicast group
- *interface*
  - **ethernet** *unit*/*port*
    - unit - Stack unit. (Always unit 1)
    - port - Port number. (Range: 1-28)
  - **port-channel** *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Global Configuration

Example

The following shows how to statically configure a multicast group on a port.

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

ip igmp snooping version

This command configures the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping version {**1** | **2**}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp query-timeout**.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

ip igmp snooping immediate-leave

This command enables IGMP immediate leave for specific VLAN. Use the no form to disable the feature for a VLAN.

Syntax

[no] ip igmp snooping immediate-leave

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

The IGMP snooping immediate-leave feature enables a Layer 2 LAN interface to be removed from the multicast forwarding table without first sending an IGMP group-specific query to the interface. Upon receiving a group-specific IGMPv2 leave message, the switch immediately removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp snooping immediate-leave
Console(config-if)#
```

show ip igmp snooping

This command shows the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Configuring IGMP Snooping and Query Parameters” on page 3-162 for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service status:          Enabled
 Querier status:          Disabled
 Query count:             2
 Query interval:          125 sec
 Query max response time: 10 sec
 Router port expire time: 300 sec
 IGMP snooping version:   Version 2
Console#
```

show mac-address-table multicast

This command shows known multicast addresses.

Syntax

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* - VLAN ID (1 to 4093)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/11    IGMP
Console#
```

IGMP Query Commands (Layer 2)

Table 4-67. IGMP Query Commands (Layer 2)

Command	Function	Mode	Page
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	4-182
ip igmp snooping query-count	Configures the query count	GC	4-182
ip igmp snooping query-interval	Configures the query interval	GC	4-183
ip igmp snooping query-max-response-time	Configures the report delay	GC	4-184
ip igmp snooping router-port-expire-time	Configures the query timeout	GC	4-185

ip igmp snooping querier

This command enables the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping querier**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

This command configures the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max-response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

ip igmp snooping query-max-response-time (4-184)

ip igmp snooping query-interval

This command configures the query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds.

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

This command configures the query report delay. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-25)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds.

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version (4-179)

ip igmp snooping query-max-response-time (4-184)

ip igmp snooping router-port-expire-time

This command configures the query timeout. Use the **no** form to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired.
(Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must use IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds.

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

Related Commands

ip igmp snooping version (4-179)

Static Multicast Routing Commands

Table 4-68. Static Multicast Routing Commands

Command	Function	Mode	Page
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	4-185
show ip igmp snooping mrouter	Shows multicast router ports	PE	4-186

ip igmp snooping vlan mrouter

This command statically configures a multicast router port. Use the **no** form to remove the configuration.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *interface*

- **ethernet** *unit*/*port*
  - unit - Stack unit. (Always unit 1)
  - port - Port number. (Range: 1-28)
- **port-channel** *channel-id* (Range: 1-8)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4093)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static or Dynamic.

Example

The following shows that port 11 in VLAN 1 is attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------ -------
    1            Eth 1/11  Static
    2            Eth 1/12  Dynamic
Console#
```

IGMP Filtering and Throttling Commands

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port and IGMP throttling limits the number of simultaneous multicast groups a port can join.

Table 4-69. IGMP Filtering and Throttling Commands

Command	Function	Mode	Page
ip igmp filter	Enables IGMP filtering and throttling on the switch	GC	4-187
ip igmp profile	Sets a profile number and enters IGMP filter profile configuration mode	GC	4-188
permit, deny	Sets a profile access mode to permit or deny	IPC	4-189
range	Specifies one or a range of multicast addresses for a profile	IPC	4-189
ip igmp filter	Assigns an IGMP filter profile to an interface	IC	4-190
ip igmp max-groups	Specifies an IGMP throttling number for an interface	IC	4-191
ip igmp max-groups action	Sets the IGMP throttling action for an interface	IC	4-191
show ip igmp filter	Displays the IGMP filtering status	PE	4-192
show ip igmp profile	Displays IGMP profiles and settings	PE	4-193
show ip igmp throttle interface	Displays the IGMP throttling setting for interfaces	PE	4-193

ip igmp filter (Global Configuration)

This command globally enables IGMP filtering and throttling on the switch. Use the **no** form to disable the feature.

Syntax

[no] ip igmp filter

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- IGMP filtering enables you to assign a profile to a switch port that specifies multcast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses, but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.
- IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.
- The IGMP filtering feature operates in the same manner when MVR is used to forward the multicast traffic.

Example

```
Console(config)#ip igmp filter
Console(config)#
```

ip igmp profile

This command creates an IGMP filter profile number and enters IGMP profile configuration mode. Use the **no** form to delete a profile number.

Syntax

[no] ip igmp profile *profile-number*

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

permit, deny

This command sets the access mode for an IGMP filter profile. Use the **no** form to delete a profile number.

Syntax

{permit | deny}

Default Setting

Deny

Command Mode

IGMP Profile Configuration

Command Usage

- Each profile has only one access mode; either permit or deny.
- When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when a multicast group is not in the controlled range.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

range

This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

Syntax

[**no**] **range** *low-ip-address* [*high-ip-address*]

- *low-ip-address* - A valid IP address of a multicast group or start of a group range.
- *high-ip-address* - A valid IP address for the end of a multicast group range.

Default Setting

None

Command Mode

IGMP Profile Configuration

Command Usage

Enter this command multiple times to specify more than one multicast address or address range for a profile.

Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
```

ip igmp filter (Interface Configuration)

This command assigns an IGMP filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

Syntax

[**no**] **ip igmp filter** *profile-number*

- *profile-number* - An IGMP filter profile number. (Range: 1-4294967295)

Default Setting

None

Command Mode

Interface Configuration

Command Usage

- The IGMP filtering profile must first be created with the **ip igmp profile** command before being able to assign it to an interface.
- Only one profile can be assigned to an interface.
- A profile can be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

ip igmp max-groups

This command sets the IGMP throttling number for an interface on the switch. Use the **no** form to restore the default setting.

Syntax

ip igmp max-groups *number*
no ip igmp max-groups

- *number* - The maximum number of multicast groups an interface can join at the same time.

Default Setting

64

Command Mode

Interface Configuration

Command Usage

- IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.
- IGMP throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

ip igmp max-groups action

This command sets the IGMP throttling action for an interface on the switch.

Syntax

ip igmp max-groups action <replace | deny>

- **replace** - The new multicast group replaces an existing group.
- **deny** - The new multicast group join report is dropped.

Default Setting

Deny

Command Mode

Interface Configuration

Command Usage

When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

show ip igmp filter

This command displays the global and interface settings for IGMP filtering.

Syntax

show ip igmp filter [*interface*]

- interface
  - **ethernet** unit/port
    - *unit* - This is unit 1.
    - *port* - Port number. (Range: 1-28)
  - **port-channel** *channel-id* (Range: 1-4)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip igmp filter
IGMP filter enable
Console#show ip igmp filter interface ethernet 1/1
Information of Eth 1/1
 IGMP Profile 19
  deny
  range 239.1.1.1 239.1.1.1
  range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp profile

This command displays IGMP filtering profiles created on the switch.

Syntax

show ip igmp profile [*profile-number*]

- *profile-number* - An existing IGMP filter profile number. (Range: 1-4294967295)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
  deny
  range 239.1.1.1 239.1.1.1
  range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp throttle interface

This command displays the interface settings for IGMP throttling.

Syntax

show ip igmp throttle interface [*interface*]

- interface
  - **ethernet** unit/port
    - *unit* - This is unit 1.
    - *port* - Port number. (Range: 1-28)
  - **port-channel** *channel-id* (Range: 1-4)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ip igmp throttle interface ethernet 1/1
Information of Eth 1/1
  status : TRUE
  action : deny
  max multicast groups : 32
  current multicast groups : 0
Console#
```

Multicast VLAN Registration Commands

This section describes commands used to configure Multicast VLAN Registration (MVR). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider’s network. Any multicast traffic entering an MVR VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

Table 4-70. Multicast VLAN Registration Commands

Command	Function	Mode	Page
mvr	Globally enables MVR, statically configures MVR group address(es), or specifies the MVR VLAN identifier	GC	4-194
mvr	Configures an interface as an MVR receiver or source port, enables immediate leave capability, or configures an interface as a static member of the MVR VLAN	IC	4-195
show mvr	Shows information about the global MVR configuration settings, the interfaces attached to the MVR VLAN, or the multicast groups assigned to the MVR VLAN	PE	4-197

mvr (Global Configuration)

This command enables Multicast VLAN Registration (MVR) globally on the switch, statically configures MVR multicast group IP address(es) using the **group** keyword, or specifies the MVR VLAN identifier using the **vlan** keyword. Use the **no** form of this command without any keywords to globally disable MVR. Use the **no** form with the **group** keyword to remove a specific address or range of addresses. Or use the **no** form with the **vlan** keyword restore the default MVR VLAN.

Syntax

[**no**] **mvr** [**group** *ip-address* [*count*] | **vlan** *vlan-id*]

- *ip-address* - IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- *count* - The number of contiguous MVR group addresses. (Range: 1-255)
- *vlan-id* - MVR VLAN ID (Range: 1-4094)

Default Setting

- MVR is disabled.
- No MVR group address is defined.
- The default number of contiguous addresses is 0.
- MVR VLAN ID is 1.

Command Mode

Global Configuration

Command Usage

- Use the **mvr group** command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated an MVR group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see **ip igmp snooping** on page 4-178). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

Example

The following example enables MVR globally, and configures a range of MVR group addresses:

```
Console(config)#mvr
Console(config)#mvr group 228.1.23.1 10
Console(config)#
```

mvr (Interface Configuration)

This command configures an interface as an MVR receiver or source port using the **type** keyword, enables immediate leave capability using the **immediate** keyword, or configures an interface as a static member of the MVR VLAN using the **group** keyword. Use the **no** form to restore the default settings.

Syntax

[**no**] **mvr** {**type** {**receiver** | **source**}| **immediate | group** *ip-address*}

- **receiver** - Configures the interface as a subscriber port that can receive multicast data.
- **source** - Configure the interface as an uplink port that can send and receive multicast data for the configured multicast groups.
- **immediate** - Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group.
- *ip-address* - Statically configures an interface to receive multicast traffic from the IP address specified for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Default Setting

- The port type is not defined.
- Immediate leave is disabled.
- No receiver port is a member of any configured multicast group.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- A port which is not configured as an MVR receiver or source port can use IGMP snooping to join or leave multicast groups using the standard rules for multicast filtering.
- MVR receiver ports cannot be members of a trunk. Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. IGMP snooping can be used to allow a receiver port to dynamically join or leave multicast groups within the MVR VLAN. Multicast groups can also be statically assigned to a receiver port using the **group** keyword.
- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through IGMP snooping or which have been statically assigned using the **group** keyword.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
- Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
- Immediate leave does not apply to multicast groups which have been statically assigned to a port.
- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see **ip igmp snooping** on page 4-178). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

Example

The following configures one source port and several receiver ports on the switch, enables immediate leave on one of the receiver ports, and statically assigns a multicast group to another receiver port:

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr type receiver
Console(config-if)#mvr immediate
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#mvr group 225.0.0.5
Console(config-if)#
```

show mvr

This command shows information about the global MVR configuration settings when entered without any keywords, the interfaces attached to the MVR VLAN using the **interface** keyword, or the multicast groups assigned to the MVR VLAN using the **members** keyword.

Syntax

show mvr [**interface** [*interface*]| **members** [*ip-address*]]

- interface
  - **ethernet** unit/port
    - *unit* - This is unit 1.
    - *port* - Port number. (Range: 1-28)
  - **port-channel** *channel-id* (Range: 1-12)
  - ip-address - IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Default Setting

Displays global configuration settings for MVR when no keywords are used.

Command Mode

Privileged Exec

Command Usage

Enter this command without any keywords to display the global settings for MVR. Use the **interface** keyword to display information about interfaces attached to the MVR VLAN. Or use the **members** keyword to display information about multicast groups assigned to the MVR VLAN.

Example

The following shows the global MVR settings:

```
Console#show mvr
MVR Status:enable
MVR running status:TRUE
MVR multicast vlan:1
MVR Max Multicast Groups:255
MVR Current multicast groups:10
Console#
```

Table 4-71. show mvr - display description

Field	Description
MVR status	Shows if MVR is globally enabled on the switch.
MVR running status	Indicates whether or not all necessary conditions in the MVR environment are satisfied.
MVR multicast vlan	Shows the VLAN used to transport all MVR multicast traffic.
MVR max multicast groups	Shows the maximum number of multicast groups which can assigned to the MVR VLAN.
MVR current multicast groups	Shows the number of multicast groups currently assigned to the MVR VLAN.

The following displays information about the interfaces attached to the MVR VLAN:

```
Console#show mvr interface
Port    Type            Status          Immediate Leave
------- --------        -------------   ---------------
eth1/1  SOURCE          ACTIVE/UP         Disable
eth1/2  RECEIVER        ACTIVE/UP         Disable
eth1/5  RECEIVER        INACTIVE/DOWN     Disable
eth1/6  RECEIVER        INACTIVE/DOWN     Disable
eth1/7  RECEIVER        INACTIVE/DOWN     Disable
Console#
```

Table 4-72. show mvr interface - display description

Field	Description
Port	Shows interfaces attached to the MVR.
Type	Shows the MVR port type.
Status	Shows the MVR status and interface status. MVR status for source ports is “ACTIVE” if MVR is globally enabled on the switch. MVR status for receiver ports is “ACTIVE” only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.
Immediate Leave	Shows if immediate leave is enabled or disabled.

The following shows information about the interfaces associated with multicast groups assigned to the MVR VLAN:

```
Console#show mvr members
MVR Group IP      Status    Members
----------------  --------  -------
225.0.0.1         ACTIVE    eth1/1(d), eth1/2(s)
225.0.0.2         INACTIVE  None
225.0.0.3         INACTIVE  None
225.0.0.4         INACTIVE  None
225.0.0.5         INACTIVE  None
225.0.0.6         INACTIVE  None
225.0.0.7         INACTIVE  None
225.0.0.8         INACTIVE  None
225.0.0.9         INACTIVE  None
225.0.0.10        INACTIVE  None
Console#
```

Table 4-73. show mvr members - display description

Field	Description
MVR Group IP	Multicast groups assigned to the MVR VLAN.
Status	Shows whether or not the there are active subscribers for this multicast group. Note that this field will also display “INACTIVE” if MVR is globally disabled.
Members	Shows the interfaces with subscribers for multicast services provided through the MVR VLAN. Also shows if an interface has dynamically joined a multicast group (d), or if a multicast group has been statically bound to the interface (s).

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers. This information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Table 4-74. LLDP Commands

Command	Function	Mode	Page
lldp transmit-interval	Configures the periodic transmit interval for LLDP advertisements	GC	*4-201*
lldp transmit-delay	Configures a delay time between the successive transmission of advertisements initiated by a change in local LLDP MIB variables	GC	*4-201*

Table 4-74. LLDP Commands

Command	Function	Mode	Page
lldp transmit-hold	Configures the time-to-live (TTL) value sent in LLDP advertisements	GC	4-202
lldp reinit-delay	Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down	GC	4-202
lldp notification-interval	Configures the allowed interval for sending SNMP notifications about LLDP changes	GC	4-203
lldp	Enables LLDP transmit, receive, or transmit and receive mode on the specified port	IC	4-204
lldp basic-tlv management-address	Configures an LLDP-enabled port to advertise the management address for this device	IC	4-204
lldp basic-tlv description	Configures an LLDP-enabled port to advertise its port description	IC	4-205
lldp basic-tlv system-capabilities	Configures an LLDP-enabled port to advertise its system capabilities	IC	4-206
lldp basic-tlv system-description	Configures an LLDP-enabled port to advertise the system description	IC	4-206
lldp basic-tlv system-name	Configures an LLDP-enabled port to advertise its system name	IC	4-207
lldp notification	Enables the transmission of SNMP trap notifications about LLDP changes	IC	4-207
lldp dot1-tlv port-vlan-id*	Configures an LLDP-enabled port to advertise its default VLAN ID	IC	4-208
lldp dot1-tlv port-protocol-vlan-id*	Configures an LLDP-enabled port to advertise portrelated VLAN information	IC	4-209
lldp dot1-tlv vlan-name*	Configures an LLDP-enabled port to advertise its VLAN name	IC	4-209
lldp dot1-tlv protocol-identity*	Configures an LLDP-enabled port to advertise the supported protocols	IC	4-210
lldp dot3-tlv mac-phy	Configures an LLDP-enabled port to advertise its MAC and physical layer capabilities	IC	4-210
lldp dot3-tlv link-aggregation	Configures an LLDP-enabled port to advertise its link aggregation capabilities	IC	4-211
lldp dot3-tlv power-via-mdi	Configures an LLDP-enabled port to advertise its Power-over-Ethernet capabilities	IC	4-211
lldp dot3-tlv maximum-frame-size	Configures an LLDP-enabled port to advertise its maximum frame size	IC	4-212
show lldp config	Shows LLDP configuration settings for all ports	PE	4-212
show lldp info local-device	Shows LLDP global and interface-specific configuration settings for this device	PE	4-213
show lldp info remote-device	Shows LLDP global and interface-specific configuration settings for remote devices	PE	4-214

Table 4-74. LLDP Commands

Command	Function	Mode	Page
show lldp info statistics	Shows statistical counters all LLDP-enabled interfaces	PE	4-215
* Vendor-specific options may or may not be advertised by neighboring devices.			

lldp transmit-interval

This command configures the periodic transmit interval for LLDP advertisements. Use the **no** form to restore the default setting.

Syntax

lldp transmit-interval <*seconds*>

no lldp transmit-delay

- *seconds* - Specifies the periodic interval at which LLDP advertisements are sent. (Range: 5 - 32768 seconds)

Default Setting

30 seconds

Command Mode

Global Configuration

Example

```
Console(config)#lldp transmit- interval 60
Console(config)#
```

lldp transmit-delay

This command configures a delay time between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Use the **no** form to restore the default setting.

Syntax

lldp transmit-delay {**auto** | <*seconds*>}
no lldp transmit-delay

- **auto** - Calculates the transmit delay in seconds based on ‘0.25’ transmit-interval (see page 535). The range of the resulting values is 1 - 8192.
- *seconds* - Specifies the transmit delay. (Range: 5 -3600 seconds)

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

- The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

Example

```
Console(config)#lldp transmit-delay 10
Console(config)#
```

lldp transmit-hold

This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the **no** form to restore the default setting.

Syntax

lldp transmit-hold <*value*>
no lldp transmit-hold

- *value* - Calculates the TTL in seconds based on transmit-hold * transmit-interval (Range: 2 - 10)

Default Setting

4 (4*30 = 120 seconds)

Command Mode

Global Configuration

Command Usage

- The transmit hold tells the receiving LLDP agent how long to hold onto all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

Example

```
Console(config)#lldp transmit-hold 10
Console(config)#
```

lldp reinit-delay

This command configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Use the **no** form to restore the default setting.

Syntax

lldp reinit-delay <*seconds*>
no lldp reinit-delay

- *seconds* - Specifies the delay before attempting to re-initialize LLDP. (Range: 5 - 10 seconds)

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

- When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

Example

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp notification-interval

This command configures the allowed interval for sending SNMP notifications about LLDP MIB changes. Use the **no** form to restore the default setting.

Syntax

lldp notification-interval <*seconds*>
no lldp notification-interval

- *seconds* - Specifies the periodic interval at which SNMP notifications are sent. (Range: 5 - 3600 seconds)

Default Setting

5 seconds

Command Mode

Global Configuration

Command Usage

- This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.
- Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or

transmission loss.

Example

```
Console(config)#lldp notification-interval 30
Console(config)#
```

lldp

This command enables LLDP transmit, receive, or transmit and receive mode on the specified port. Use the **no** form to restore the default setting.

Syntax

lldp {*transmit-and-receive* | *transmit-only* | *receive-only*}
no lldp

- *transmit-and-receive* - Both transmit and receive LLDP Protocol Data Units (PDUs).
- *transmit-only* - Only transmit LLDP PDUs.
- *receive-only* - Only receive LLDP PDUs.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp transmit-and-receive
Console(config-if)#
```

lldp basic-tlv management-address

This command configures an LLDP-enabled port to advertise the management address for this device. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp basic-tlv management-address**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The management address protocol packet includes the IPv4 address of the ECN430-switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
- The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications perform network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.
- Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.
- Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp basic-tlv management-address
```

lldp basic-tlv description

This command configures an LLDP-enabled port to advertise its port description. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp basic-tlv description**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp basic-tlv description
Console(config-if)#
```

lldp basic-tlv system-capabilities

This command configures an LLDP-enabled port to advertise its system capabilities. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp basic-tlv system-capabilities**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description

This command configures an LLDP-enabled port to advertise the system description. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp basic-tlv system-description**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name

This command configures an LLDP-enabled port to advertise the system name. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp basic-tlv system-name**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The system name is taken from the sysName object in RFC 3418, which contains the systemís administratively assigned name, and is in turn based on the **hostname** command (page 56).

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp notification

This command enables the transmission of SNMP trap notifications about LLDP changes. Use the **no** form to restore the default setting.

Syntax

[**no**] **lldp notification**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This option sends out SNMP trap notifications to designated target stations at the interval specified by the **lldp notificationinterval** command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- SNMP trap destinations are defined using the **snmp-server host** command.
- Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp notification
Console(config-if)#
```

lldp dot1-tlv port-vlan-id

This command configures an LLDP-enabled port to advertise its default VLAN ID. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot1-tlv port-vlan-id**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp dot1-tlv port-vlan-id
Console(config-if)#
```

lldp dot1-tlv port-protocol-vlan-id

This command configures an LLDP-enabled port to advertise port-related VLAN information. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot1-tlv port-protocol-vlan-id**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This option advertises the port-based and protocol-based VLANs configured on this interface.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp dot1-tlv port-protocol-vlan-id
Console(config-if)#
```

lldp dot1-tlv vlan-name

This command configures an LLDP-enabled port to advertise its VLAN name. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot1-tlv vlan-name**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This option advertises the name of all VLANs to which this interface has been assigned.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp dot1-tlv port-vlan-id
Console(config-if)#
```

lldp dot1-tlv protocol-identity

This command configures an LLDP-enabled port to advertise the supported protocols. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot1-tlv protocol-identity**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This option advertises the protocols that are accessible through this interface.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp dot1-tlv protocol-identity
Console(config-if)#
```

lldp dot3-tlv mac-phy

This command configures an LLDP-enabled port to advertise its MAC and physical layer capabilities. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot3-tlv mac-phy**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This option advertises MAC/PHY configuration/status which includes information about auto-negotiation capabilities, port speed, and duplex mode.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp dot3-tlv mac-phy
Console(config-if)#
```

lldp dot3-tlv link-aggregation

This command configures an LLDP-enabled port to advertise its link aggregation capabilities. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot3-tlv link-aggregation**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This option advertises link aggregation capabilities, aggregation status of the link, and the 802.3 aggregated port identifier if this interface is currently a link aggregation member.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp dot3-tlv link-aggregation
Console(config-if)#
```

lldp dot3-tlv power-via-mdi

This command configures an LLDP-enabled port to advertise its Power-over-Ethernet (PoE) capabilities. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot3-tlv power-via-mdi**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This option advertises Power-over-Ethernet capabilities, including whether or not PoE is supported, currently enabled, if the port pins through which power is delivered can be controlled, the port pins selected to deliver power, and the power class.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp dot3-tlv power-via-mdi
Console(config-if)#
```

lldp dot3-tlv maximum-frame-size

This command configures an LLDP-enabled port to advertise its maximum frame size. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot3-tlv maximum-frame-size**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Refer to System MTU Commands on page 65 for information on configuring the maximum frame size for the ECN430-switch.

Example

```
Console(config)#interface ge1/1
Console(config-if)#lldp dot3-tlv maximum-frame-size
Console(config-if)#
```

show lldp config

This command shows LLDP configuration settings for all ports.

Syntax

show lldp config [**detail**]

- **detailed** - Shows detailed information.

Command Mode

Privileged Exec

Example

switch#show lldp config

```
Console#show lldp config
LLDP Global Configuation
LLDP Transmit interval : 30
LLDP Hold Time Multiplier : 4
LLDP Delay Interval : 2
LLDP Reinit Delay : 2
LLDP Notification Interval : 5

LLDP Port Configuration
Port AdminStatus NotificationEnabled
-------- + ---------- ------------------
ge1/1 Rx False
ge1/2 Rx False
ge1/3 Rx False
ge1/4 Rx False
... ge1/5 Rx False


switch#show lldp config detail
LLDP Port Configuration Detail
Port : ge1/1
Admin Status : Rx
...Notification Enabled : False
```

show lldp info local-device

This command shows LLDP global and interface-specific configuration settings for this device.

Syntax

show lldp info local-device [**detail**]

- **detail** - Shows detailed information.

Command Mode

Privileged Exec

Example

```
Console#show lldp info local-device
LLDP Local System Information
Chassis Type : MAC Address
Chassis ID : 00-01-22-33-44-AB
System Description : ECN430
System Capabilities Support : Bridge, Router
System Capabilities Enable : Bridge, Router
Management Address : 0.0.0.0 (IPv4)
LLDP Port Information
Port | PortID Type PortID PortDesc
----- + ---------------- ---------------- -----------------
ge1/1 MAC Address 00-01-22-33-44-AC ge1/1
ge1/2 MAC Address 00-01-22-33-44-AD ge1/2
ge1/3 MAC Address 00-01-22-33-44-AE ge1/3
ge1/4 MAC Address 00-01-22-33-44-AF ge1/4
... ge1/5 MAC Address 00-01-22-33-44-B0 ge1/5

Console#show lldp info local-device detail
LLDP Port Information Detail
Port : ge1/1
Port Type : MAC Address
Port ID : 00-01-22-33-44-AC
...P ort Desc : ge1/1
```

show lldp info remote-device

This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

Syntax

show lldp info remote-device [**detail**]

- **detailed** - Shows detailed information.

Command Mode

Privileged Exec

Example

```
switch#show lldp info remote-device
LLDP Remote Devices Information
Interface | ChassisId PortId SysName
--------- + ----------------- ---------------- ------------
please provide sample data
switch#show lldp info remote-device detail
LLDP Remote Devices Information
please provide sample data
switch#
```

show lldp info statistics

This command shows statistical counters all LLDP-enabled interfaces.

Syntax

show lldp info statistics [**detail**]

- **detailed** - Shows detailed information.

Command Mode

Privileged Exec

Example

```
switch#show lldp info statistics
LLDP Device Statistics
Neighbor Entries List Last Updated : 0 seconds
New Neighbor Entries Count : 0
Neighbor Entries Deleted Count : 0
Neighbor Entries Dropped Count : 0
Neighbor Entries Ageout Count : 0
Port | NumFramesRecvd NumFramesSent NumFramesDiscarded
----- + -------------- ------------ -----------------
1 | 0 0 0
2 | 0 0 0
3 | 0 0 0
4 | 0 0 0
... 5 | 0 0 0
switch#sh lldp info statistics detail
LLDP Port Statistics Detail
PortName : ge1/1
Frames Discarded : 0
Frames Invalid : 0
Frames Received : 0
Frames Sent : 0
TLVs Unrecognized : 0
TLVs Discarded : 0
... Ne ighbor Ageouts
```

UPnP

Universal Plug and Play (UPnP) is a set of computer network protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards.

Given an IP address, the first step in UPnP networking is discovery. When a device is added to the network, the UPnP discovery protocol allows that device to advertise its services to control points on the network. Similarly, when a control point is added to the network, the UPnP discovery protocol allows that control point to search for devices of interest on the network.

The next step in UPnP networking is description. After a control point has discovered a device, the control point still knows very little about the device. For the control point to learn more about the device and its capabilities, or to interact with the device, the control point must retrieve the device's description from the URL provided by the device in the discovery message.

After a control point has retrieved a description of the device, the control point can send actions to a device's service. To do this, a control point sends a suitable control message to the control URL for the service (provided in the device description).

The next step in UPnP networking is event notification, or "eventing". A UPnP description for a service includes a list of actions the service responds to and a list of variables that model the state of the service at run time. The service publishes updates when these variables change, and a control point may subscribe to receive this information. The service publishes updates by sending event messages.

The final step in UPnP networking is presentation. If a device has a URL for presentation, then the control point can retrieve a page from this URL, load the page into a web browser, and depending on the capabilities of the page, allow a user to control the device and/or view device status. The degree to which each of these can be accomplished depends on the specific capabilities of the presentation page and device.

UPnP Configuration

Table 4-75. UPnP Commands

Command	Function	Mode	Page
upnp device	Enables/disables UPnP on the network	GC	4-217
upnp device ttl	Sets the time-to-live (ttl) value.	GC	4-217
upnp device advertise duration	Sets the advertisement duration of the device	GC	4-218
show upnp	Displays UPnP status and parameters	PE	4-218

upnp device

This command enables UPnP on the device. Use the **no** form to disable UPnP.

Syntax

[**no**] **upnp device**}

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

You must enable UPnP before you can configure time out settings for sending of UPnP messages.

Example

In the following example, UPnP is enabled on the device.

```
Console(config)#upnp device
Console(config)#
```

Related Commands

upnp device ttl (4-217)
upnp device advertise duration (4-218)

upnp device ttl

This command sets the time-to-live (ttl) value for receiving of UPnP messages on the device.

Syntax

upnp device ttl {*value*}

- *value* - A time out value expressed in seconds. (Range: 1-255 seconds)

Default Setting

4 seconds

Command Mode

Global Configuration

Command Usage

You must set the ttl value before the device can listen for UPnP messages. After the ttl has expired, the device will listen again for new UPnP information.

Example

In the following example, the ttl is set to 20 seconds.

```
Console(config)#upnp device ttl 20
Console(config)#
```

Related Commands

upnp device advertise duration (4-218)

upnp device advertise duration

This command sets the duration of which a device will advertise its status to the control point.

Syntax

upnp device advertise duration {*value*}

- *value* - A time out value expressed in seconds. (Range: 6-86400 seconds)

Default Setting

100 seconds

Command Mode

Global Configuration

Command Usage

You must set the time for which the attached devices advertise their status.

Example

In the following example, the device advertise duration is set to 200 seconds.

```
Console(config)#upnp device advertise duration 200
Console(config)#
```

Related Commands

upnp device ttl (4-217)

show upnp

This command displays the UPnP management status and time out settings.

Default Setting

All interfaces

Command Mode

Privileged Exec

Example

```
Console#show upnp
UPnP global settings:
 Status:                  Enabled
 Advertise duration:      200
 TTL:                     20
Console#
```

IP Interface Commands

An IP addresses may be used for management access to the switch over your network. The IP address for this switch is obtained via DHCP by default. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server when it is powered on. You may also need to a establish a default gateway between this device and management stations or other devices that exist on another network segment.

Basic IP Configuration

Table 4-76. IP Interface Commands

Command	Function	Mode	Page
ip address	Sets the IP address for the current interface	IC	4-219
ip dhcp restart	Submits a BOOTP or DCHP client request	PE	4-220
ip default-gateway	Defines the default gateway through which this switch can reach other subnetworks	GC	4-221
show ip interface	Displays the IP settings for this device	PE	4-222
show ip redirects	Displays the default gateway configured for this device	PE	4-222
ping	Sends ICMP echo request packets to another node on the network	NE, PE	4-222

ip address

This command sets the IP address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**}
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.

Default Setting

DHCP

Command Mode

Interface Configuration (VLAN)

Command Usage

- You must assign an IP address to this device to gain management access over the network. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
- If you select the **bootp** or **dhcp** option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- You can start broadcasting BOOTP or DHCP requests by entering an **ip dhcp restart** command, or by rebooting the switch.

Note: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart (4-220)

ip dhcp restart

This command submits a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode via the **ip address** command.

- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: Dhcp.
Console#
```

Related Commands

ip address (4-219)

ip default-gateway

This command establishes a static route between this switch and devices that exist on another network segment. Use the **no** form to remove the static route.

Syntax

ip default-gateway *gateway*
no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

A gateway must be defined if the management station is located in a different IP segment.

Example

The following example defines a default gateway for this device.

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

Related Commands

show ip redirects (4-222)

show ip interface

This command displays the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Example

```
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Related Commands

show ip redirects (4-222)

show ip redirects

This command shows the default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain. (4-221)

ping

This command sends ICMP echo request packets to another node on the network.

Syntax

ping *host* [**size** *size*] [**count** *count*]

- *host* - IP address or IP alias of the host.
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32)
  The actual packet size will be eight bytes larger than the size specified

because the switch adds header information.
- *count* - Number of packets to send. (Range: 1-16, default: 5)

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- Following are some results of the **ping** command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface (4-111)

IP Source Guard Commands

IP Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or static and dynamic entries in the DHCP Snooping table when enabled (see “DHCP Snooping Commands” on page 4-227). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands used to configure IP Source Guard.

Table 4-77. IP Source Guard Commands

Command	Function	Mode	Page
ip source-guard	Configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address	IC	4-224
ip source-guard binding	Adds a static address to the source-guard binding table	GC	4-225
show ip source-guard	Shows whether source guard is enabled or disabled on each interface	PE	4-227
show ip source-guard binding	Shows the source guard binding table	PE	4-227

ip source-guard

This command configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. Use the no form to disable this function.

Syntax

[**no**] **ip source-guard** {sip | sip-mac}

- sip - Filters traffic based on IP addresses stored in the binding table.
- sip-mac - Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Source guard is used to filter traffic on an unsecure port which receives messages from outside the network or firewall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.
- Setting source guard mode to “sip” or “sip-mac” enables this function on the selected port. Use the “sip” option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the “sip-mac” option to check these same parameters, plus the source MAC address. Use the **no source guard** command to disable this function on the selected port.
- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, static entries configured in the DHCP snooping table, or static addresses configured in the source guard binding table.
- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, Static-DHCP-Binding),

VLAN identifier, and port identifier.

- Static addresses entered in the source guard binding table with the **ip source-guard binding** command (page *4-225*) are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself; static entries include a manually configured lease time.
- If the IP source guard is enabled, an inbound packet's IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- Filtering rules are implemented as follows:
  - If the DHCP snooping is disabled (page *4-228*), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.
  - If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, static DHCP snooping binding or dynamic DHCP snooping binding, the packet will be forwarded.
  - If IP source guard if enabled on an interface for which IP source bindings (dynamically learned via DHCP snooping or manually configured) are not yet configured, the switch will drop all IP traffic on that port, except for DHCP packets.

Example

This example maps enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

Related Command

ip source-guard binding (4-225)

ip dhcp snooping (4-228)

ip dhcp snooping vlan (4-230)

ip source-guard binding

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

Syntax

ip source-guard *mac-address* vlan *vlan-id ip-address* interface ethernet *unit/ port*

no ip source-guard *mac-address* vlan *vlan-id*

- *mac-address* - A valid unicast MAC address.
- *vlan-id* - ID of a configured VLAN (Range: 1-4094)
- *ip-address* - A valid unicast IP address, including classful types A, B or C.
- *unit* - Stack unit. (Always unit 1)
- *port* - Port number.

Default Setting

No configured entries

Command Mode

Global Configuration

Command Usage

- Table entries include a MAC address, IP address, lease time, entry type
- (Static-IP-SG-Binding, Dynamic-DHCP-Binding, Static-DHCP-Binding), VLAN identifier, and port identifier.
- All static entries are configured with an infinite lease time, which is indicated with a value of zero by the **show ip source-guard** command (page *4-227*).
- When source guard is enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, static entries configured in the DHCP snooping table, or static addresses configured in the source guard binding table with this command.
- Static bindings are processed as follows:
  - If there is no entry with same VLAN ID and MAC address, a new entry is added to binding table using the type of static IP source guard binding.
  - If there is an entry with same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
  - If there is an entry with same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

Example

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

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1
  192.168.0.99 interface ethernet 1/5
Console(config-if)#
```

Related Command

ip source-guard (4-224)

ip dhcp snooping (4-228)

ip dhcp snooping vlan (4-230)

show ip source-guard

This command shows whether source guard is enabled or disabled on each interface.

Command Mode

Privileged Exec

Example

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

show ip source-guard binding

This command shows the source guard binding table.

Command Mode

Privileged Exec

Example

```
Console#show ip source-guard binding
MacAddress        IpAddress     Lease(sec) Type      VLAN Interface
----------------- ------------ ---------- --------- ---- ---------
11-22-33-44-55-66 192.168.0.99          0 Static       1 Eth 1/5
Console#
```

DHCP Snooping Commands

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

Table 4-78. DHCP Snooping Commands

Command	Function	Mode	Page
ip dhcp snooping	Enables DHCP snooping globally	GC	*4-228*
ip dhcp snooping vlan	Deletes entries from the host name-to-address table	GC	*4-230*
ip dhcp snooping trust	Defines a default domain name for incomplete host names	IC	*4-230*
ip dhcp snooping verify mac-address	Defines a list of default domain names for incomplete host names	GC	*4-231*
ip dhcp snooping information option	Specifies the address of one or more name servers to use for host name-to-address translation	GC	*4-232*

Table 4-78. DHCP Snooping Commands

Command	Function	Mode	Page
ip dhcp snooping information policy	Enables DNS-based host name-to-address translation	GC	4-233
ip dhcp snooping database flash	Displays the static host name-to-address mapping table	GC	4-233
show ip dhcp snooping	Displays the configuration for DNS services	PE	4-234
show ip dhcp snooping binding	Displays entries in the DNS cache	PE	4-234

ip dhcp snooping

This command enables DHCP snooping globally. Use the no form to restore the default setting.

Syntax

[**no**] **ip dhcp snooping**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or firewall. When DHCP snooping is enabled globally by this command, and enabled on a VLAN interface by the **ip dhcp snooping vlan** command (page 4-230), DHCP messages received on an untrusted interface (as specified by the **no ip dhcp snooping trust** command, page 4-230) from a device not listed in the DHCP snooping table will be dropped.
- When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- Table entries are only learned for untrusted interfaces. Each entry includes a MAC address, IP address, lease time, entry type (Dynamic-DHCP-Binding, Static-DHCP-Binding), VLAN identifier, and port identifier.
- When DHCP snooping is enabled, the rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.
- Filtering rules are implemented as follows:
  - If the global DHCP snooping is disabled, all DHCP packets are forwarded.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for

a trusted port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:
- If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
- If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
- If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled (as specified by the **ip dhcp snooping verify mac-address** command, page *4-231*). However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
- If the DHCP packet is not a recognizable type, it is dropped.
- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

• If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.
• Additional considerations when the switch itself is a DHCP client – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted (**ip dhcp snooping trust**, page *4-230*). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

Example

This example enables DHCP snooping globally for the switch.

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

Related Command

ip dhcp snooping vlan (4-230)

ip dhcp snooping trust (4-230)

ip dhcp snooping vlan

This command enables DHCP snooping on the specified VLAN. Use the **no** form to restore the default setting.

Syntax

[no] ip dhcp snooping vlan *vlan-id*

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

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- When DHCP snooping enabled globally using the **ip dhcp snooping** command (page *4-228*), and enabled on a VLAN with this command, DHCP packet filtering will be performed on any untrusted ports within the VLAN as specified by the **ip dhcp snooping trust** command (page *4-230*).
- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.
- When DHCP snooping is globally enabled, configuration changes for specific VLANs have the following effects:
  - If DHCP snooping is disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

Example

This example enables DHCP snooping for VLAN 1.

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

Related Command

ip dhcp snooping (4-228)

ip dhcp snooping trust (4-230)

ip dhcp snooping trust

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

Syntax

[**no**] **ip dhcp snooping trust**

Default Setting

All interfaces are untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.
- When DHCP snooping enabled globally using the **ip dhcp snooping** command (page *4-228*), and enabled on a VLAN with this command, DHCP packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the no **ip dhcp snooping trust** command.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- Additional considerations when the switch itself is a DHCP client – The port(s) through which it submits a client request to the DHCP server must be configured as trusted.

Example

This example sets port 5 to untrusted.

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

Related Commands

ip dhcp snooping (4-228)

ip dhcp snooping vlan (4-230)

ip dhcp snooping verify mac-address

This command verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. Use the **no** form to disable this function.

Syntax

[**no**] **ip dhcp snooping verify mac-address**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped.

Example

This example enables MAC address verification.

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```

Related Commands

ip dhcp snooping (4-228)

ip dhcp snooping vlan (4-230)

ip dhcp snooping trust (4-230)

ip dhcp snooping information option

This command enables the DHCP Option 82 information relay for the switch. Use the **no** form to disable this function.

Syntax

[no] ip dhcp snooping information option

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. Known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients.
- When the DHCP Snooping Information Option is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCP client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.
- DHCP snooping must be enabled on the switch for the DHCP Option 82 information to be inserted into packets.

Example

This example enables the DHCP Snooping Information Option.

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

ip dhcp snooping information policy

This command sets the DHCP snooping information option policy for DHCP client packets that include Option 82 information.

Syntax

ip dhcp snooping information policy <**drop** | **keep** | **replace**>

- **drop** - Discards all DHCP client packets with Option 82 information.
- **keep** - Retains the client's DHCP information
- **replace** - Overwrites the DHCP client packet information with the switch's relay information.

Default Setting

replace

Command Mode

Global Configuration

Command Usage

When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. Either the switch can drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

Example

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

ip dhcp snooping database flash

This command writes all dynamically learned snooping entries to flash memory.

Command Mode

Global Configuration

Command Usage

This command can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

Example

```
Console(config)#ip dhcp snooping database flash
Console(config)#
```

show ip dhcp snooping

This command shows the DHCP snooping configuration settings.

Command Mode

Privileged Exec

Example

```
Console#show ip dhcp snooping
Global DHCP Snooping status: disable
DHCP Snooping is configured on the following VLANs:
1
Verify Source Mac-Address: enable
Interface  Trusted
---------- ----------
Eth 1/1    No
Eth 1/2    No
Eth 1/3    No
Eth 1/4    No
Eth 1/5    Yes
.
```

show ip dhcp snooping binding

This command shows the DHCP snooping binding table entries.

Command Mode

Privileged Exec

Example

```
Console#show ip dhcp snooping binding
MacAddress        IpAddress    Lease(sec) Type   VLAN Interface
----------------- ------------ ---------- ------ ---- ---------
11-22-33-44-55-66 192.168.0.99          0  Static    1 Eth 1/5
Console#
```

Switch Cluster Commands

Switch Clustering is a method of grouping switches together to enable centralized management through a single unit. A switch cluster has a “Commander” unit that is used to manage all other “Member” switches in the cluster. The management station uses Telnet to communicate directly with the Commander throught its IP address, and the Commander manages Member switches using cluster “internal” IP addresses. There can be up to 36 Member switches in one cluster. Cluster switches are limited to within a single IP subnet.

Table 4-79. Switch Cluster Commands

Command	Function	Mode	Page
cluster	Configures clustering on the switch	GC	*4-228*
cluster commander	Configures the switch as a cluster Commander	GC	*4-230*
cluster ip-pool	Sets the cluster IP address pool for Members	GC	*4-230*
cluster member	Sets Candidate switches as cluster members	GC	*4-231*
rcommand	Provides configuration access to Member switches	GC	*4-232*
show cluster	Displays the switch clustering status	PE	*4-233*
show cluster members	Displays current cluster Members	PE	4-233
show cluster candidates	Displays current cluster Candidates in the network	PE	4-234

cluster

This command enables clustering on the switch. Use the **no** form to disable clustering.

Syntax

[no] cluster

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- To create a switch cluster, first be sure that clustering is enabled on the switch (the default is enabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with any other IP subnets in the network. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- Switch clusters are limited to a single IP subnet (Layer 2 domain).
- A switch can only be a Member of one cluster.

- Cnfigured switch clusters are maintained across power resets and network changes.

Example

```
Console(config)#cluster
Console(config)#
```

cluster commander

This command enables the switch as a cluster Commander. Use the **no** form to disable the switch as cluster Commander.

Syntax

[**no**] **cluster commander**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.
- Cluster Member switches can be managed through only using a Telnet connection to the Commander. From the Commander CLI prompt, use the **rcommand id** command to connect to the Member switch.

Example

```
Console(config)#cluster commander
Console(config)#
```

cluster ip-pool

This command sets the cluster IP address pool. Use the **no** form to reset to the default address.

Syntax

cluster ip-pool <*ip-address*>
no cluster ip-pool

- *ip-address* - The base IP address for IP addresses assigned to cluster Members. The IP address must start 10.x.x.x.

Default Setting

10.254.254.1

Command Mode

Global Configuration

Command Usage

- An “internal” IP address pool is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.member-ID. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36.
- Set a Cluster IP Pool that does not conflict with addresses in the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- You cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled.

Example

```
Console(config)#cluster ip-pool 10.2.3.4
Console(config)#
```

cluster member

This command configures a Candidate switch as a cluster Member. Use the **no** form to remove a Member switch from the cluster.

Syntax

cluster member mac-address <*mac-address*> **id** <*member-id*>
no cluster member mac-address <*member-id*>

- *mac-address* - The MAC address of the Candidate switch.
- *member-id* - The ID number to assign to the Member switch. (Range: 1-36)

Default Setting

No Members

Command Mode

Global Configuration

Command Usage

- The maximum number of cluster Members is 36.
- The maximum number of switch Candidates is 100.

Example

```
Console(config)#cluster member mac-address 00-12-34-56-78-9a id 5
Console(config)#
```

rcommand

This command provides access to a cluster Member CLI for configuration.

Syntax

rcommand id *<member-id>*

- *member-id* - The ID number to assign to the Member switch. (Range: 1-36)

Command Mode

Privileged Exec

Command Usage

- This command only operates through a Telnet connection to the Commander switch. Managing cluster Members using the local console CLI on the Commander is not supported.
- There is no need to enter the username and password for access to the Member switch CLI.

Example

```
Console#rcommand id 1

   CLI session with the SMC8124PL2 is opened.
   To end the CLI session, enter [Exit].

Console#
```

show cluster

This command shows the switch clustering configuration.

Command Mode

Privileged Exec

Example

```
Console#show cluster
Role: commander
Interval heartbeat: 30
Heartbeat loss count: 3
Number of Members: 1
Number of Candidates: 2
Console#
```

show cluster members

This command shows the current switch cluster members.

Command Mode

Privileged Exec

Example

```
Console#show cluster members
Cluster Members:
ID: 1
Role: Active member
IP Address: 10.254.254.2
MAC Address: 00-12-cf-23-49-c0
Description: SMC8124PL2
Console#
```

show cluster candidates

This command shows the discovered Candidate switches in the network.

Command Mode

Privileged Exec

Example

```
Console#show cluster candidates
Cluster Candidates:
Role          Mac               Description
------------- ----------------- --------------------------------
ACTIVE MEMBER 00-12-cf-23-49-c0 SMC8124PL2
CANDIDATE     00-12-cf-0b-47-a0 SMC8124PL2
Console#
```

Appendix A: Software Specifications

Software Features

Authentication
Local, RADIUS, TACACS, Port (802.1X), HTTPS, SSH, Port Security

Access Control Lists
IP

DHCP Client

Port Configuration
1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex
1000BASE-SX/LX/LH - 1000 Mbps at full duplex (SFP),

Flow Control
Full Duplex: IEEE 802.3x
Half Duplex: Back pressure

Broadcast Storm Control
Traffic throttled above a critical threshold

Port Mirroring
One source ports, one destination port

Rate Limits
Input Limit

Port Trunking
Static trunks (Cisco EtherChannel compliant)
Dynamic trunks (Link Aggregation Control Protocol)

Spanning Tree Algorithm
Spanning Tree Protocol (STP, IEEE 802.1D)
Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)

VLAN Support
Up to 255 groups; port-based, protocol-based, or tagged (802.1Q),
GVRP for automatic VLAN learning, private VLANs

Class of Service
Supports eight levels of priority and Weighted Round Robin Queueing
(which can be configured by VLAN tag or port),
Layer 3/4 priority mapping: IP Port, IP DSCP

Multicast Filtering
IGMP Snooping (Layer 2)

Additional Features
BOOTP client

SNTP (Simple Network Time Protocol)
SNMP (Simple Network Management Protocol)
RMON (Remote Monitoring, groups 1,2,3,9)
SMTP Email Alerts

Management Features

In-Band Management
Telnet, Web-based HTTP or HTTPS, SNMP manager, or Secure Shell

Out-of-Band Management
RS-232 DB-9 console port

Software Loading
TFTP in-band or XModem out-of-band

SNMP
Management access via MIB database
Trap management to specified hosts

RMON
Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

Standards

IEEE 802.1D Spanning Tree Protocol and traffic priorities
IEEE 802.1p Priority tags
IEEE 802.1Q VLAN
IEEE 802.1v Protocol-based VLANs
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1X Port Authentication
IEEE 802.3-2005
  Ethernet, Fast Ethernet, Gigabit Ethernet
  Link Aggregation Control Protocol (LACP)
  Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3ac VLAN tagging
DHCP Client (RFC 1541)
HTTPS
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
RADIUS+ (RFC 2618)
RMON (RFC 1757 groups 1,2,3,9)
SNMP (RFC 1157)
SNMPv2c (RFC 2571)
SNMPv3 (RFC DRAFT 3414, 3410, 2273, 3411, 3415)
SNTP (RFC 2030)
SSH (Version 2.0)
TFTP (RFC 1350)

Management Information Bases

Bridge MIB (RFC 1493)
Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP Multicasting related MIBs
MAU MIB (RFC 2668)
MIB II (RFC 1213)
Port Access Entity MIB (IEEE 802.1X)
Port Access Entity Equipment MIB
Private MIB
RADIUS Authentication Client MIB (RFC 2621)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
SNMPv2 IP MIB (RFC 2011)
SNMP Framework MIB (RFC 3411)
SNMP-MPD MIB (RFC 3412)
SNMP Target MIB, SNMP Notification MIB (RFC 3413)
SNMP User-Based SM MIB (RFC 3414)
SNMP View Based ACM MIB (RFC 3415)
SNMP Community MIB (RFC 3584)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2013)
Trap (RFC 1215)
UDP MIB (RFC 2012)

Appendix B: Troubleshooting

Problems Accessing the Management Interface

Table 2-1. Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, web browser, or SNMP software	• Be sure the switch is powered up. • Check network cabling between the management station and the switch. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. • Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. • If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. • If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot connect using Secure Shell	• If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time. • Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station. • Be sure you have generated a public key on the switch, and exported this key to the SSH client. • Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password. • Be sure you have imported the client's public key to the switch (if public key authentication is used).
Cannot access the on-board configuration program via a serial port connection	• 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 any of the following (9600, 19200, 38400, 57600, 115200 bps). • Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	• Contact SMC Technical Support for help.

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. Designate the SNMP host that is to receive the error messages.
4. Repeat the sequence of commands or other actions that lead up to the error.
5. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
6. Contact your distributor's service engineer.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
..
.
```

Glossary

Access Control List (ACL)

ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

Boot Protocol (BOOTP)

BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS)

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, or DSCP priority bit.

Differentiated Services Code Point Service (DSCP)

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Domain Name Service (DNS)

A system used for translating host names for network nodes into IP addresses.

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

Group Attribute Registration Protocol (GARP)

See Generic Attribute Registration Protocol.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s

An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1X

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MD5 Message-Digest Algorithm

An algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Authentication

See IEEE 802.1X.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Secure Shell (SSH)

A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

Simple Mail Transfer Protocol (SMTP)

A standard host-to-host mail transport protocol that operates over TCP, port 25.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Spanning Tree Protocol (STP)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

User Datagram Protocol (UDP)

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Index

Numerics

802.1x, port authentication 4-80
81047
  Heading 2
    LLDP 3-140

A

acceptable frame type 3-132, 4-155
Access Control List *See* ACL
ACL
  Extended IP 3-72, 4-88, 4-89, 4-91
  Standard IP 3-72, 4-88, 4-89, 4-90
address table 3-108, 4-135
  aging time 3-110, 4-138

B

BOOTP 3-16, 4-217, 4-218, 4-219
BPDU 3-112
broadcast storm, threshold 3-96, 4-121

C

Class of Service *See* CoS
CLI, showing commands 4-3
command line interface *See* CLI
community string 2-7, 3-36, 4-98
configuration settings, saving or restoring 2-8, 3-20, 4-64
console port, required connections 2-2
CoS
  configuring 3-145, 3-153, 4-169
  DSCP 3-152, 4-175
  layer 3/4 priorities 3-151, 4-175
  queue mapping 3-147, 4-172
  queue mode 3-149, 4-170
  traffic class weights 3-150, 4-172

D

default gateway, configuration 3-14, 4-221
default priority, ingress port 3-146, 4-171
default settings, system 1-5
DHCP 3-16, 4-217, 4-218, 4-219
  client 3-14
  dynamic configuration 2-5
Differentiated Code Point Service *See* DSCP
downloading software 3-18, 4-64
DSCP
  enabling 3-151, 4-175
  mapping priorities 3-152, 4-176
dynamic addresses, displaying 3-109, 4-137

E

edge port, STA 3-119, 3-122, 4-147
event logging 4-43

F

firmware
  displaying version 3-11, 4-62
  upgrading 3-18, 4-64

G

gateway, default 3-14, 4-221
GVRP
  global setting 4-165
  interface configuration 4-166

H

hardware version, displaying 3-11, 4-62
HTTPS 3-54, 4-30
HTTPS, secure server 3-54, 4-30

I

IEEE 802.1D 3-111, 4-140
IEEE 802.1w 3-111, 4-140
IEEE 802.1x 4-80
IGMP
  description of protocol 3-161
  groups, displaying 3-166, 4-181
  Layer 2 3-162, 4-178
  query 3-162, 4-182
  query, Layer 2 3-163, 4-182

snooping 3-162, 4-178
snooping, configuring 3-162, 4-178
ingress filtering 3-132, 4-156
IP address
BOOTP/DHCP 3-16, 4-217, 4-218, 4-219
setting 2-4, 3-14, 3-17, 4-217, 4-218, 4-219
IP precedence
enabling 3-151

J

jumbo frame 4-63

L

link type, STA 3-120, 3-121, 4-148
LLDP
configuration 3-140
display device information 3-143
port and trunk information 3-141
time information 3-140
logging
syslog traps 4-46
to syslog servers 4-45
log-in, Web interface 3-2
logon authentication 3-50, 4-70
RADIUS client 3-51, 4-72
RADIUS server 3-51, 4-72
TACACS+ client 3-51, 3-52, 4-76
TACACS+ server 3-51, 3-52, 4-76
logon authentication, sequence 3-52, 4-70, 4-71

M

main menu 3-3
Management Information Bases (MIBs) A-3
mirror port, configuring 3-97, 4-122
multicast filtering 3-161, 3-168, 3-183, 4-178
multicast groups 3-166, 4-181
displaying 4-181
static 3-166, 4-179, 4-181
multicast services
configuring 3-167, 3-169, 3-170, 3-172, 4-179
displaying 3-166, 4-181
multicast, static router port 3-165, 4-185

P

password, line 4-12
passwords 2-4
administrator setting 3-50, 4-25
path cost 3-113, 3-119
method 3-116, 4-144
STA 3-113, 3-119, 4-144
port authentication 4-80
port power
displaying status 3-106
inline 3-107
inline status 3-106
maximum allocation 3-106
priority 3-108
showing mainpower 3-106
port priority
configuring 3-145, 3-153, 4-169
default ingress 3-146, 4-171
STA 3-119, 4-146
port security, configuring 3-63, 4-78
port, statistics 3-99, 4-118
ports
autonegotiation 3-83, 4-113
broadcast storm threshold 3-96, 4-121
capabilities 3-83, 4-114
duplex mode 3-83, 4-112
flow control 3-83, 4-115
speed 3-83, 4-112
ports, configuring 3-81, 4-111
ports, mirroring 3-97, 4-122
power budgets
port 3-106
port priority 3-108
priority, default port ingress 3-146, 4-171
problems, troubleshooting B-1
protocol migration 3-122, 4-149

Q

queue weights 3-150, 4-172

R

RADIUS, logon authentication 3-51, 4-72
rate limits, setting 3-98, 4-124
remote logging 4-46
restarting the system 4-21
RSTP 3-111, 4-140
  global configuration 3-112, 4-140

S

secure shell 3-56, 4-33
Secure Shell configuration 3-56, 4-36, 4-37
serial port
  configuring 4-9
SNMP
  community string 3-36, 4-98
  enabling traps 3-37, 4-102
  trap manager 3-37, 4-102
  version 3 3-34, 3-39, 4-100, 4-103–4-110
software
  displaying version 3-11, 4-62
  downloading 3-18, 4-64
Spanning Tree Protocol *See* STA
specifications, software A-1
SSH, configuring 3-56, 4-36, 4-37
STA 3-111, 4-139
  edge port 3-119, 3-122, 4-147
  global settings, configuring 3-114, 4-139–4-144
  global settings, displaying 3-112, 4-150
  interface settings 3-118, ??–4-149, 4-150
  link type 3-120, 3-121, 4-148
  path cost 3-113, 3-119
  path cost method 3-116, 4-144
  port priority 3-119, 4-146
  protocol migration 3-122, 4-149
  transmission limit 3-116, 4-144
standards, IEEE A-2
startup files
  creating 3-21, 4-64
  displaying 3-18, 4-57
  setting 3-18, 4-69
static addresses, setting 3-108, 4-135
statistics
  port 3-99, 4-118
STP 3-115, 4-140
STP *Also see* STA
system clock, setting 3-32, 4-53
system software, downloading from server 3-18, 4-64

T

TACACS+, logon authentication 3-51, 3-52, 4-76
time, setting 3-32, 4-53
traffic class weights 3-150, 4-172
trap manager 2-7, 3-37, 4-102
troubleshooting B-1
trunk
  configuration 3-85, 4-125
  LACP 3-88, 4-127
  static 3-86, 4-126

U

upgrading software 3-18, 4-64
UPnP, configuration 3-187
user password 3-50, 4-25, 4-26

V

VLANs 3-123, 4-152–4-162
  adding static members 3-129, 3-131, 4-157
  creating 3-128, 4-153
  description 3-123
  displaying basic information 3-126, 4-166
  displaying port members 3-126, 4-159
  egress mode 3-132, 4-155
  interface configuration 3-132, 4-155–4-158
  private 3-133, 3-139, 4-160

W

Web interface
  access requirements 3-1
  configuration buttons 3-2
  home page 3-2

menu list 3-3
panel display 3-3

TECHNICAL SUPPORT

From U.S.A. and Canada (24 hours a day, 7 days a week)
Phn: 800-SMC-4-YOU / 949-679-8000
Fax: 949-502-3400

ENGLISH
Technical Support information available at www.smc.com

FRENCH
Informations Support Technique sur www.smc.com

DEUTSCH
Technischer Support und weitere Information unter www.smc.com

SPANISH
En www.smc.com Ud. podrá encontrar la información relativa a servicios de soporte técnico

DUTCH
Technische ondersteuningsinformatie beschikbaar op www.smc.com

PORTUGUES
Informações sobre Suporte Técnico em www.smc.com

SWEDISH
Information om Teknisk Support finns tillgängligt på www.smc.com

INTERNET
E-mail address: techsupport@smc.com

Driver updates
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web
http://www.smc.com/

SMC8124PL2