LevelOne

GEL-2870

24 GE + 4 GE Combo SFP
L2 SNMP Switch

Management Guide

version 1.0

MANAGEMENT GUIDE

GEL-2870

Layer 2 SNMP Switch
with 24 10/100/1000BASE-T (RJ-45) Ports,
and 4 Gigabit Combination Ports (RJ-45/SFP)

GEL-2870
E112009/AP-R01
149100000054A

About This Guide

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

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

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

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

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

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

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

The *Installation Guide*

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

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

November 2009 Revision
This is the first version of this guide. This guide is valid for software release v1.0.1.

CONTENTS

ABOUT THIS GUIDE 3
CONTENTS 5
FIGURES 17
TABLES 21

SECTION I GETTING STARTED 23

1 INTRODUCTION 24
Key Features 24
Description of Software Features 25
Configuration Backup and Restore 25
Authentication 25
Access Control Lists 26
Port Configuration 26
Rate Limiting 26
Port Mirroring 26
Port Trunking 26
Storm Control 26
Static Addresses 26
IEEE 802.1D Bridge 27
Store-and-Forward Switching 27
Spanning Tree Algorithm 27
Virtual LANs 28
Traffic Prioritization 28
Quality of Service 29
Multicast Filtering 29
System Defaults 30
2 INITIAL SWITCH CONFIGURATION 32
Connecting to the Switch 32
Configuration Options 32

Required Connections 33
Remote Connections 34
Basic Configuration 35
Setting Passwords 35
Setting an IP Address 35
Enabling SNMP Management Access 38
Managing System Files 42
Saving or Restoring Configuration Settings 42

SECTION II WEB CONFIGURATION 43

3 USING THE WEB INTERFACE 44
Connecting to the Web Interface 44
Navigating the Web Browser Interface 45
Home Page 45
Configuration Options 45
Panel Display 46
Main Menu 46
4 CONFIGURING THE SWITCH 50
Configuring System Information 50
Setting an IP Address 51
Setting an IPv4 Address 51
Setting an IPv6 Address 53
Setting the System Password 56
Filtering IP Addresses for Management Access 56
Configuring Port Connections 58
Configuring Authentication for Management Access and 802.1X 60
Creating Trunk Groups 64
Configuring Static Trunks 65
Configuring LACP 67
Configuring the Spanning Tree Algorithm 71
Configuring Global Settings for STA 72
Configuring Interface Settings for STA 73
Configuring 802.1X Port Authentication 76
Configuring HTTPS 81
Configuring SSH 83

IGMP Snooping 84
Configuring IGMP Snooping and Query 85
Configuring IGMP Filtering 88
Configuring Link Layer Discovery Protocol 89
Configuring the MAC Address Table 92
IEEE 802.1Q VLANs 94
Assigning Ports to VLANs 95
Configuring VLAN Attributes for Port Members 96
Configuring Private VLANs 98
Using Port Isolation 99
Quality of Service 100
Configuring Port-Level Queue Settings 101
Configuring DSCP Remarking 102
Configuring QoS Control Lists 104
Configuring Rate Limiting 107
Configuring Storm Control 109
Access Control Lists 110
Assigning ACL Policies and Responses 110
Configuring Rate Limiters 111
Configuring Access Control Lists 112
Configuring Port Mirroring 120
Simple Network Management Protocol 121
Configuring SNMP System and Trap Settings 123
Setting SNMPv3 Community Access Strings 126
Configuring SNMPv3 Users 127
Configuring SNMPv3 Groups 129
Configuring SNMPv3 Views 130
Configuring SNMPv3 Group Access Rights 131
Configuring UPnP 132
Configuring DHCP Relay and Option 82 Information 134
5 MONITORING THE SWITCH 136
Displaying Basic Information About the System 136
Displaying System Information 136
Displaying Log Messages 137
Displaying Log Details 139
Displaying Access Management Statistics 139

Displaying Information About Ports 140
Displaying Port Status On the Front Panel 140
Displaying an Overview of Port Statistics 140
Displaying QoS Statistics 141
Displaying Detailed Port Statistics 142
Displaying Information on Authentication Servers 145
Displaying a List of Authentication Servers 145
Displaying Statistics for Configured Authentication Servers 146
Displaying Information on LACP 150
Displaying an Overview of LACP Groups 150
Displaying LACP Port Status 150
Displaying LACP Port Statistics 151
Displaying Information on the Spanning Tree 152
Displaying Bridge Status for STA 152
Displaying Port Status for STA 154
Displaying Port Statistics for STA 155
Displaying Port Security Information 156
Displaying Port Security Status 156
Displaying Port Security Statistics 157
Showing IGMP Snooping Information 160
Displaying LLDP Information 161
Displaying LLDP Neighbor Information 162
Displaying LLDP Port Statistics 163
Displaying DHCP Relay Statistics 164
Displaying the MAC Address Table 166
6 PERFORMING BASIC DIAGNOSTICS 168
Pinging an IPv4 or IPv6 Address 168
Running Cable Diagnostics 169
7 PERFORMING SYSTEM MAINTENANCE 171
Resetting the Switch 171
Restoring Factory Defaults 171
Upgrading Firmware 172
Registering the Product 173
Managing Configuration Files 173
Saving Configuration Settings 173
Restoring Configuration Settings 174

SECTION III COMMAND LINE INTERFACE 175

8 USING THE COMMAND LINE INTERFACE 177
Accessing the CLI 177
Console Connection 177
Telnet Connection 178
Entering Commands 179
Keywords and Arguments 179
Minimum Abbreviation 180
Getting Help on Commands 180
Partial Keyword Lookup 181
Using Command History 182
Command Line Processing 182
CLI Command Groups 183

9 SYSTEM COMMANDS 185
system configuration 186
system reboot 186
system restore default 187
system contact 187
system name 187
system location 188
system password 188
system timezone 189
system log 189
system access configuration 190
system access mode 190
system access add 191
system access ipv6 add 192
system access delete 193
system access lookup 193
system access clear 193
system access statistics 193

10 IP COMMANDS 195
ip configuration 195
ip dhcp 196
ip setup 197

ip ping 198
ip dns 199
ip dns_proxy 199
ip sntp 200
ip ipv6 autoconfig 200
ip ipv6 setup 201
ip ipv6 ping6 202
ip ipv6 sntp 203
11 AUTHENTICATION COMMANDS 205
auth configuration 205
auth timeout 206
auth deadtime 207
auth radius 207
auth acct_radius 208
auth tacacs+ 210
auth client 211
auth statistics 212
12 PORT COMMANDS 215
port configuration 215
port state 217
port mode 217
port flow control 218
port maxframe 219
port power 219
port excessive 220
port statistics 221
port veriphy 222
port numbers 223
13 LINK AGGREGATION COMMANDS 224
aggr configuration 225
aggr add 226
aggr delete 226
aggr lookup 227
aggr mode 227
14 LACP COMMANDS 229
lacp configuration 231

lacp mode 231
lacp key 232
lacp role 232
lacp status 233
lacp statistics 233
15 RSTP COMMANDS 235
rstp configuration 236
rstp sysprio 236
rstp age 237
rstp delay 237
rstp txhold 238
rstp version 238
rstp mode 239
rstp cost 239
rstp priority 241
rstp edge 241
rstp autoedge 242
rstp p2p 243
rstp status 243
rstp statistics 244
rstp mcheck 244
16 IEEE 802.1X COMMANDS 246
dot1x configuration 246
dot1x mode 248
dot1x state 248
dot1x authenticate 249
dot1x reauthentication 250
dot1x period 251
dot1x timeout 251
dot1x clients 251
dot1x agetime 252
dot1x holdtime 253
dot1x statistics 253
17 IGMP COMMANDS 255
igmp configuration 255
igmp mode 257

igmp state 257
igmp querier 258
igmp fastleave 259
igmp leave proxy 260
igmp throttling 260
igmp filtering 261
igmp router 262
igmp flooding 262
igmp groups 263
igmp status 263
18 LLDP COMMANDS 264
lldp configuration 264
lldp mode 265
lldp optional_tlv 265
lldp interval 266
lldp hold 267
lldp delay 267
lldp reinit 268
lldp info 268
lldp statistics 269
lldp cdp_aware 270
19 MAC COMMANDS 271
mac configuration 271
mac add 272
mac delete 272
mac lookup 273
mac agetime 273
mac learning 273
mac dump 274
mac statistics 275
mac flush 275
20 VLAN COMMANDS 276
vlan configuration 276
vlan aware 277
vlan pvid 278
vlan frametype 278

vlan ingressfilter 279
vlan qinq 279
vlan add 280
vlan delete 280
vlan lookup 281
21 PVLAN COMMANDS 282
pvlan configuration 282
pvlan add 283
pvlan delete 283
pvlan lookup 284
pvlan isolate 284
22 QOS COMMANDS 285
qos configuration 286
qos default 286
qos tagprio 287
qos qcl port 287
qos qcl add 288
qos qcl delete 289
qos qcl lookup 290
qos mode 290
qos weight 291
qos rate limiter 291
qos shaper 292
qos storm unicast 293
qos storm multicast 293
qos storm broadcast 294
qos dscp remarking 294
qos dscp queue mapping 295
23 ACL COMMANDS 296
acl configuration 296
acl action 297
acl policy 298
acl rate 298
acl add 299
acl delete 302
acl lookup 302

acl clear 303
24 MIRROR COMMANDS 304
mirror configuration 304
mirror port 304
mirror mode 305
25 CONFIG COMMANDS 306
config save 306
config load 307
26 SNMP COMMANDS 308
snmp configuration 309
snmp mode 310
snmp version 311
snmp read community 311
snmp write community 312
snmp trap mode 312
snmp trap version 313
snmp trap community 313
snmp trap destination 314
snmp trap ipv6 destination 314
snmp trap authentication failure 314
snmp trap link-up 315
snmp trap inform mode 315
snmp trap inform timeout 316
snmp trap inform retry times 316
snmp trap probe security engine id 317
snmp trap security engine id 317
snmp trap security name 318
snmp engine id 318
snmp community add 319
snmp community delete 319
snmp community lookup 320
snmp user add 320
snmp user delete 321
snmp user changekey 322
snmp user lookup 322
snmp group add 323

snmp group delete 324
snmp group lookup 324
snmp view add 325
snmp view delete 325
snmp view lookup 326
snmp access add 326
snmp access delete 327
snmp access lookup 327

27 HTTPS COMMANDS 329

https configuration 329
https mode 329
https redirect 330

28 SSH COMMANDS 332

ssh configuration 332
ssh mode 332

29 UPNP COMMANDS 334

upnp configuration 334
upnp mode 334
upnp ttl 335
upnp advertising duration 336

30 DHCP COMMANDS 337

dhcp relay configuration 337
dhcp relay mode 337
dhcp relay server 338
dhcp relay information mode 338
dhcp relay information policy 339
dhcp relay statistics 339

31 FIRMWARE COMMANDS 341

firmware load 341
firmware ipv6 load 342

SECTION IV APPENDICES 344

A SOFTWARE SPECIFICATIONS 345

Software Features 345
Management Features 346

Standards 347
Management Information Bases 347
B TROUBLESHOOTING 349
Problems Accessing the Management Interface 349
Using System Logs 350
GLOSSARY 351
INDEX 358

FIGURES

Figure 1: Home Page 45
Figure 2: Front Panel Indicators 46
Figure 3: System Information Configuration 51
Figure 4: IP & Time Configuration 53
Figure 5: IPv6 & Time Configuration 55
Figure 6: System Password 56
Figure 7: Access Management Configuration 57
Figure 8: Port Configuration 59
Figure 9: Authentication Configuration 63
Figure 10: Static Trunk Configuration 67
Figure 11: LACP Port Configuration 70
Figure 12: RSTP System Configuration 73
Figure 13: RSTP Port Configuration 75
Figure 14: Port Security Configuration 81
Figure 15: HTTPS Configuration 82
Figure 16: SSH Configuration 84
Figure 17: IGMP Snooping Configuration 88
Figure 18: IGMP Snooping Port Group Filtering Configuration 89
Figure 19: LLDP Configuration 92
Figure 20: MAC Address Table Configuration 94
Figure 21: VLAN Membership Configuration 96
Figure 22: VLAN Port Configuration 98
Figure 23: Private VLAN Membership Configuration 99
Figure 24: Port Isolation Configuration 100
Figure 25: Port QoS Configuration 102
Figure 26: DSCP Remarking Configuration 104
Figure 27: QoS Control List Configuration 106
Figure 28: Rate Limit Configuration 108
Figure 29: Storm Control Configuration 110
Figure 30: ACL Port Configuration 111
Figure 31: ACL Rate Limiter Configuration 112

Figure 32: Access Control List Configuration 120
Figure 33: Mirror Configuration 121
Figure 34: SNMP System Configuration 126
Figure 35: SNMPv3 Communities Configuration 127
Figure 36: SNMPv3 Users Configuration 129
Figure 37: SNMPv3 Group Configuration 130
Figure 38: SNMPv3 View Configuration 131
Figure 39: SNMPv3 Access Configuration 132
Figure 40: UPnP Configuration 134
Figure 41: DHCP Relay Configuration 135
Figure 42: System Information 137
Figure 43: System Log Information 138
Figure 44: Detailed System Log Information 139
Figure 45: Access Management Statistics 140
Figure 46: Port State Overview 140
Figure 47: Port Statistics Overview 141
Figure 48: Queuing Counters 142
Figure 49: Detailed Port Statistics 144
Figure 50: RADIUS Overview 145
Figure 51: RADIUS Details 149
Figure 52: LACP System Status 150
Figure 53: LACP Port Status 151
Figure 54: LACP Port Statistics 152
Figure 55: Spanning Tree Bridge Status 154
Figure 56: Spanning Tree Port Status 155
Figure 57: Spanning Tree Port Statistics 156
Figure 58: Port Security Status 157
Figure 59: Port Security Statistics 160
Figure 60: IGMP Snooping Status 161
Figure 61: LLDP Neighbor Information 163
Figure 62: LLDP Port Statistics 164
Figure 63: DHCP Relay Statistics 166
Figure 64: MAC Address Table 167
Figure 65: ICMP Ping 169
Figure 66: VeriPHY Cable Diagnostics 170
Figure 67: Reset Device 171

Figure 68: Factory Defaults 172
Figure 69: Software Upload 172
Figure 70: Register Product 173
Figure 71: Configuration Save 174
Figure 72: Configuration Upload 174

TABLES

Table 1: Key Features 24
Table 2: System Defaults 30
Table 3: Web Page Configuration Buttons 45
Table 4: Main Menu 46
Table 5: Recommended STA Path Cost Range 74
Table 6: Recommended STA Path Costs 74
Table 7: Default STA Path Costs 74
Table 8: HTTPS System Support 82
Table 9: QCE Modification Buttons 105
Table 10: Mapping CoS Values to Egress Queues 105
Table 11: QCE Modification Buttons 114
Table 12: SNMP Security Models and Levels 122
Table 13: System Capabilities 162
Table 14: Keystroke Commands 182
Table 15: Command Group Index 183
Table 16: System Commands 185
Table 17: IP Commands 195
Table 18: Authentication Commands 205
Table 19: Port Commands 215
Table 20: Port Configuration 215
Table 21: Link Aggregation Commands 224
Table 22: LACP Commands 229
Table 23: RSTP Commands 235
Table 24: Recommended STA Path Cost Range 240
Table 25: Recommended STA Path Costs 240
Table 26: Default STA Path Costs 240
Table 27: IEEE 802.1X Commands 246
Table 28: 802.1X Configuration 247
Table 29: IGMP Commands 255
Table 30: IGMP Configuration 256
Table 31: LLDP Commands 264

Table 32: MAC Commands 271
Table 33: VLAN Commands 276
Table 34: PVLAN Commands 282
Table 35: QoS Commands 285
Table 36: Mapping CoS Values to Egress Queues 288
Table 37: ACL Commands 296
Table 38: Mirror Commands 304
Table 39: Configuration Commands 306
Table 40: SNMP Commands 308
Table 41: HTTPS Commands 329
Table 42: HTTPS System Support 330
Table 43: SSH Commands 332
Table 44: UPnP Commands 334
Table 45: DHCP Commands 337
Table 46: Firmware Commands 341
Table 47: Troubleshooting Chart 349

SECTION I

GETTING STARTED

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

This section includes these chapters:

- "Introduction" on page 24
- "Initial Switch Configuration" on page 32

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: Key Features

Feature	Description
Configuration Backup and Restore	Backup to management station or TFTP server
Authentication	Console, Telnet, web – user name/password, RADIUS, TACACS+ Web – HTTPS Telnet – SSH SNMP v1/2c - Community strings SNMP version 3 – MD5 or SHA password Port – IEEE 802.1X, MAC address filtering DHCP Snooping (with Option 82 relay information) IP Source Guard
Access Control Lists	Supports up to 128 rules
DHCP Client	Supported
DNS	Proxy service
Port Configuration	Speed, duplex mode, flow control, MTU, response to excessive collisions, power saving mode
Rate Limiting	Input rate limiting per port (using ACL)
Port Mirroring	One or more ports mirrored to single analysis port
Port Trunking	Supports up to 14 trunks using either static or dynamic trunking (LACP)
Storm Control	Throttling for broadcast, multicast, and unknown unicast storms
Address Table	Up to 8K MAC addresses in the forwarding table, 1024 static MAC addresses
IP Version 4 and 6	Supports IPv4 and IPv6 addressing, management, and QoS
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Algorithm	Supports Rapid Spanning Tree Protocol (RSTP), which includes STP backward compatible mode

Table 1: Key Features (Continued)

Feature	Description
Virtual LANs	Up to 256 using IEEE 802.1Q, port-based, and private VLANs
Traffic Prioritization	Queue mode and CoS configured by Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS bit, VLAN tag priority, or port
Qualify of Service	Supports Differentiated Services (DiffServ), and DSCP remarking
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. Storm suppression prevents broadcast, multicast, and unknown unicast traffic storms from engulfing the network. Untagged (port-based) and tagged VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering provides support for real-time network applications.

Some of the management features are briefly described below.

CONFIGURATION BACKUP AND RESTORE

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

AUTHENTICATION

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

ACCESS CONTROL LISTS ACLs provide packet filtering for IP frames (based on protocol, TCP/UDP port number or frame type) or layer 2 frames (based on any destination MAC address for unicast, broadcast or multicast, or based on VLAN ID or VLAN tag priority). 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. Policies can be used to differentiate service for client ports, server ports, network ports or guest ports. They can also be used to strictly control network traffic by only allowing incoming frames that match the source MAC and source IP on specific port.

PORT CONFIGURATION You can manually configure the speed and 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 (now incorporated in IEEE 802.3-2002).

RATE LIMITING This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

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

PORT TRUNKING Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using Link Aggregation Control Protocol (LACP – IEEE 802.3-2005). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 14 trunks.

STORM CONTROL Broadcast, multicast and unknown unicast storm suppression prevents 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 0.75 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

SPANNING TREE ALGORITHM

The switch supports these spanning tree protocols:

- Spanning Tree Protocol (STP, IEEE 802.1D) – Supported by using the STP backward compatible mode provided by RSTP. STP provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

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

VIRTUAL LANS

The switch supports up to 256 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

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

TRAFFIC PRIORITIZATION

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

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

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

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

SYSTEM DEFAULTS

The following table lists some of the basic system defaults.

Table 2: System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	115200 bps
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication	User Name	"admin"
	Password	"admin"
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Disabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Disabled
	HTTP Secure Server Redirect	Disabled
SNMP	SNMP Agent	Disabled
	Community Strings	"public" (read only) "private" (read/write)
	Traps	Global: disabled Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: default_view Group: default_rw_group
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Storm Protection	Status	Broadcast: disabled Multicast: disabled Unknown unicast: disabled

Table 2: System Defaults (Continued)

Function	Parameter	Default
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: RSTP standard)
	Edge Port	Enabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Tagged frames
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	Strict
	Weighted Round Robin	Queue: 0 1 2 3 Weight: 1 2 4 8
	Ethernet Type	Disabled
	VLAN ID	Disabled
	VLAN Priority Tag	Disabled
	ToS Priority	Disabled
	IP DSCP Priority	Disabled
	TCP/UDP Port Priority	Disabled
IP Settings	Management. VLAN	Any VLAN configured with an IP address
	IP Address	DHCP assigned, fallback is 192.168.1.1
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled
	DNS	Disabled
Multicast Filtering	IGMP Snooping	Snooping: Enabled Querier: Disabled
System Log (console only)	Status	Disabled
	Messages Logged to Flash	All levels
SNTP	Clock Synchronization	Disabled

2 INITIAL SWITCH CONFIGURATION

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

CONNECTING TO THE SWITCH

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

NOTE: An IPv4 address for this switch is obtained via DHCP by default. To change this address, see "Setting an IP Address" on page 35.

If the switch does not receive a response from a DHCP server, it will default to the IP address 192.168.1.1 and subnet mask 255.255.255.0.

CONFIGURATION OPTIONS

The switch's HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Internet Explorer 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above. The switch's web management interface can be accessed from any computer attached to the network.

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

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

- Set the administrator password
- 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 or output rates
- Control port access through IEEE 802.1X security or static address filtering
- Filter packets using Access Control Lists (ACLs)
- Configure up to 256 IEEE 802.1Q VLANs
- Configure IGMP multicast filtering
- Upload and download system firmware or configuration files via HTTP (using the web interface) or TFTP (using the command line interface)
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to 14 static or LACP trunks
- Enable port mirroring
- Set storm control on any port for excessive broadcast, multicast, or unknown unicast traffic
- Display system information and statistics

REQUIRED CONNECTIONS

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

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

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

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

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

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

For a description of how to use the CLI, see "Using the Command Line Interface" on page 177. For a list of all the CLI commands and detailed information on using the CLI, refer to "CLI Command Groups" on page 183.

REMOTE CONNECTIONS

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

An IPv4 address for this switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP, see "Setting an IP Address" on page 35.

If the switch does not receive a response from a DHCP server, it will default to the IP address 192.168.1.1 and subnet mask 255.255.255.0.

NOTE: This switch supports four Telnet sessions or four SSH sessions. Telnet and SSH cannot be used concurrently.

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, Netscape 6.2 or above, or Mozilla Firefox 2.0.0.0 or above), or from a network computer using SNMP network management software.

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

BASIC CONFIGURATION

SETTING PASSWORDS

If this is your first time to log into the console interface, you should define a new password for access to the web interface, record it, and put it in a safe place. The password can consist of up to 8 alphanumeric characters and is case sensitive. To prevent unauthorized access to the switch, set the password as follows:

Type "system password *password*," where *password* is your new password.

```
>system password ?
Description:
------------
Set or show the system password.

Syntax:
-------
System Password [<password>]

Parameters:
-----------
<password>: System password or 'clear' to clear
>system password admin
>
```

SETTING AN IP ADDRESS

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

- **Manual** — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.
- **Dynamic** — The switch can send an IPv4 configuration request to DHCP address allocation servers on the network, or can automatically generate a unique IPv6 host address based on the local subnet address prefix received in router advertisement messages.

MANUAL CONFIGURATION

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

NOTE: An IPv4 address for this switch is obtained via DHCP by default.

ASSIGNING AN IPV4 ADDRESS

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

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

To assign an IPv4 address to the switch, type

"ip setup *ip-address ip-mask ip-router vid*"

where "ip-address" is the switch's IP address, "ip-mask" is the mask for the network portion of the address, "ip-router" is the IP address of the default gateway, and "vid" is the VLAN identifier for the interface to which this address will be assigned. Press <Enter>.

```
>ip setup ?
Description:
------------
Set or show the IP setup.

Syntax:
-------
IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

Parameters:
-----------
<ip_addr>  : IP address (a.b.c.d), default: Show IP address
<ip_mask>  : IP subnet mask (a.b.c.d), default: Show IP mask
<ip_router>: IP router (a.b.c.d), default: Show IP router
<vid>      : VLAN ID (1-4095), default: Show VLAN ID
>ip setup 192.168.0.10 255.255.255.0 192.168.0.1 1
>
```

ASSIGNING AN IPV6 ADDRESS

This section describes how to configure a "global unicast" address by specifying the full IPv6 address (including network and host portions) and the length of the network prefix.

An IPv6 address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.

Before you can assign an IPv6 address to the switch that will be used to connect to a multi-segment network, you must obtain the following information from your network administrator:

- IP address for the switch
- Length of the network prefix
- Default gateway for the network

When configuring the IPv6 address and gateway, one double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields. To generate an IPv6 global unicast address for the switch, type the following command, and press <Enter>.

"ip ipv6 setup *ipv6-address ipv6-prefix ipv6-router vid*"

where "ipv6-address" is the full IPv6 address of the switch including the network prefix and host address bits. "ipv6-prefix" indicates the length of the network prefix, "ipv6-router" is the IPv6 address of the default next hop router to use when the management station is located on a different network segment, and "vid" is the VLAN identifier for the interface to which this address will be assigned.

```
>ip ipv6 setup ?
Description:
------------
Set or show the IPv6 setup.

Syntax:
-------
IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>] [<vid>]

>ip ipv6 setup 2001:DB8:2222:7272::72 64 2001:DB8:2222:7272::254 1
>ip ipv6 setup
IPv6 AUTOCONFIG mode  : Disabled
IPv6 Address      : 2001:db8:2222:7272::72
IPv6 Prefix       : 64
IPv6 Router       : 2001:db8:2222:7272::254
IPv6 VLAN ID      : 1
>
```

DYNAMIC CONFIGURATION

OBTAINING AN IPV4 ADDRESS

If you enable the "IP DHCP" option, IP will be enabled but will not function until a DHCP reply has been received. Requests will be sent periodically in an effort to obtain IP configuration information. DHCP values can include the IP address, subnet mask, and default gateway.

If the IP DHCP option is enabled, the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with DHCP address allocation servers on the network, type the following command, and press <Enter>. Wait a few minutes, and then check the IP configuration settings using the "ip dhcp" command.

"ip dhcp enable"

```
>ip dhcp enable
>ip dhcp
DHCP Client       : Enabled

Active Configuration:
IP Address        : 192.168.0.3
IP Mask           : 255.255.255.0
IP Router         : 0.0.0.0
DNS Server        : 0.0.0.0
SNTP Server       :
>
```

NOTE: Response time from DHCP servers vary considerably for different network environments. If you do not get a response in a reasonable amount of time, try entering the "dhcp disable" command followed by the "dhcp enable" command. Otherwise, set the static IP address to a null address (see page 35), and then enter the "dhcp enable" command or reboot the switch.

OBTAINING AN IPV6 ADDRESS

To generate an IPv6 address that can be used in a network containing more than one subnet, the switch can be configured to automatically generate a unique host address based on the local subnet address prefix received in router advertisement messages.

To dynamically generate an IPv6 host address for the switch, type the following command, and press <Enter>.

"ip ipv6 autoconfig enable"

```
>ip ipv6 autoconfig enable
>ip ipv6 autoconfig
IPv6 AUTOCONFIG mode  : Enabled
IPv6 Address      : 2001:db8:2222:7272::72
IPv6 Prefix       : 64
IPv6 Router       : 2001:db8:2222:7272::254
IPv6 VLAN ID      : 1
>
```

ENABLING SNMP MANAGEMENT ACCESS

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as HP OpenView. 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 "Configuring SNMPv3 Views" on page 130).

COMMUNITY STRINGS (FOR SNMP VERSION 1 AND 2C CLIENTS)

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

The default strings are:

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

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

To change the read-only or read/write community string, type either of the following commands, and press <Enter>.

"snmp read community *string*"
"snmp write community *string*"

where "string" is the community access string.

```
>snmp read community rd
>snmp read community
Read Community                : rd
>
```

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, enter the "snmp trap" commands shown below, and press <Enter>.

"snmp trap version *version"*
"snmp trap commuity *community-string"*
"snmp trap destination *host-address"*
"snmp trap mode enable"
"snmp mode enable"

where "version" indicates the SNMP client version (1, 2c, 3), "community-string" specifies access rights for a version 1/2c host, and "host-address" is the IP address for the trap receiver. For a more detailed description of these parameters and other SNMP commands, see "SNMP Commands" on page 308. The following example creates a trap host for a version 1 SNMP client.

```
>snmp trap version 1
>snmp trap community remote_user
>snmp trap destination 192.168.1.19
>snmp trap mode enable
>snmp mode enable
>snmp configuration
SNMP Mode                      : Enabled
SNMP Version                   : 1
Read Community                 : rd
Write Community                : private
Trap Mode                      : Enabled
Trap Version                   : 1
Trap Community                 : remote_user
Trap Destination               : 192.168.1.19
Trap IPv6 Destination          : ::
Trap Authentication Failure    : Enabled
Trap Link-up and Link-down     : Enabled
Trap Inform Mode               : Disabled
Trap Inform Timeout (seconds)  : 1
Trap Inform Retry Times        : 5
Trap Probe Security Engine ID  : Enabled
Trap Security Engine ID        :
Trap Security Name             : None
⋮
```

CONFIGURING ACCESS FOR SNMP VERSION 3 CLIENTS

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

```
>snmp user add 800007e5017f000001 steve md5 greenearth des blueseas
>snmp group add usm steve r&d
>snmp view add mib-2 included .1.3.6.1.2.1
>snmp view add 802.1d included .1.3.6.1.2.1.17
>snmp access add r&d usm noauthnopriv mib-2 802.1d
>snmp configuration
⋮
SNMPv3 Users Table:
Idx Engine ID User Name                         Level          Auth Priv
--- --------- --------------------------------- -------------- ---- ----
1   Local     default_user                      NoAuth, NoPriv None None
2   Local     steve                             Auth, Priv     MD5  DES
⋮
SNMPv3 Groups Table;
Idx Model Security Name                    Group Name
--- ----- ---------------------------------- --------------------------------
1   v1    public                           default_ro_group
2   v1    private                          default_rw_group
3   v2c   public                           default_ro_group
4   v2c   private                          default_rw_group
5   usm   default_user                     default_rw_group
6   usm   steve                            r&d
⋮
SNMPv3 Views Table:
Idx View Name                      View Type OID Subtree
--- ---------------------------------- --------- --------------------------------
1   default_view                     included  .1
2   mib-2                            included  .1.3.6.1.2.1
3   802.1d                           included  .1.3.6.1.2.1.17
⋮
```

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 121, or refer to the specific CLI commands for SNMP starting on page 308.

MANAGING SYSTEM FILES

The switch's flash memory supports two 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 or downloaded.

The types of files are:

- **Configuration** — This file type stores system configuration information. Configuration files can be saved to a TFTP server for backup, or uploaded from a TFTP server to restore previous settings using the CLI. Configuration files can also be saved to or restored from a management station using the web interface. See "Managing Configuration Files" on page 173 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. It can be uploaded from a TFTP server using the CLI or from a management station using the web interface. See "Upgrading Firmware" on page 172 for more information.

SAVING OR RESTORING CONFIGURATION SETTINGS

Configuration commands modify the running configuration, and are saved in nonvolatile storage. To save the current configuration settings to a backup server, enter the following command, and press <Enter>.

"config save *tftp-server file-name"*

where "tftp-server" is the ip address of the backup server, and "file-name" is the name under which the configuration settings are saved.

```
>config save 192.168.1.19 GEL-2870.cfg
>
```

To restore configuration settings from a backup server, enter the following command, and press <Enter>.

"config load *tftp-server file-name"*

```
>config load 192.168.1.19 GEL-2870.cfg
>
```

SECTION II

WEB CONFIGURATION

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

This section includes these chapters:

- "Using the Web Interface" on page 44
- "Configuring the Switch" on page 50
- "Monitoring the Switch" on page 136
- "Performing Basic Diagnostics" on page 168
- "Performing System Maintenance" on page 171

3 USING THE WEB INTERFACE

This switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0, Netscape 6.2, Mozilla Firefox 2.0.0.0, or more recent versions).

NOTE: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to "Using the Command Line Interface" on page 177.

CONNECTING TO THE WEB INTERFACE

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

1. Configured the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, or DHCP protocol. (See "Setting an IP Address" on page 35.)

2. Set the system password using an out-of-band serial connection. (See "Setting Passwords" on page 35.)

3. After you enter a user name and password, you will have access to the system configuration program.

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

NOTE: If 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 AdminEdge) to improve the switch's response time to management commands issued through the web interface. See "Configuring Interface Settings for STA" on page 73.

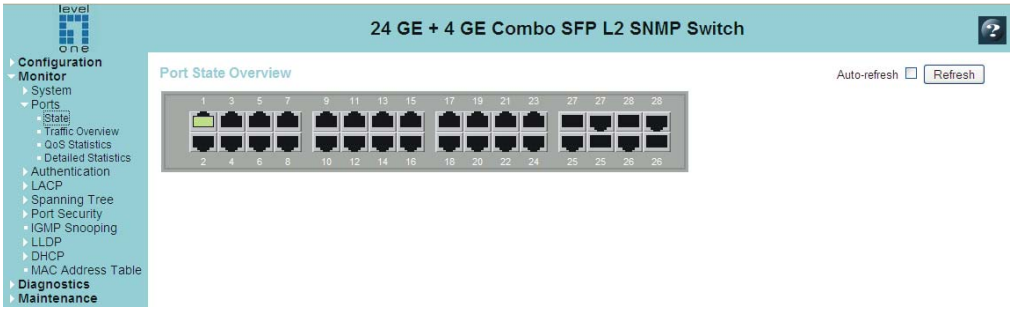
NAVIGATING THE WEB BROWSER INTERFACE

To access the web-browser interface you must first enter a user name and password. By default, the user name is "admin" with password "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 an image of the front panel on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.

Figure 1: Home Page



CONFIGURATION OPTIONS

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

Table 3: Web Page Configuration Buttons

Button	Action
Save	Sets specified values to the system.
Reset	Cancels specified values and restores current values prior to pressing "Save."
	Links directly to Online Help.

NOTE: To ensure proper screen refresh, be sure that Internet Explorer is configured so that the setting "Check for newer versions of stored pages" reads "Every visit to the page."

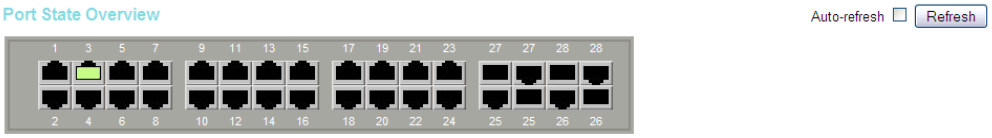
Internet Explorer 6.x and earlier: This option is available under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings."

Internet Explorer 7.x: This option is available under "Tools / Internet Options / General / Browsing History / Settings / Temporary Internet Files."

PANEL DISPLAY

The web agent displays an image of the switch's ports. The refresh mode is disabled by default. Tick Auto-refresh to refresh the data displayed on the screen approximately once every 5 seconds, or press the Refresh button to refresh the screen right away. Clicking on the image of a port opens the Detailed Statistics page as described on page 142.

Figure 2: Front Panel Indicators



MAIN MENU

By using the web agent, it is easily to manage and control the switch or to monitor the network conditions. The following table briefly describes the selections available from this program.

Table 4: Main Menu

Menu	Description	Page
Configuration		50
System		
Information	Configures system contact, name and location	50
IP & Time	Configures IPv4 and SNTP settings	51
IPv6 & Time	Configures IPv6 and SNTP settings	53
Password	Configures system password	56
Access Management	Sets IP addresses of clients allowed management access via HTTP/HTTPS, SNMP, and Telnet/SSH	56
Ports	Configures port connection settings	58
Authentication	Configures authentication method for management access via local database, RADIUS or TACACS+	60
Aggregation		64
Static	Specifies ports to group into static trunks	65
LACP	Allows ports to dynamically join trunks	67
Spanning Tree		71
System	Configures global bridge settings for RSTP	72
Ports	Configures individual port settings for RSTP	73
Port Security	Configures global and port settings for IEEE 802.1X	76
HTTPS	Configures secure HTTP settings	81
SSH	Configures Secure Shell server	83
IGMP Snooping		84
Basic Configuration	Configures global and port settings for multicast filtering	85

Table 4: Main Menu

Menu	Description	Page
Port Group Filtering	Configures multicast groups to be filtered on specified port	88
LLDP	Configures global LLDP timing parameters, and port-specific TLV attributes	89
MAC Address Table	Configures address aging, dynamic learning, and static addresses	92
VLANs		94
VLAN Membership	Configures VLAN groups	95
Ports	Specifies default PVID and VLAN attributes	96
Private VLANs		
PVLAN Membership	Configures PVLAN groups	98
Port Isolation	Prevents communications between designated ports within the same private VLAN	99
QoS		100
Ports	Configures default traffic class, user priority, queue mode, and queue weights	101
DSCP Remarking	Remarks DSCP values to standard CoS classes, best effort, or expedited forwarding	102
QoS Control List	Configures QoS policies for handling ingress packets based on Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS, or VLAN priority tag	104
Rate Limiters	Configures ingress and egress rate limits	107
Storm Control	Sets limits for broadcast, multicast, and unknown unicast traffic	109
ACL		110
Ports	Assigns ACL, rate limiter, and other parameters to ports	110
Rate Limiters	Configures rate limit policies	111
Access Control List	Configures ACLs based on frame type, destination MAC type, VLAN ID, VLAN priority tag; and the action to take for matching packets	112
Mirroring	Sets source and target ports for mirroring	120
SNMP		121
System	Configures read-only and read/write community strings for SNMP v1/v2c, engine ID for SNMP v3, and trap parameters	123
Communities	Configures community strings	126
Users	Configures SNMP v3 users on this switch	127
Groups	Configures SNMP v3 groups	129
Views	Configures SNMP v3 views	130
Access	Assigns security model, security level, and read/write views to SNMP groups	131
UPnP	Enables UPNP and defines timeout values	132
DHCP		

Table 4: Main Menu

Menu	Description	Page
Relay	Configures DHCO relay information status and policy	134
Monitor		136
System		136
Information	Displays basic system description, switch's MAC address, system time, and software version	136
Log	Limits the system messages logged based on severity; displays logged messages	137
Detailed Log	Displays detailed information on each logged message	139
Access Management Statistics	Displays the number of packets used to manage the switch via HTTP, HTTPS, SNMP, Telnet, and SSH	139
Ports		140
State	Displays a graphic image of the front panel indicating active port connections	140
Traffic Overview	Shows basic Ethernet port statistics	140
QoS Statistics	Shows the number of packets entering and leaving the egress queues	141
Detailed Statistics	Shows detailed Ethernet port statistics	142
Authentication		145
RADIUS Overview	Displays status of configured RADIUS authentication and accounting servers	145
RADIUS Details	Displays the traffic and status associated with each configured RADIUS server	146
LACP		150
System Status	Displays administration key and associated local ports for each partner	150
Port Status	Displays administration key, LAG ID, partner ID, and partner ports for each local port	150
Port Statistics	Displays statistics for LACP protocol messages	151
Spanning Tree		152
Bridge Status	Displays global bridge and port settings for STA	152
Port Status	Displays STA role, state, and uptime for each port	154
Port Statistics	Displays statistics for RSTP, STP and TCN protocol packets	155
Port Security		156
Status	Displays 802.1X security state of each port, last source address used for authentication, and last ID	156
Statistics	Displays 802.1X protocol statistics for the selected port	157
IGMP Snooping	Displays statistics related to IGMP packets passed upstream to the IGMP Querier or downstream to multicast clients	160
LLDP		161
Neighbors	Displays LLDP information about a remote device connected to a port on this switch	162

Table 4: Main Menu

Menu	Description	Page
Port Statistics	Displays statistics for all connected remote devices, and statistics for LLDP protocol packets crossing each port	163
DHCP		
Relay Statistics	Displays server and client statistics for packets affected by the relay information policy	164
MAC Address Table	Displays dynamic and static address entries associated with the CPU and each port	166
Diagnostics		168
Ping	Tests specified path using IPv4 ping	168
Ping6	Tests specified path using IPv6 ping	168
VeriPHY	Performs cable diagnostics for all ports or selected port to diagnose any cable faults (short, open etc.) and report the cable length	169
Maintenance		171
Reset Device	Restarts the switch	171
Factory Defaults	Restores factory default settings	171
Software Upload	Updates software on the switch with a file specified on the management station	172
Register Product	Opens product registration page	173
Configuration		173
Save	Saves configuration settings to a file on the management station	173
Upload	Restores configuration settings from a file on the management station	173

4 CONFIGURING THE SWITCH

This chapter describes all of the basic configuration tasks.

CONFIGURING SYSTEM INFORMATION

You can identify the system by configuring the contact information, name, and location of the switch.

PARAMETERS

These parameters are displayed on the System Information page:

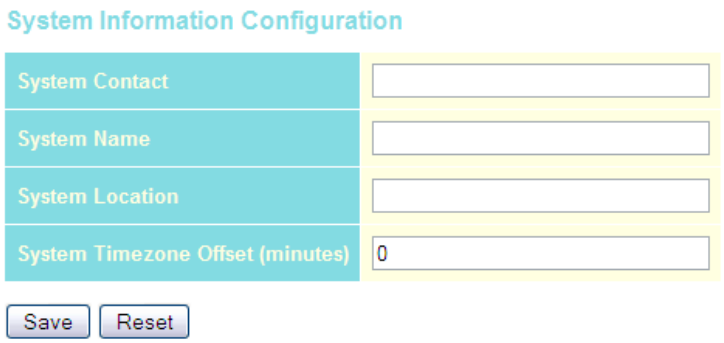
- **System Contact** – Administrator responsible for the system. (Maximum length: 255 characters)
- **System Name** – Name assigned to the switch system. (Maximum length: 255 characters)
- **System Location** – Specifies the system location. (Maximum length: 255 characters)
- **System Timezone Offset** (minutes) – Sets the time zone as an offset from Greenwich Mean Time (GMT). Negative values indicate a zone before (east of) GMT, and positive values indicate a zone after (west of) GMT.

WEB INTERFACE

To configure System Information in the web interface:

1. Click Configuration, System, Information.
2. Specify the contact information for the system administrator, as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.
3. Click Save.

Figure 3: System Information Configuration



SETTING AN IP ADDRESS

This section describes how to configure an IP interface for management access to the switch over the network. This switch supports both IP Version 4 and Version 6, and can be managed simultaneously through either of these address types. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a DHCP server when it is powered on. An IPv6 address can either be manually configured or dynamically generated.

SETTING AN IPV4 ADDRESS

The IPv4 address for the switch is obtained via DHCP by default for VLAN 1. To manually configure an address, you need to change the switch's default settings 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.

NOTE: An IPv4 address for this switch is obtained via DHCP by default. If the switch does not receive a response from a DHCP server, it will default to the IP address 192.168.1.1 and subnet mask 255.255.255.0.

You can manually configure a specific IP address, or direct the device to obtain an address from a DHCP server. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted by the CLI program.

PARAMETERS

The following parameters are displayed on the IP & Time page:

IP Configuration

- **DHCP Client** – Specifies whether IP functionality is enabled via Dynamic Host Configuration Protocol (DHCP). If DHCP 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 values can include the IP address, subnet mask, and default gateway. (Default: Enabled)

- **IP Address** – Address of the VLAN specified in the VLAN ID field. This should be the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 192.168.1.1)

- **IP Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)

- **IP Router** – IP address of the gateway router between the switch and management stations that exist on other network segments.

- **VLAN ID** – ID of the configured VLAN. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4095; Default: 1)

- **SNTP Server** – Sets the IPv4 address for a time server (NTP or SNTP). The switch attempts to periodically update the time from the specified server. The polling interval is fixed at 15 minutes.

- **DNS Server** – A Domain Name Server to which client requests for mapping host names to IP addresses are forwarded.

IP DNS Proxy Configuration

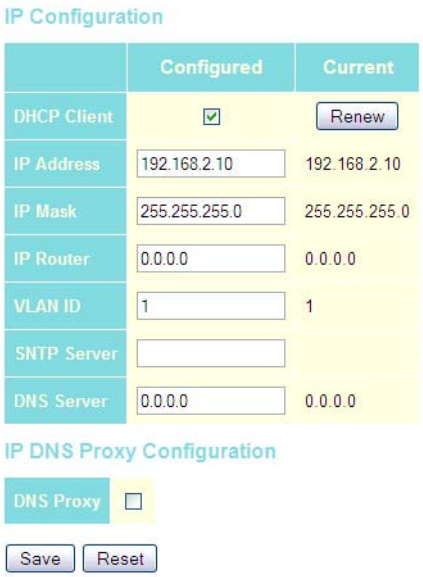
- **IP DNS Proxy** – If enabled, the switch maintains a local database based on previous responses to DNS queries forwarded on behalf of attached clients. If the required information is not in the local database, the switch forwards the DNS query to a DNS server, stores the response in its local cache for future reference, and passes the response back to the client.

WEB INTERFACE

To configure an IP address and SNTP in the web interface:

1. Click Configuration, System, IP & Time.
2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click Save.

Figure 4: IP & Time Configuration



SETTING AN IPV6 ADDRESS

This section describes how to configure an IPv6 interface for management access over the network. This switch supports both IPv4 and IPv6, and can be managed through either of these address types. For information on configuring the switch with an IPv4 address, see "Setting an IP Address" on page 51.

IPv6 includes two distinct address types - link-local unicast and global unicast. A link-local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. Management traffic using this kind of address cannot be passed by any router outside of the subnet. A link-local address is easy to set up, and may be useful for simple networks or basic troubleshooting tasks. However, to connect to a larger network with multiple segments, the switch must be configured with a global unicast address. A link-local address must be manually configured, but a global unicast address can either be manually configured or dynamically assigned.

USAGE GUIDELINES

- All IPv6 addresses must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal

values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- When configuring a link-local address, note that the prefix length is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier (i.e., the physical MAC address). You can manually configure a link-local address by entering the full address with the network prefix FE80.

- To connect to a larger network with multiple subnets, you must configure a global unicast address. There are several alternatives to configuring this address type:

  - The global unicast address can be automatically configured by taking the network prefix from router advertisements observed on the local interface, and using the modified EUI-64 form of the interface identifier to automatically create the host portion of the address. This option can be selected by enabling the Auto Configuration option.

  - You can also manually configure the global unicast address by entering the full address and prefix length.

PARAMETERS

The following parameters are displayed on the IPv6 & Time page:

IPv6 Configuration

- **Auto Configuration** – Enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 functionality on the interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the interface identifier; i.e., the switch's MAC address. (Default: Disabled)

- **Address** – Manually configures a global unicast address by specifying the full address and network prefix length (in the Prefix field). (Default: ::192.168.1.1)

- **Prefix** – Defines the prefix length as a decimal value indicating how many contiguous bits (starting at the left) of the address comprise the prefix; i.e., the network portion of the address. (Default: 96 bits)

  Note that the default prefix length of 96 bits specifies that the first six colon-separated values comprise the network portion of the address.

- **Router** – Sets the IPv6 address of the default next hop router.

  An IPv6 default gateway must be defined if the management station is located in a different IPv6 segment.

An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

- **VLAN ID** – ID of the configured VLAN. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4095; Default: 1)

- **SNTP Server** – Sets the IPv6 address for a time server (NTP or SNTP). The switch attempts to periodically update the time from the specified server. The polling interval is fixed at 15 minutes.

WEB INTERFACE

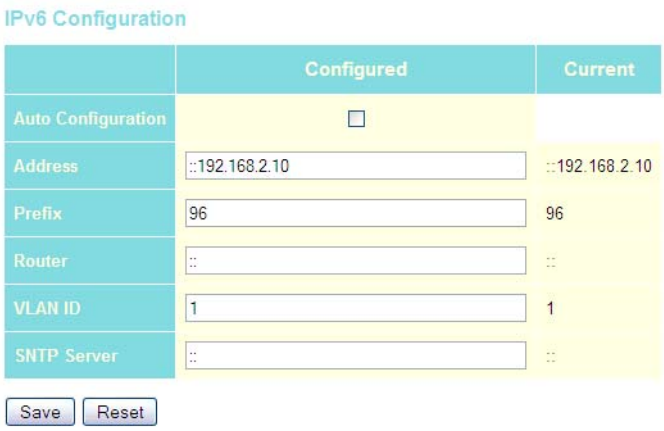
To configure an IPv6 address and SNTP in the web interface:

1. Click Configuration, System, IPv6 & Time.

2. Specify the IPv6 settings. The information shown below provides a example of how to manually configure an IPv6 address.

3. Click Save.

Figure 5: IPv6 & Time Configuration



SETTING THE SYSTEM PASSWORD

The administrator has read/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.

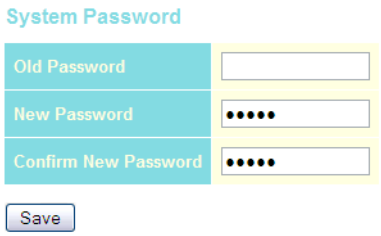
The administrator name is "admin" with password "admin" by default. The input range for the password is 0-8 plain text characters, and is case sensitive.

WEB INTERFACE

To configure the System Password in the web interface:

1. Click Configuration, System, Password.
2. Enter the old password.
3. Enter the new password.
4. Enter the new password again to confirm your input.
5. Click Save.

Figure 6: System Password



FILTERING IP ADDRESSES FOR MANAGEMENT ACCESS

You can create a list of up to 16 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.

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.

PARAMETERS

The following parameters are displayed on the Access Management page:

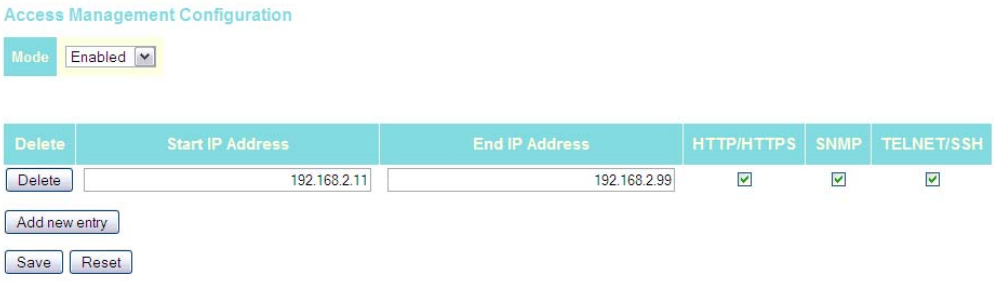
- **Mode** – Enables or disables filtering of management access based on configured IP addresses. (Default: Disabled)
- **Start IP Address** – The starting address of a range.
- **End IP Address** – The ending address of a range.
- **HTTP/HTTPS** – Filters IP addresses for access to the web interface over standard HTTP, or over HTTPS which uses the Secure Socket Layer (SSL) protocol to provide an encrypted connection.
- **SNMP** – Filters IP addresses for access through SNMP.
- **TELNET/SSH** – Filters IP addresses for access through Telnet, or through Secure Shell which provides authentication and encryption.

WEB INTERFACE

To configure Access Management controls in the web interface:

1. Click Configuration, System, Access Management.
2. Set the Mode to Enabled.
3. Enter the start and end of an address range.
4. Mark the protocols to restrict based on the specified address range.The information shown below provides a example of how to restrict management access for all protocols to a specific address range.
5. Click Save.

Figure 7: Access Management Configuration



CONFIGURING PORT CONNECTIONS

The Port Configuration page includes configuration options for enabling auto-negotiation or manually setting the speed and duplex mode, enabling flow control, setting the maximum frame size, specifying the response to excessive collisions, or enabling power saving mode.

PARAMETERS

The following parameters are displayed on the Port Configuration page:

- **Link** – Indicates if the link is up or down.
- **Speed** – Sets the port speed and duplex mode using auto-negotiation or manual selection. The following options are supported:
  - **Disable** - Disables the interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons.
  - **Auto** - Enables auto-negotiation. When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities.
  - **1G FDX** - Supports 1 Gbps full-duplex operation
  - **100Mbps FDX** - Supports 100 Mbps full-duplex operation
  - **100Mbps HDX** - Supports 100 Mbps half-duplex operation
  - **10Mbps FDX** - Supports 10 Mbps full-duplex operation
  - **10Mbps HDX** - Supports 10 Mbps half-duplex operation

  (Default: Autonegotiation enabled; Advertised capabilities for RJ-45: 1000BASE-T - 10half, 10full, 100half, 100full, 1000full; SFP: 1000BASE-SX/LX/LH - 1000full)

NOTE: The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.

- **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 802.3-2005 (formally IEEE 802.3x) for full-duplex operation. (Default: Disabled)

  When auto-negotiation is used, this parameter indicates the flow control capability advertised to the link partner. When the speed and duplex mode are manually set, the Current Rx field indicates whether pause frames are obeyed by this port, and the Current Tx field indicates if pause frames are transmitted from this 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.

- **Maximum Frame** – Sets the maximum transfer unit for traffic crossing the switch. Packets exceeding the maximum frame size are dropped. (Range: 9600-1518 bytes; Default: 9600 bytes)

- **Excessive Collision Mode** – Sets the response to take when excessive transmit collisions are detected on a port.
  - **Discard** - Discards a frame after 16 collisions (default).
  - **Restart** - Restarts the backoff algorithm after 16 collisions.

- **Power Control** – Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements.

  IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can significantly reduce power used for cable lengths of 20 meters or less, and continue to ensure signal integrity.

  The following options are supported:
  - **Disabled** – All power savings mechanisms disabled (default).
  - **Enabled** – Both link up and link down power savings enabled.
  - **ActiPHY** – Link down power savings enabled.
  - **PerfectReach** – Link up power savings enabled.

WEB INTERFACE

To configure port connection settings in the web interface:

1. Click Configuration, Ports.
2. Make any required changes to the connection settings.
3. Click Save.

Figure 8: Port Configuration

Port Configuration

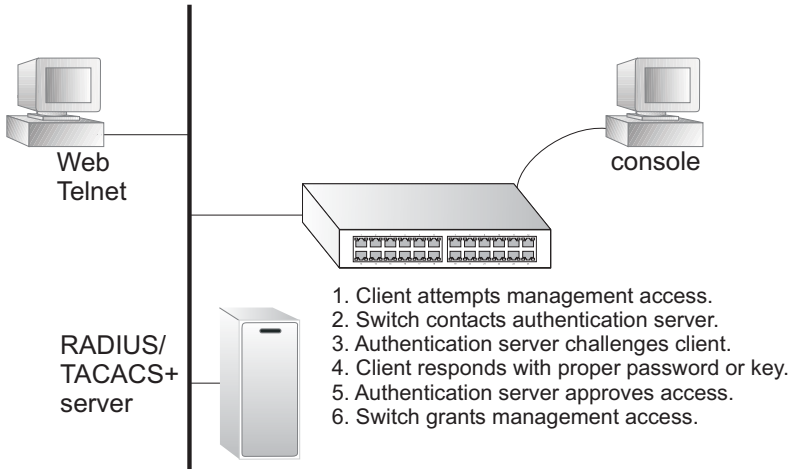
Refresh

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
1		Down	Auto	✕	✕	☐	9600	Discard	Disabled
2		Down	Auto	✕	✕	☐	9600	Discard	Disabled
3		100fdx	Auto	✕	✕	☐	9600	Discard	Disabled
4		Down	Auto	✕	✕	☐	9600	Discard	Disabled
5		Down	Auto	✕	✕	☐	9600	Discard	Disabled

CONFIGURING AUTHENTICATION FOR MANAGEMENT ACCESS AND 802.1X

Use the Authentication Configuration page to specify the authentication method for controlling management access through Telnet, SSH or HTTP/HTTPS. Access can be based on the (local) user name and password configured on the switch, or can be controlled with a RADIUS or TACACS+ remote access authentication server. Note that the RADIUS servers used to authenticate client access for IEEE 802.1X port authentication are also configured on this page (see page 76).

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.



USAGE GUIDELINES

- The switch supports the following authentication services:
  - Authorization of users that access the Telnet, SSH, the web, or console management interfaces on the switch.
  - Accounting for users that access the Telnet, SSH, the web, or console management interfaces on the switch.
  - Accounting for IEEE 802.1X authenticated users that access the network through the switch. This accounting can be used to provide reports, auditing, and billing for services that users have accessed.
- 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 method and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via Telnet, SSH, a web browser, or the console interface.

- When using RADIUS or TACACS+ logon authentication, the user name and password must be configured on the authentication server. The encryption methods used for the authentication process must also be configured or negotiated between the authentication server and logon client. This switch can pass authentication messages between the server and client that have been encrypted using MD5 (Message-Digest 5), TLS (Transport Layer Security), or TTLS (Tunneled Transport Layer Security).

NOTE: This guide assumes that RADIUS and TACACS+ servers have already been configured to support AAA. The configuration of RADIUS and TACACS+ server software is beyond the scope of this guide. Refer to the documentation provided with the RADIUS and TACACS+ server software.

PARAMETERS

The following parameters are displayed on the Authentication Configuration page:

Client Configuration

- **Client** – Specifies how the administrator is authenticated when logging into the switch via Telnet, SSH, a web browser, or the console interface.

- **Authentication Method** – Selects the authentication method. (Options: None, Local, RADIUS, TACACS+; Default: Local)

  Selecting the option "None" disables access through the specified management interface.

- **Fallback** – Uses the local user database for authentication if none of the configured authentication servers are alive. This is only possible if the Authentication Method is set to something else than "none" or "local."

Common Server Configuration

- **Timeout** – The time the switch waits for a reply from an authentication server before it resends the request. (Range: 3-3600 seconds; Default: 15 seconds)

- **Dead Time** – The time after which the switch considers an authentication server to be dead if it does not reply. (Range: 0-3600 seconds; Default: 300 seconds)

  Setting the Dead Time to a value greater than 0 (zero) will cause the authentication server to be ignored until the Dead Time has expired. However, if only one server is enabled, it will never be considered dead.

RADIUS/TACACS+ Server Configuration

- **Enabled** – Enables the server specified in this entry.

- **IP Address** – IP address or IP alias of authentication server.

- **Port** – Network (UDP) port of authentication server used for authentication messages. (Range: 1-65535; Default: 0)

  If the UDP port is set to 0 (zero), the switch will use 1812 for RADIUS authentication servers, 1813 for RADIUS accounting servers, or 49 for TACACS+ authentication servers.

- **Secret** – Encryption key used to authenticate logon access for the client. (Maximum length: 29 characters)

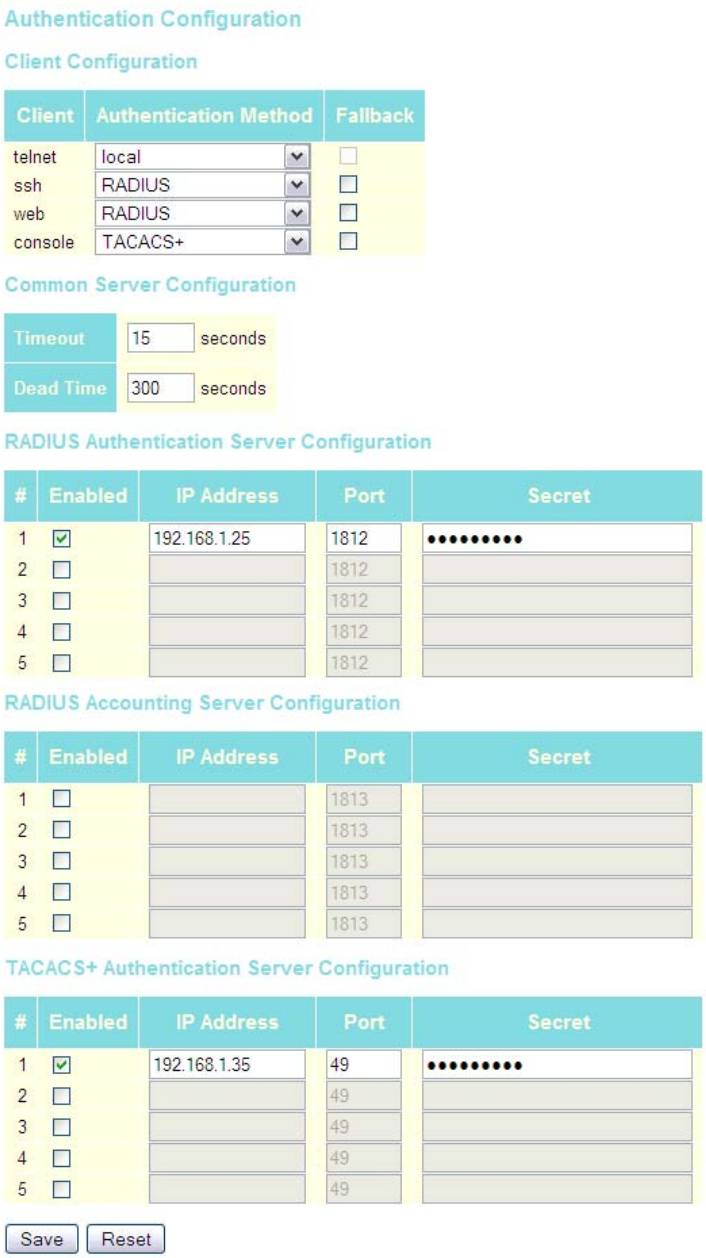
  To set an empty secret, use two quotes (“”). To use spaces in the secret, enquote the secret. Quotes in the secret are not allowed.

WEB INTERFACE

To configure authentication for management access in the web interface:

1. Click Configuration, Authentication.
2. Configure the authentication method for management client types, the common server timing parameters, and address, UDP port, and secret key for each required RADIUS or TACACS+ server.
3. Click Save.

Figure 9: Authentication Configuration



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 switches.

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 to use LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured to use LACP, the switch and the other device will negotiate a trunk between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

USAGE GUIDELINES

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, configure 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 14 trunks on a switch, with up to 16 ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

CONFIGURING STATIC TRUNKS

Use the Static Aggregation page to configure the aggregation mode and members of each static trunk group.

USAGE GUIDELINES

- 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.

- When incoming data frames are forwarded through the switch to a trunk, the switch must determine to which port link in the trunk an outgoing frame should be sent. To maintain the frame sequence of various traffic flows between devices in the network, the switch also needs to ensure that frames in each "conversation" are mapped to the same trunk link. To achieve this requirement and to distribute a balanced load across all links in a trunk, the switch uses a hash algorithm to calculate an output link number in the trunk. However, depending on the device to which a trunk is connected and the traffic flows in the network, this load-balance algorithm may result in traffic being distributed mostly on one port in a trunk. To ensure that the switch traffic load is distributed evenly across all links in a trunk, the hash method used in the load-balance calculation can be selected to provide the best result for trunk connections. The switch provides four load-balancing modes as described in the following section.

- Aggregation Mode Configuration also applies to LACP (see "Configuring LACP" on page 67).

PARAMETERS

The following parameters are displayed on the configuration page for static trunks:

Aggregation Mode Configuration

- **Hash Code Contributors** – Selects the load-balance method to apply to all trunks on the switch. If more than one option is selected, each factor is used in the hash algorithm to determine the port member within the trunk to which a frame will be assigned. The following options are supported:

  - **Source MAC Address** – All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts. (One of the defaults.)

  - **Destination MAC Address** – All traffic with the same destination MAC address is output on the same link in a trunk. This mode works

best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.

- **IP Address** – All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic. (One of the defaults.)

- **TCP/UDP Port Number** – All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk. Avoid using his mode as a lone option. It may overload a single port member of the trunk for application traffic of a specific type, such as web browsing. However, it can be used effectively in combination with the IP Address option. (One of the defaults.)

Aggregation Group Configuration

- **Group ID** – Trunk identifier. (Range: 1-14)

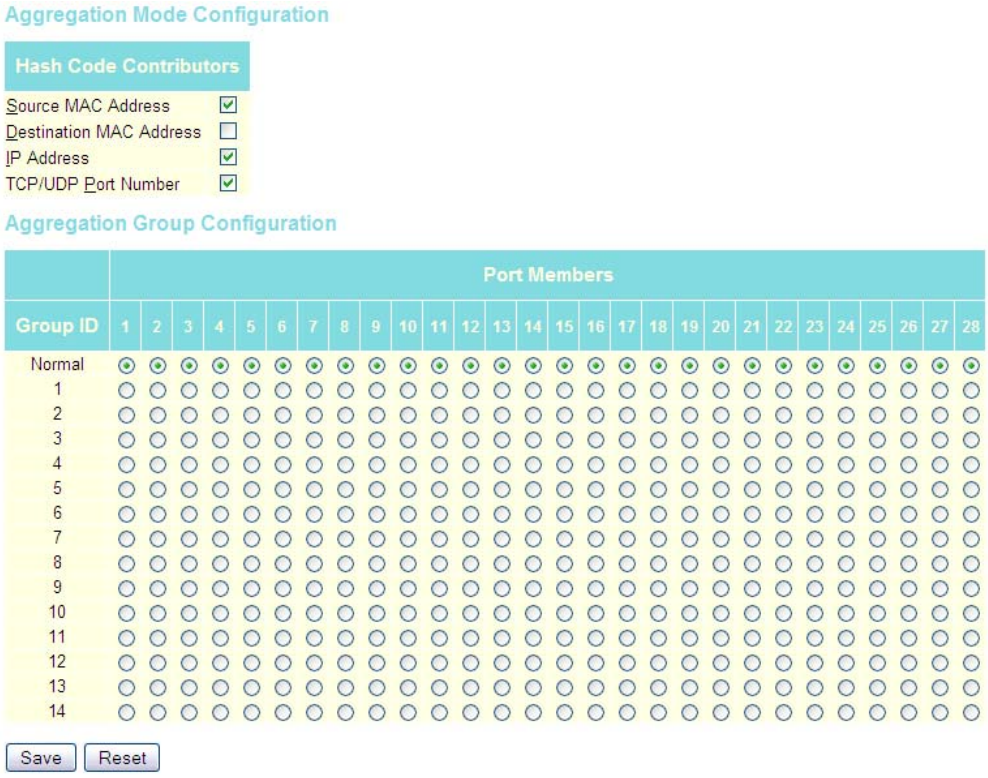
- **Port Members** – Port identifier. (Range: 1-28)

WEB INTERFACE

To configure a static trunk:

1. Click Configuration, Aggregation, Static.
2. Select one or more load-balancing methods to apply to the configured trunks.
3. Assign port members to each trunk that will be used.
4. Click Save.

Figure 10: Static Trunk Configuration



CONFIGURING LACP

Use the LACP Port Configuration page to enable LACP on selected ports, configure the administrative key, and the protocol initiation mode.

USAGE GUIDELINES

- 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, either by forced mode or auto-negotiation.
- Trunks dynamically established through LACP will be shown on the LACP System Status page (page 150) and LACP Port Status (page 150) pages under the Monitor menu.
- Ports assigned to a common link aggregation group (LAG) must meet the following criteria:
  - Ports must have the same LACP Admin Key. Using auto-configuration of the Admin Key will avoid this problem.
  - One of the ports at either the near end or far end must be set to active initiation mode.
- Aggregation Mode Configuration located under the Static Aggregation menu (see "Configuring Static Trunks" on page 65) also applies to LACP.

PARAMETERS

The following parameters are displayed on the configuration page for dynamic trunks:

- **Port** – Port identifier. (Range: 1-28)
- **LACP Enabled** – Controls whether LACP is enabled on this switch port. LACP will form an aggregation when two or more ports are connected to the same partner. LACP can form up to 12 LAGs per switch.
- **Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: Auto)

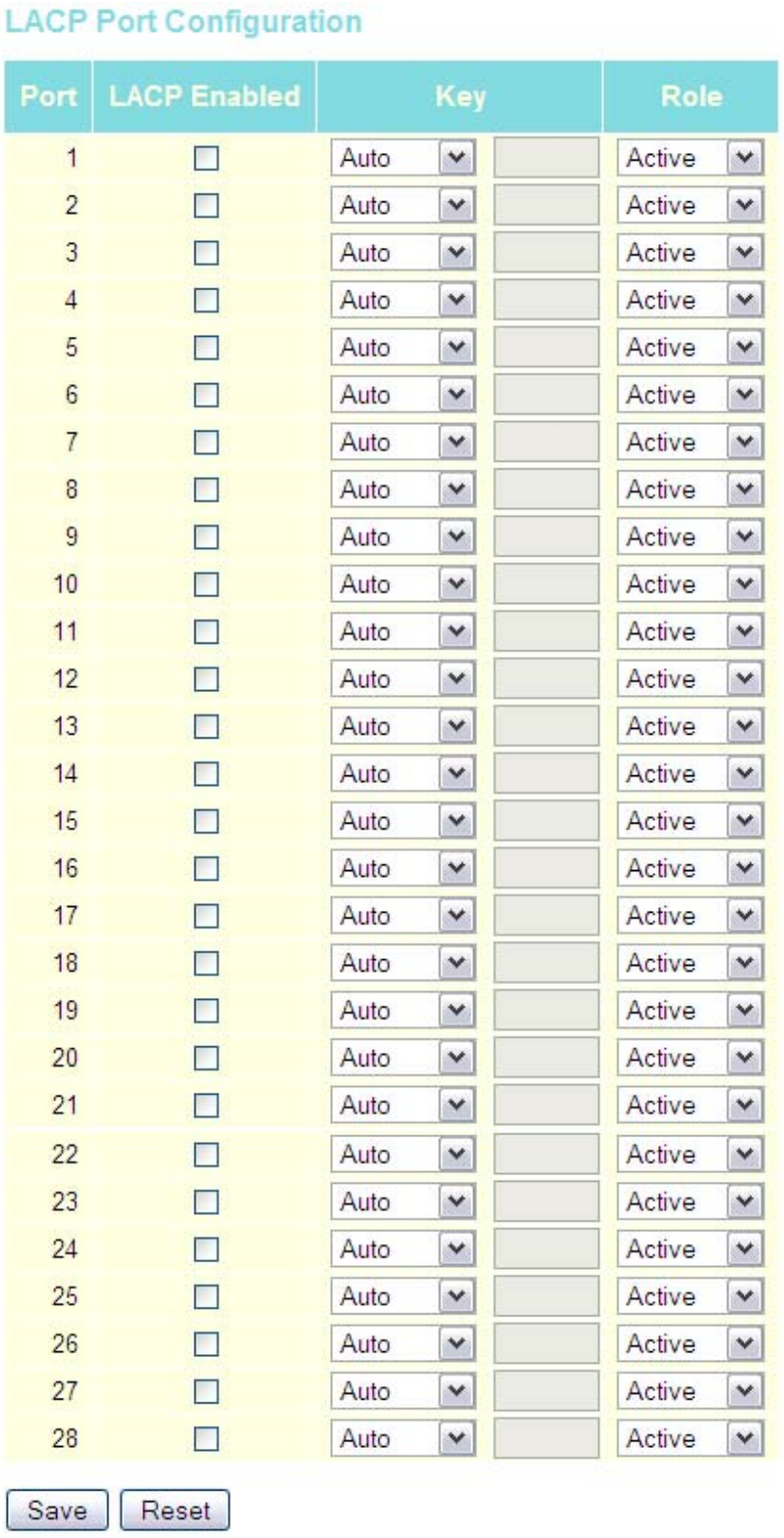
  Select the Specific option to manually configure a key. Use the Auto selection to automatically set the key based on the actual link speed, where 10Mb = 1, 100Mb = 2, and 1Gb = 3.
- **Role** – Configures active or passive LACP initiation mode. Use Active initiation of LACP negotiation on a port to automatically send LACP negotiation packets (once each second). Use Passive initiation mode on a port to make it wait until it receives an LACP protocol packet from a partner before starting negotiations.

WEB INTERFACE

To configure a dynamic trunk:

1. Click Configuration, Aggregation, LACP.
2. Enable LACP on all of the ports to be used in an LAG.
3. Specify the LACP Admin Key to restrict a port to a specific LAG.
4. Set at least one of the ports in each LAG to Active initiation mode, either at the near end or far end of the trunk.
5. Click Save.

Figure 11: LACP Port Configuration

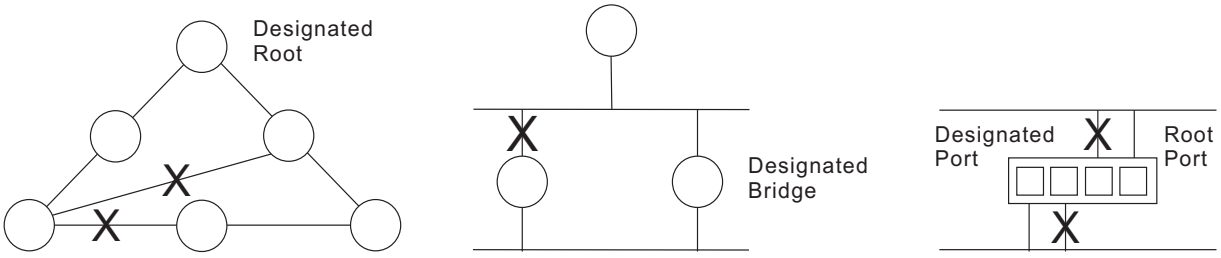


CONFIGURING THE SPANNING TREE ALGORITHM

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.

This switch supports Rapid Spanning Tree Protocol (RSTP), but is backward compatible with Spanning Tree Protocol (STP).

STP - STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



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

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

CONFIGURING GLOBAL SETTINGS FOR STA

Use the RSTP System Configuration page to configure settings for STA which apply globally to the switch.

PARAMETERS

The following parameters are displayed on the RSTP System Configuration page:

- **System 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. (Options: 0-61440, in steps of 4096; Default: 32768)

- **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. (Note that references to "ports" in this section mean "interfaces," which includes both ports and trunks.)

  Minimum: The higher of 6 or [2 x (Hello Time + 1)]
  Maximum: The lower of 40 or [2 x (Forward Delay - 1)]
  Default: 20

- **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.

  Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  Maximum: 30
  Default: 15

- **Transmit Hold Count** – The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. (Range: 1-10; Default: 6)

- **Protocol Version** – Specifies the type of spanning tree used on this switch. (Options: Normal – RSTP, or Compatible – STP;
  Default: Normal)

  RSTP supports connections to either RSTP or STP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  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.

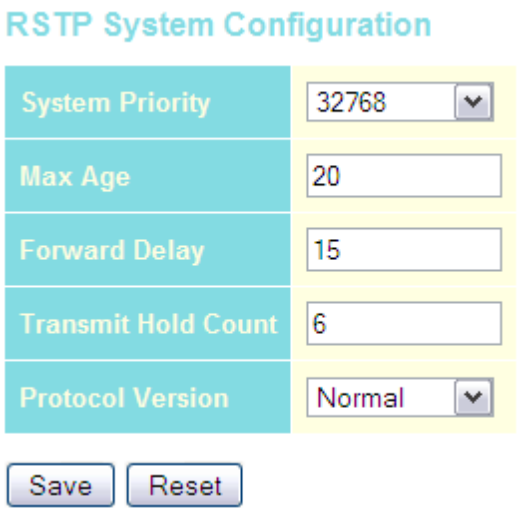
STP Compatible Mode - If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

WEB INTERFACE

To configure global settings for RSTP:

1. Click Configuration, Spanning Tree, System.
2. Modify the required attributes.
3. Click Save.

Figure 12: RSTP System Configuration



CONFIGURING INTERFACE SETTINGS FOR STA

Use the RSTP Port Configuration page to configure RSTP attributes for specific interfaces, including path cost, port priority, edge port (for fast forwarding), automatic detection of an edge port, and point-to-point link type.

PARAMETERS

The following parameters are displayed on the RSTP Port Configuration page:

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

  This field is not applicable to static trunks or dynamic trunks created through LACP. Also, note that only one set of interface configuration settings can be applied to all trunks.

- **RSTP Enabled** – Enables RSTP on this interface. (Default: Enabled)

- **Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

Table 5: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 6: Recommended STA Path Costs

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Table 7: Default STA Path Costs

Port Type	Link Type	IEEE 802.1w-2001
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

- **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. (Range: 0-240, in steps of 16; Default: 128)

- **Admin Edge** (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 this feature should only be enabled for ports connected to an end-node device. (Default: Edge)

- **Auto Edge** – Controls whether automatic edge detection is enabled on a bridge port. When enabled, the bridge can determine that a port is at the edge of the network if no BPDU's received on the port. (Default: Enabled)

- **Point2Point** – The link type attached to an interface can be set to automatically detect the link type, or manually configured as point-to-point or shared medium. Transition to the forwarding state is faster for point-to-point links than for shared media. These options are described below:

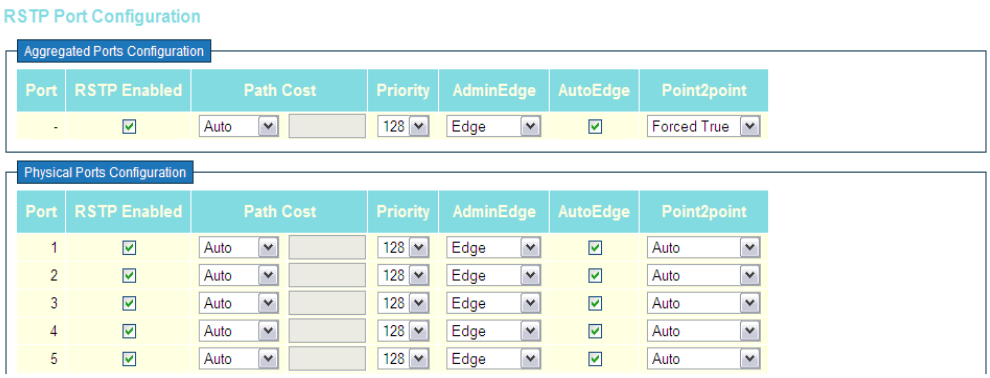
  - **Auto** – The switch automatically determines if the interface is attached to a point-to-point link or to shared medium. (This is the default setting.)
  - **Forced True** – A point-to-point connection to exactly one other bridge.
  - **Forced False** – A shared connection to two or more bridges.

WEB INTERFACE

To configure interface settings for RSTP:

1. Click Configuration, Spanning Tree, Ports.
2. Modify the required attributes.
3. Click Save.

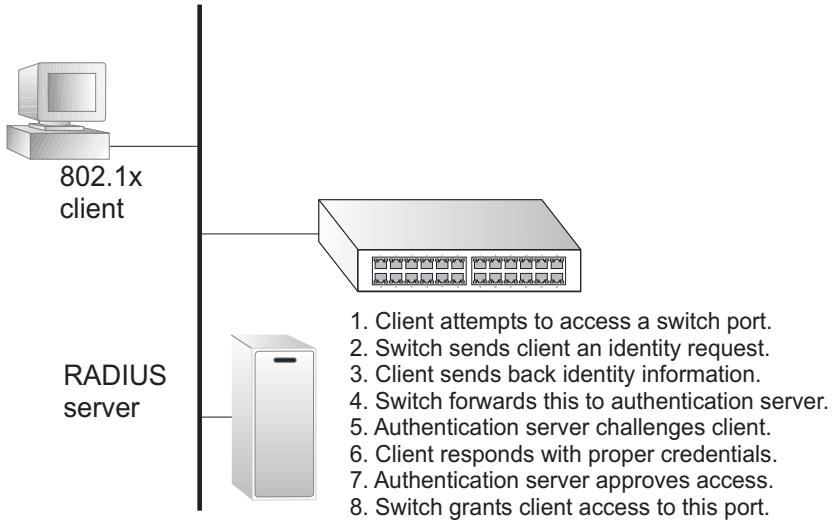
Figure 13: RSTP Port Configuration



CONFIGURING 802.1X PORT AUTHENTICATION

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

The IEEE 802.1X (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.



This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The encryption method used by IEEE 802.1X to pass authentication messages can be MD5 (Message-Digest 5), TLS (Transport Layer Security), PEAP (Protected Extensible Authentication Protocol), or TTLS (Tunneled Transport Layer Security). However, note that the only encryption method supported by MAC-Based authentication is MD5. 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 (see page 51).
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified. Backend RADIUS servers are configured on the Authentication configuration page (see page 60).
- 802.1X / MAC-based authentication must be enabled globally for the switch.
- The Admin State for each switch port that requires client authentication must be set to 802.1X or MAC-based.
- When using 802.1X authentication:
  - Each client that needs to be authenticated must have dot1x client software installed and properly configured.
  - When using 802.1X authentication, the RADIUS server and 802.1X client must support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
  - The RADIUS server and client also have to support the same EAP authentication type - MD5, PEAP, TLS, or TTLS. (Native support for these encryption methods is provided in Windows XP, and in Windows 2000 with Service Pack 4. To support these encryption methods in Windows 95 and 98, you can use the AEGIS dot1x client or other comparable client software.)

MAC-based authentication allows for authentication of more than one user on the same port, and does not require the user to have special 802.1X software installed on his system. The switch uses the client's MAC address to authenticate against the backend server. However, note that intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

USAGE GUIDELINES

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.

PARAMETERS

The following parameters are displayed on the Port Security Configuration page:

System Configuration

- **Mode** - Indicates if 802.1X and MAC-based authentication are globally enabled or disabled on the switch. If globally disabled, all ports are allowed to forward frames.

- **Reauthentication Enabled** - 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)

  For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore does not imply that a client is still present on a port (see Age Period below).

- **Reauthentication Period** - Sets the time period after which a connected client must be re-authenticated. (Range: 1-3600 seconds; Default: 3600 seconds)

- **EAP Timeout** - Sets the time the switch waits for a supplicant response during an authentication session before retransmitting an EAP packet. (Range: 1-255; Default: 30 seconds)

- **Age Period** - The period used to calculate when to age out a client allowed access to the switch through MAC-based authentication as described below. (Range: 10-1000000 seconds; Default: 300 seconds)

  Suppose a client is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch that is running MAC-based authentication, and suppose the client gets successfully authenticated. Now assume that the client powers down his PC. What should make the switch forget about the authenticated client? Reauthentication will not solve this problem, since this doesn't require the client to be present, as discussed under Reauthentication Enabled above. The solution is aging out authenticated clients.

  A timer is started when the client gets authenticated. After half the age period, the switch starts looking for frames sent by the client. If another half age period elapses and no frames are seen, the client is considered removed from the system, and it will have to authenticate again the next time a frame is seen from it. If, on the other hand, the client transmits a frame before the second half of the age period

expires, the switch will consider the client alive, and leave it authenticated. Therefore, an age period of T will require the client to send frames more frequent than T/2 to stay authenticated.

- **Hold Time** - The time after an EAP Failure indication or RADIUS timeout that a client is not allowed access. This setting applies to ports running MAC-based authentication only. (Range: 10-1000000 seconds; Default: 10 seconds)

  If the RADIUS server denies a client access, or a RADIUS server request times out (according to the timeout specified on the Authentication menu, page 60), the client is put on hold in the Unauthorized state. In this state, frames from the client will not cause the switch to attempt to reauthenticate the client.

Port Configuration

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

- **Admin State** - Sets the authentication mode to one of the following options:
  - **Authorized** - Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.)
  - **Unauthorized** - Forces the port to deny access to all clients, either dot1x-aware or otherwise.
  - **802.1X** - Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **MAC-Based** - Enables MAC-based authentication on the port. The switch does not transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic from an unsuccessfully authenticated client will be dropped. Clients that are not (or not yet) successfully authenticated will not be allowed to transmit frames of any kind.

  Port Admin state can only be set to Authorized for ports participating in the Spanning Tree algorithm (see page 73).

  When 802.1X authentication is enabled on a port, the MAC address learning function for this interface is disabled, and the addresses dynamically learned on this port are removed from the common address table.

  Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table. Configured static MAC addresses are added to the secure address table when seen on a switch port (see page 92). Static addresses are treated as authenticated without sending a request to a RADIUS server.

  When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.

- **Port State** - The current state of the port:
  - **Disabled** - 802.1X and MAC-based authentication are globally disabled. (This is the default state.)
  - **Link Down** - 802.1X or MAC-based authentication is enabled, but there is no link on the port.
  - **Authorized** - The port is authorized. This state exists when 802.1X authentication is enabled, the port has a link, the Admin State is "802.1X," and the supplicant is authenticated, or when the Admin State is "Authorized."
  - **Unauthorized** - The port is unauthorized. This state exists when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto," but the supplicant is not (or not yet) authenticated, or when the Admin State is "Unauthorized".
  - X **Auth/**Y **Unauth** - X clients are currently authorized and Y are unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to "MAC-Based."

- **Max Clients** - The maximum number of hosts that can connect to a port when the Admin State is set to "MAC-Based." (Range: 1-112; Default: 112)

  The switch has a fixed pool of state-machines, from which all ports draw whenever a new client is seen on the port. When a given port's maximum is reached (counting both authorized and unauthorized clients), further new clients are disallowed access. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available state-machines.

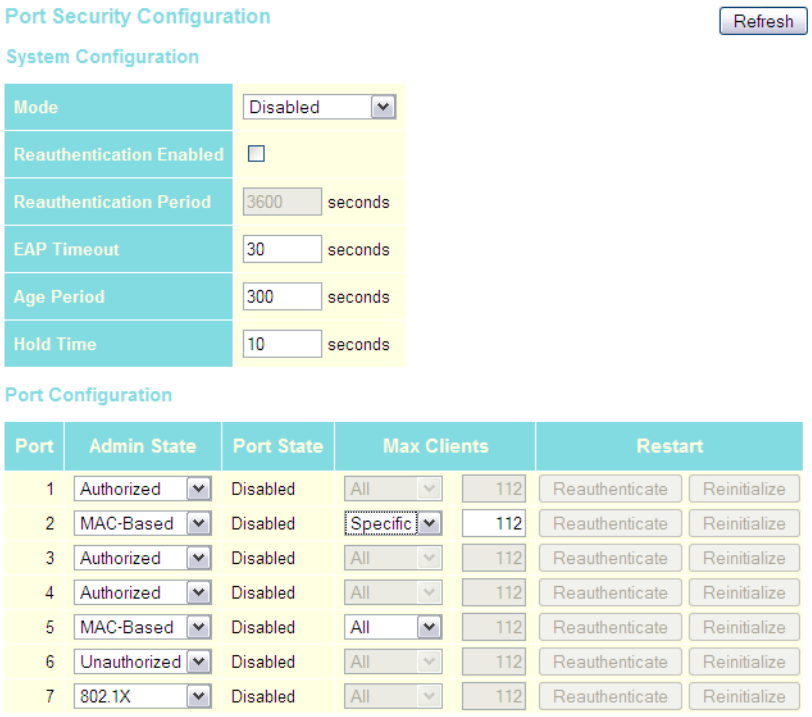
- **Restart** - Restarts client authentication using one of the methods described below. Note that the restart buttons are only enabled when the switch's authentication mode is globally enabled (under System Configuration) and the port's Admin State is "802.X" or "MAC-Based."
  - **Reauthenticate** - Schedules reauthentication to whenever the quiet-period of the port runs out (port-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only effects successfully authenticated ports/clients and will not cause the port/client to be temporarily unauthorized.
  - **Reinitialize** - Forces reinitialization of the port/clients, and therefore immediately starts reauthentication. The port/clients are set to the unauthorized state while reauthentication is ongoing.

WEB INTERFACE

To configure 802.1X Port Security:

1. Click Configuration, Port Security.
2. Modify the required attributes.
3. Click Save.

Figure 14: Port Security Configuration



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.

USAGE GUIDELINES

- 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, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above.

- The following web browsers and operating systems currently support HTTPS:

Table 8: 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, Windows Vista
Netscape 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows Vista, Solaris 2.6
Mozilla Firefox 2.0.0.0 or later	Windows 2000, Windows XP, Windows Vista, Linux

PARAMETERS

The following parameters are displayed on the HTTPS Configuration page:

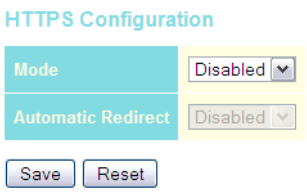
- **Mode** - Enables HTTPS service on the switch. (Default: Disabled)
- **Automatic Redirect** - Sets the HTTPS redirect mode operation. When enabled, management access to the HTTP web interface for the switch are automatically redirected to HTTPS. (Default: Disabled)

WEB INTERFACE

To configure HTTPS:

1. Click Configuration, HTTPS.
2. Enable HTTPS if required and set the Automatic Redirect mode.
3. Click Save.

Figure 15: HTTPS Configuration



CONFIGURING SSH

Secure Shell (SSH) provides 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.

USAGE GUIDELINES

- You need to install an SSH client on the management station to access the switch for management via the SSH protocol. The switch supports both SSH Version 1.5 and 2.0 clients.

- SSH service on this switch only supports password authentication. The password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified on the Authentication menu (page 60).

  To use SSH with 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.

- The SSH service on the switch supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

PARAMETERS

The following parameters are displayed on the SSH Configuration page:

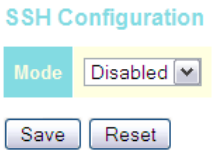
- **Mode** - Allows you to enable/disable SSH service on the switch. (Default: Disabled)

WEB INTERFACE

To configure SSH:

1. Click Configuration, SSH.
2. Enable SSH if required.
3. Click Save.

Figure 16: SSH Configuration



IGMP SNOOPING

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 can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or "snoop" on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the switch. In this case (Layer 2) IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

CONFIGURING IGMP SNOOPING AND QUERY

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.

If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic.

Multicast routers use information from IGMP snooping and query reports, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

PARAMETERS

The following parameters are displayed on the IGMP Snooping Configuration page:

Global Configuration

- **Snooping Enabled** - When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. (Default: Enabled)

  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.

- **Unregistered IPMC Flooding Enabled** - Floods unregistered multicast traffic into the attached VLAN. (Default: Disabled)

  Once the table used to store multicast entries for IGMP snooping is filled, no new entries are learned. If no router port is configured in the attached VLAN, and Unregistered IPMC Flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

- **Leave Proxy Enabled** - Suppresses leave messages unless received from the last member port in the group. (Default: Disabled)

  IGMP leave proxy suppresses all unnecessary IGMP leave messages so that a non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.

  The leave-proxy feature does not function when a switch is set as the querier. When the switch is a non-querier, the receiving port is not the last dynamic member port in the group, the receiving port is not a router port, and no IGMPv1 member port exists in the group, the switch will generate and send a group-specific (GS) query to the member port which received the leave message, and then start the last member query timer for that port.

When the conditions in the preceding item all apply, except that the receiving port is a router port, then the switch will not send a GS-query, but will immediately start the last member query timer for that port.

VLAN Related Configuration

- **VLAN ID** - VLAN Identifier.

- **Snooping Enabled** - When enabled, the switch will monitor network traffic on the indicated VLAN interface to determine which hosts want to receive multicast traffic. (Default: Enabled)

  When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence. When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

- **IGMP Querier** - When enabled, the switch can serve as the Querier (on the selected interface), which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)

  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. This feature is not supported for IGMPv3 snooping.

Port Related Configuration

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

- **Router Port** - Sets a port to function as a router port, which leads towards a Layer 3 multicast device or IGMP querier. (Default: Disabled)

  If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). 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.

- **Fast Leave** - Immediately deletes a member port of a multicast service if a leave packet is received at that port. (Default: Disabled)

  The switch can be configured to immediately delete a member port of a multicast service if a leave packet is received at that port and the Fast Leave function is enabled. This allows the switch to remove a port from the multicast forwarding table without first having to send an IGMP group-specific (GS) query to that interface.

  If Fast Leave is *not* used, a multicast router (or querier) will send a GS-query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.

If Fast Leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, Fast Leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.

Fast Leave is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

Fast Leave does not apply to a port if the switch has learned that a multicast router is attached to it.

Fast Leave can improve bandwidth usage for a network which frequently experiences many IGMP host add and leave requests.

- **Throttling** - Limits the number of multicast groups to which a port can belong. (Range: 1-10; Default: unlimited)

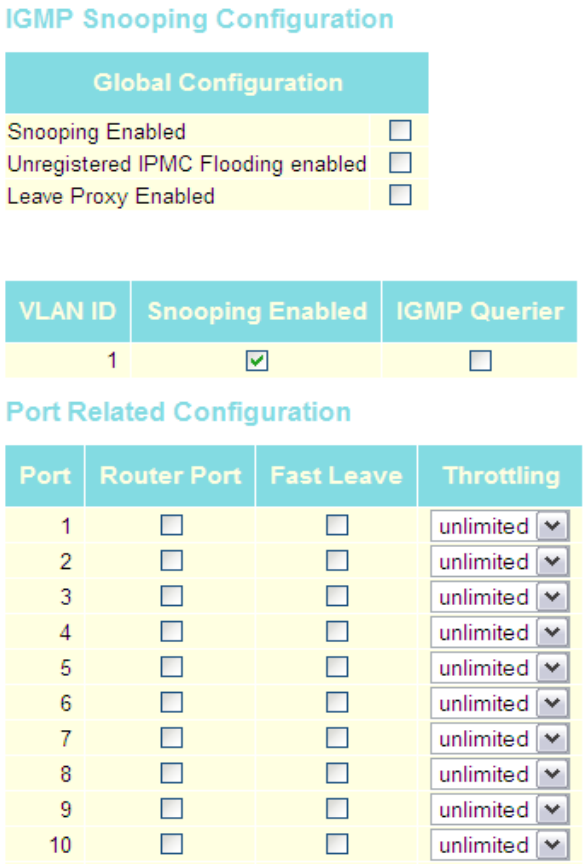
  IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, any new IGMP join reports will be dropped.

WEB INTERFACE

To configure IGMP Snooping:

1. Click Configuration, IGMP Snooping, Basic Configuration.
2. Adjust the IGMP settings as required.
3. Click Save.

Figure 17: IGMP Snooping Configuration



CONFIGURING IGMP FILTERING

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 denying access to specified multicast services on a switch port.

PARAMETERS

The following parameters are displayed on the IGMP Snooping Port Group Filtering Configuration page:

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

- **Filtering Groups** – Multicast groups that are denied on a port. When filter groups are defined, IGMP join reports received on a port are checked against the these groups. If a requested multicast group is denied, the IGMP join report is dropped.

WEB INTERFACE

To configure IGMP Snooping Port Group Filtering:

1. Click Configuration, IGMP Snooping, Port Group Filtering.
2. Click Add New Filtering Group to display a new entry in the table.
3. Select the port to which the filter will be applied.
4. Enter the IP address of the multicast service to be filtered.
5. Click Save.

Figure 18: IGMP Snooping Port Group Filtering Configuration

CONFIGURING LINK LAYER DISCOVERY PROTOCOL

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

PARAMETERS

The following parameters are displayed on the LLDP Configuration page:

LLDP Timing Attributes

- **Tx Interval** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)

  This attribute must comply with the following rule:

(Transmission Interval * Transmission Hold Time) ≤ 65536,
and Transmission Interval ≥ (4 * Transmission Delay)

- **Tx Hold** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 3)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

  TTL in seconds is based on the following rule:

  (Transmission Interval * Transmission Hold Time) ≤ 65536.
  Therefore, the default TTL is 30*3 = 90 seconds.

- **Tx Delay** – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds)

  The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

  This attribute must comply with the rule:
  (4 * Transmission Delay) ≤ Transmission Interval

- **Tx Reinit** – Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds)

  When LLDP is re-initialized on a port, all information in the remote system's LLDP MIB associated with this port is deleted.

LLDP Interface Attributes

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

- **Mode** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Disabled, Enabled - TxRx, Rx only, Tx only; Default: Disabled)

- **CDP Aware** – Enables decoding of Cisco Discovery Protocol frames. (Default: Disabled)

  If enabled, CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded, all others are discarded. CDP TLVs are mapped into LLDP neighbors table as shown below:

  - CDP TLV "Device ID" is mapped into the LLDP "Chassis ID" field.
  - CDP TLV "Address" is mapped into the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.
  - CDP TLV "Port ID" is mapped into the LLDP "Port ID" field.
  - CDP TLV "Version and Platform" is mapped into the LLDP "System Description" field.

- Both the CDP and LLDP support "system capabilities," but the CDP capabilities cover capabilities that are not part of LLDP. These capabilities are shown as "others" in the LLDP neighbors table.

If all ports have CDP awareness disabled, the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the switch.

When CDP awareness for a port is disabled, the CDP information is not removed immediately, but will be removed when the hold time is exceeded.

Optional TLVs - Configures the information included in the TLV field of advertised messages.

- **Port Descr** – 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.

- **Sys Name** – The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name. To configure the system name, see page 50.

- **Sys Descr** – 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.

- **Sys Capa** – 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.

- **Mgmt Addr** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

  The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

  Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

WEB INTERFACE

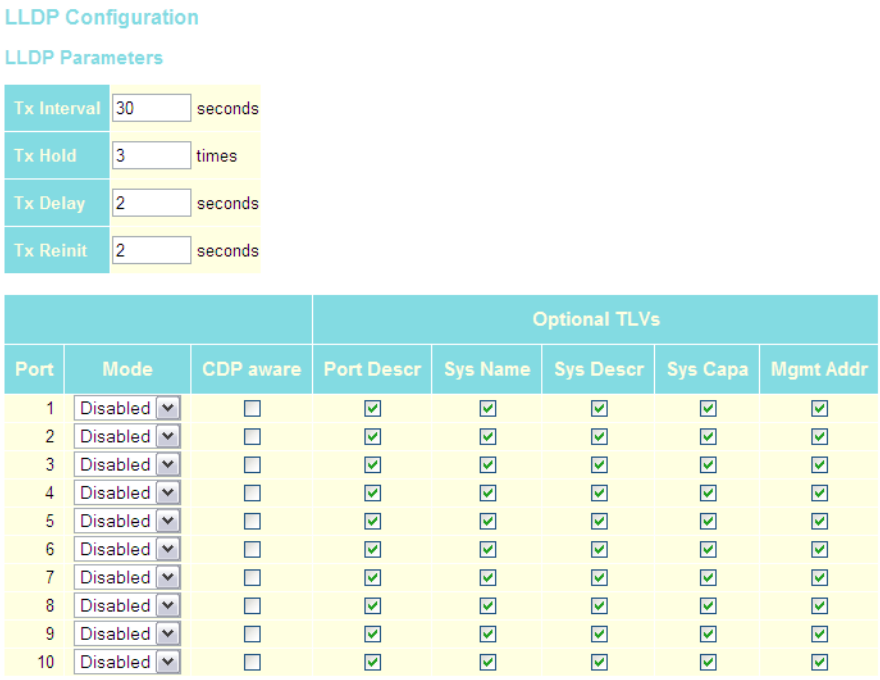
To configure LLDP:

1. Click Configuration, LLDP.

2. Modify any of the timing parameters as required.

3. Set the required mode for transmitting or receiving LLDP messages.
4. Enable or disable decoding CDP frames.
5. Specify the information to include in the TLV field of advertised messages.
6. Click Save.

Figure 19: LLDP Configuration



CONFIGURING THE MAC ADDRESS TABLE

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.

PARAMETERS

The following parameters are displayed on the MAC Address Table Configuration page:

Aging Configuration

- **Disable Automatic Aging** - Disables the automatic aging of dynamic entries. (Address aging is enabled by default.)

- **Age Time** - The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

MAC Table Learning

- **Auto** - Learning is done automatically as soon as a frame with an unknown source MAC address is received. (This is the default.)
- **Disable** - No addresses are learned and stored in the MAC address table.
- **Secure** - Only static MAC address entries are used, all other frames are dropped.

  Make sure that the link used for managing the switch is added to the Static MAC Table before changing to secure learning mode. Otherwise the management link will be lost, and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

NOTE: If the learning mode for a given port in the MAC Learning Table is grayed out, another software module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Static MAC Table Configuration

- **VLAN ID** - VLAN Identifier. (Range: 1-4095)
- **MAC Address** - Physical address of a device mapped to a port.

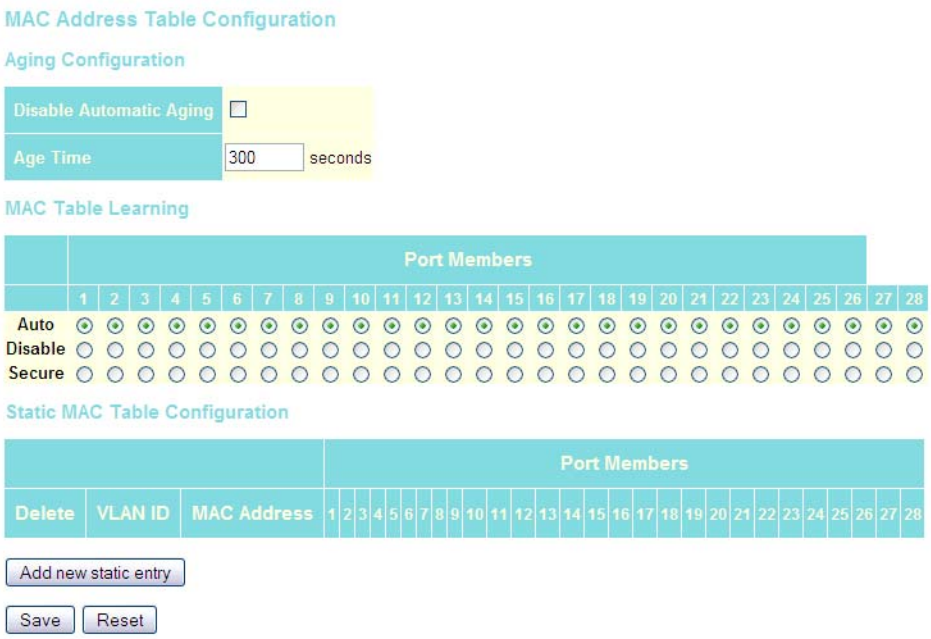
  A static address can be assigned to a specific port on this switch. Static addresses are bound to the assigned port and will not be moved. When a static address is seen on another port, the address will be ignored and will not be written to the address table.
- **Port Members** - Port identifier.

WEB INTERFACE

To configure the MAC Address Table:

1. Click Configuration, MAC Address Table.
2. Change the address aging time if required.
3. Specify the way in which MAC addresses are learned on any port.
4. Add any required static MAC addresses by clicking the Add New Static Entry button, entering the VLAN ID and MAC address, and marking the ports to which the address is to be mapped.
5. Click Save.

Figure 20: MAC Address Table Configuration



IEEE 802.1Q VLANs

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

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

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as 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 256 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging
- 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.

ASSIGNING PORTS TO VLANS

To enable VLANs for this switch, assign each port to the VLAN group(s) in which it will participate.

PARAMETERS

The following parameters are displayed on the VLAN Membership Configuration page:

- **VLAN ID** - VLAN Identifier. (Range: 1-4095)
- **Port Members** - Port identifier.

  Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or

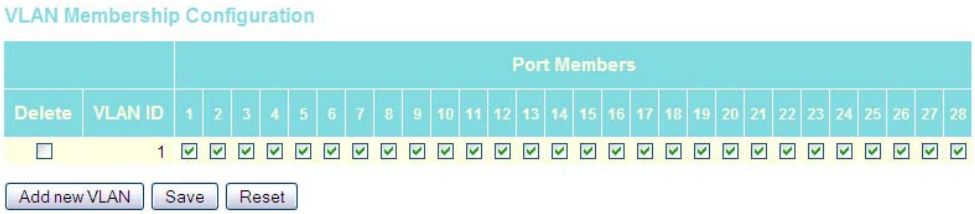
printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you must connect them through a router.

WEB INTERFACE

To configure IEEE 802.1Q VLAN groups:

1. Click Configuration, VLANs, VLAN Membership.
2. Change the ports assigned to the default VLAN (VLAN 1) if required.
3. To configure a new VLAN, click Add New VLAN, enter the VLAN ID, and then mark the ports to be assigned to the new group.
4. Click Save.

Figure 21: VLAN Membership Configuration



CONFIGURING VLAN ATTRIBUTES FOR PORT MEMBERS

You can configure VLAN attributes for specific interfaces, including whether or not the ports are VLAN aware, enabling ingress filtering, accepting Queue-in-Queue frames with embedded tags, setting the accepted frame types, and configuring the default VLAN identifier (PVID).

PARAMETERS

The following parameters are displayed on the VLAN Port Configuration page:

- **Port** - Port identifier.
- **VLAN Aware** - Configures whether or not a port processes the VLAN ID in ingress frames. (Default: Disabled)

  If a port is *not* VLAN aware, all frames are assigned to the default VLAN (as specified by the Port VLAN ID) and tags are not removed.

  If a port is VLAN aware, each frame is assigned to the VLAN indicated in the VLAN tag, and the tag is removed.
- **Ingress Filtering** - Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)
  - Ingress filtering only affects tagged frames.
  - If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.

- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports.
- 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.

- **Queue in Queue** - Determines whether the port accepts double tagged frames. If the port doesn't accepts double tagged frames, double tagged frames received on the port are discarded. (Default: Disabled)

- **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. When set to receive only tagged frames, all untagged frames received on the interface are discarded. (Option: All, Tagged; Default: All)

- **Port VLAN Mode** - Determines how to process VLAN tags for ingress and egress traffic. (Options: Specific, None; Default: Specific)

  - **Specific** - If the port is VLAN aware, untagged frames received on the port are assigned to the default PVID, and tagged frames are processed using the frame's VLAN ID. If the port is not VLAN aware, all frames received on the port are assigned to the default PVID.

    Regardless of whether or not a port is VLAN aware, if the VLAN to which the frame has been assigned is different from the default PVID, a tag indicating the VLAN to which this frame was assigned will be inserted in the egress frame. Otherwise, the frame is transmitted without a VLAN tag.

  - **None** - The ID for the VLAN to which this frame has been assigned is inserted in frames transmitted from the port. The assigned VLAN ID can be based on the ingress tag for tagged frames, or the default PVID for untagged ingress frames. Note that this mode is normally used for ports connected to VLAN-aware switches.

  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 should first strip off the VLAN tag before forwarding the frame.

- **Port VLAN ID** - VLAN ID assigned to untagged frames received on the interface. (Range: 1-4095; Default: 1)

  The port must be a member of the same VLAN as the Port VLAN ID.

WEB INTERFACE

To configure attributes for VLAN port members:

1. Click Configuration, VLANs, Ports.
2. Configure in the required settings for each interface.
3. Click Save.

Figure 22: VLAN Port Configuration

VLAN Port Configuration

Port	VLAN Aware	Ingress Filtering	Queue in Queue	Frame Type	Port VLAN	
					Mode	ID
1	☐	☐	☐	All	Specific	1
2	☐	☐	☐	All	Specific	1
3	☐	☑	☐	Tagged	Specific	3
4	☐	☐	☐	All	Specific	1
5	☐	☐	☐	All	Specific	1
6	☐	☐	☐	All	Specific	1
7	☐	☐	☐	All	Specific	1
8	☐	☐	☐	All	Specific	1
9	☐	☐	☐	All	Specific	1
10	☐	☐	☐	All	Specific	1

CONFIGURING PRIVATE VLANS

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on ports assigned to a private VLAN can only be forwarded to, and from, uplink ports (that is, ports configured as members of both a standard IEEE 802.1Q VLAN and the private VLAN).

Ports isolated in the private VLAN are designated as downlink ports, and can not communicate with any other ports on the switch except for the uplink ports. Ports assigned to both a private VLAN and an 802.1Q VLAN are designated as uplink ports, and can communicate with any downlink ports within the same private VLAN to which it has been assigned, and to any other ports within the 802.1Q VLANs to which it has been assigned.

One example of how private VLANs can be used is in servicing multi-tenant dwellings. If all of the tenants are assigned to a private VLAN, then no traffic can pass directly between the tenants on the local switch. Communication with the outside world is restricted to the uplink ports which may connect to one or more service providers (such as Internet, IPTV, or VOIP). More than one private VLAN can be configured on the switch if a different set of service providers is required for other client groups.

PARAMETERS

The following parameters are displayed on the Private VLAN Membership Configuration page:

- **PVLAN ID** - Private VLAN identifier. (Range: 1-4095)

  By default, all ports are configured as members of VLAN 1 and PVLAN 1. Because all of these ports are members of 802.1Q VLAN 1, isolation cannot be enforced between the members of PVLAN 1. To use PVLAN 1 properly, remove the ports to be isolated from VLAN 1 (see page 95). Then connect the uplink ports to the local servers or other service providers to which the members of PVLAN 1 require access.

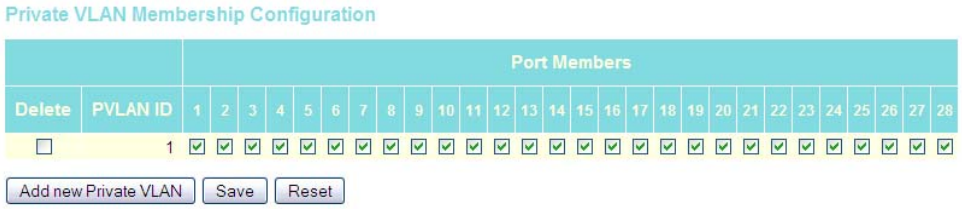
- **Port** - Port identifier.

WEB INTERFACE

To configure VLAN port members for private VLANs:

1. Click Configuration, Private VLANs, PVLAN Membership.
2. Add or delete members of any existing PVLAN, or click Add New Private VLAN and mark the port members.
3. Click Save.

Figure 23: Private VLAN Membership Configuration



USING PORT ISOLATION

Ports within a private VLAN (PVLAN) are isolated from other ports which are not in the same PVLAN. Port Isolation can be used to further prevent communications between ports within the same PVLAN. An isolated port cannot forward any unicast, multicast, or broadcast traffic to any other ports in the same PVLAN.

PARAMETERS

The following parameters are displayed on the Port Isolation Configuration page:

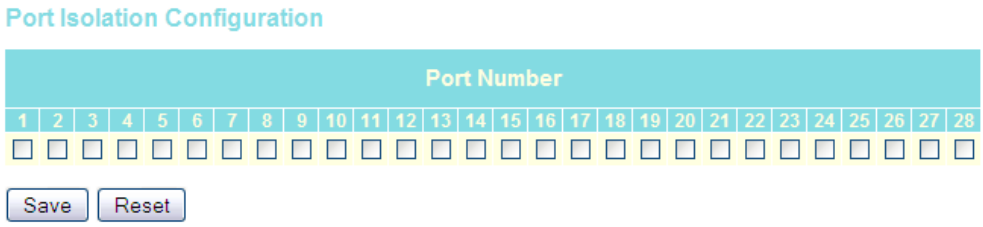
- **Port** - Port identifier.

WEB INTERFACE

To configure isolated ports:

1. Click Configuration, Private VLANs, Port Isolation.
2. Mark the ports which are to be isolated from each other.
3. Click Save.

Figure 24: Port Isolation Configuration



QUALITY OF SERVICE

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 is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end Quality of Service (QoS) solution.

This section describes how to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch provides four 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 queuing mode, and queue weights.

The switch also allows you to configure QoS classification criteria and service policies. The switch's resources can be prioritized to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS, or its VLAN priority tag. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

CONFIGURING PORT-LEVEL QUEUE SETTINGS

You can specify the default port priority for each port on the switch, a Quality Control List (which sets the priority for ingress packets based on detailed criteria), the default tag assigned to egress packets, the queuing mode, and queue weights.

PARAMETERS

The following parameters are displayed on the Port QoS Configuration page:

- **Port** - Port identifier.
- **Default Class** - The priority assigned to frames that do not match any of the entries in the assigned Quality Control List (see page 104). (Options: Low, Normal, Medium, High; Default: Low)
- **QCL #** - A Quality Control List which classifies ingress frames based on criteria including Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS, or VLAN priority tag (see page 104). Traffic matching the first entry in the QCL is assigned to the traffic class (output queue) defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port. (Range: 1-28)
- **Tag Priority** - The default priority used when adding a tag to untagged frames. (Range: 0-7; Default: 0)

  The default tag priority applies to untagged frames 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.

  Inbound frames that do not have VLAN tags are tagged with the input port's default ingress tag priority, and then placed in the appropriate priority queue at 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.)
- **Queuing Mode** - Sets the switch to service the queues based on a strict rule that requires all traffic in a higher priority queues to be processed before lower priority queues are serviced, or uses Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. (Default: Strict)
- **Queue Weight** - When the Queuing Mode is set to Weighted, the switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. The traffic classes are mapped to one of the egress queues provided for each port. You can assign a weight to each of these queues, and thereby to the corresponding traffic priorities. (Range: 1, 2, 4, 8; Default: Low - 1, Normal - 2, Medium - 4, High - 8)

  WRR uses a relative weighting for each queue which determines the number of packets the switch transmits every time it services each queue before moving on to the next queue. Thus, a queue weighted 8

will be allowed to transmit up to 8 packets, after which the next lower priority queue will be serviced according to it's weighting. This prevents the head-of-line blocking that can occur with strict priority queuing. This weight determines 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.

WEB INTERFACE

To configure port-level QoS:

1. Click Configuration, QoS, Ports.
2. Set the required queue attributes for each port.
3. Click Save.

Figure 25: Port QoS Configuration

Port QoS Configuration

Ingress Configuration				Egress Configuration				
Port	Default Class	QCL #	Tag Priority	Queuing Mode	Queue Weighted			
					Low	Normal	Medium	High
1	Low	1	0	Strict Priority	1	2	4	8
2	Low	1	0	Strict Priority	1	2	4	8
3	Low	1	0	Weighted	1	2	4	8
4	Low	1	0	Strict Priority	1	2	4	8
5	Low	1	0	Strict Priority	1	2	4	8
6	Low	1	0	Strict Priority	1	2	4	8
7	Low	1	0	Strict Priority	1	2	4	8
8	Low	1	0	Strict Priority	1	2	4	8
9	Low	1	0	Strict Priority	1	2	4	8
10	Low	1	0	Strict Priority	1	2	4	8

CONFIGURING DSCP REMARKING

The Differentiated Services Code Point should be set at network boundaries, or by trusted hosts within those boundaries, to ensure a consistent service policy for different types of traffic. Services can be realized by the use of particular packet classification (based on DSCP remarking), buffer management, and traffic conditioning mechanisms (that is, traffic shaping as provided by the Rate Limiters described on page 111).

In the packet forwarding path, differentiated services are realized by mapping the codepoint contained in a field in the IP packet header to a particular forwarding treatment, or per-hop behavior (PHB), at each network node along its path. Traffic conditioners may include the primitives of marking, metering, policing and shaping.

PARAMETERS

The following parameters are displayed on the DSCP Remarking Configuration page:

- **Port** - Port identifier.
- **DSCP Remarking Mode** - Enables or disables remarking of the DSCP bits for egress packets placed in this queue. (Default: Disabled)
- **DSCP Queue Mapping** - Maps the DSCP value assigned to egress packets entering each queue. Supported DSCP code points include:
  - **Best Effort** - This is the common, best-effort forwarding behavior standardized in RFC1812. When no other suitable criteria are available to classify a packet, it is assumed that it belongs to this service aggregate. Such packets may be sent into a network without adhering to any particular rules, and the network will deliver as many of these packets as possible and as soon as possible. A reasonable implementation would be a queueing discipline that sends packets of this aggregate whenever the output link is not required to service any of the other queues.
  - **CS1**-**CS7** - Class Selector code points which use values compatible with IP Precedence and IEEE 802.1p.
  - **Expedited Forwarding** - DSCP value assigned to highest priority traffic as described in RFC2598. This code point can be used to build a low loss, low latency, low jitter, assured bandwidth, end-to-end service through DiffServ domains. Such a service appears to the endpoints like a point-to-point connection or a "virtual leased line."

WEB INTERFACE

To configure port-level DSCP remarking:

1. Click Configuration, QoS, DSCP Remarking.
2. Enable remarking on each port for which it is required.
3. Assign DSCP values to use for each of the egress queues.
4. Click Save.

Figure 26: DSCP Remarking Configuration

DSCP Remarking Configuration

Port	DSCP Remarking Mode	DSCP Queue Mapping			
		Low	Normal	Medium	High
1	Disabled	CS1	CS2	CS3	CS4
2	Disabled	CS1	CS2	CS3	CS4
3	Disabled	CS1	CS2	CS3	CS4
4	Disabled	CS1	CS2	CS3	CS4
5	Disabled	CS1	CS2	CS3	CS4
6	Disabled	CS1	CS2	CS3	CS4
7	Disabled	CS1	CS2	CS3	CS4
8	Disabled	CS1	CS2	CS3	CS4
9	Disabled	CS1	CS2	CS3	CS4
10	Disabled	CS1	CS2	CS3	CS4

CONFIGURING QOS CONTROL LISTS

Configures Quality of Service policies for handling ingress packets based on Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS, or VLAN priority tag. Each list may consist of up to 24 entries, and can be mapped to a specific port using the Port QoS Configuration menu (page 101).

Once a QCL is mapped to a port, traffic matching the first entry in the QCL is assigned to the traffic class (Low, Medium, Normal or High) defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port.

PARAMETERS

The following parameters are displayed on the QoS Control List Configuration page:

QCL Configuration

- **QCL** - A list of classification criteria used to determine the traffic class to which a frame is assigned. Up to 28 QCLs can be configured, each containing up to 24 entries. QCLs can be mapped to a port using the Port QoS Configuration menu (page 101)
- **QCE Type** - Specifies which frame field the Quality Control Entry (QCE) processes to determine the QoS class of the frame. QCE types are described later in this section.

- **Type Value** - A value which depends on the selected QCE type. Type values are also described later in this section.
- **Traffic Class** - The QoS class associated with a QCE.

The following buttons are used to edit or move the QCEs:

Table 9: QCE Modification Buttons

Button	Description
	Inserts a new QCE before the current row.
	Edits the QCE.
	Moves the QCE up the list.
	Moves the QCE down the list.
	Deletes the QCE.
	The lowest plus sign adds a new entry at the bottom of the list.

QCE Configuration

- **QCE Type** - Specifies which frame field the Quality Control Entry (QCE) processes to determine the QoS class of the frame. The supported types are listed below:
  - **Ethernet Type** - This option can only be used to filter Ethernet II formatted packets. (Range: 600-ffff hex; Default: ffff)

    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).
  - **VLAN ID** - VLAN ID. (Range: 1-4095; Default: 1)
  - **TCP/UDP Port** - Source/destination port number or range. (Range: 0-65535; Default: 0-65535)
  - **DSCP** - IPv4/IPv6 DSCP priority level. (Range: 0-63; Default: 63)
  - **ToS** - Type of Service level, which processes the precedence part of the IPv4/IPv6 ToS (3 bits) as an index to the eight QoS Class values. (Range: Low, Normal, Medium, High; Default: Low)
  - **Tag Priority** - Uses the User Priority value (3 bits as defined by IEEE 802.1p) as an index to the eight QoS Class values.

    The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

    Table 10: Mapping CoS Values to Egress Queues

Priority	0	1	2	3	4	5	6	7
Queue	Normal	Low	Low	Normal	Medium	Medium	High	High

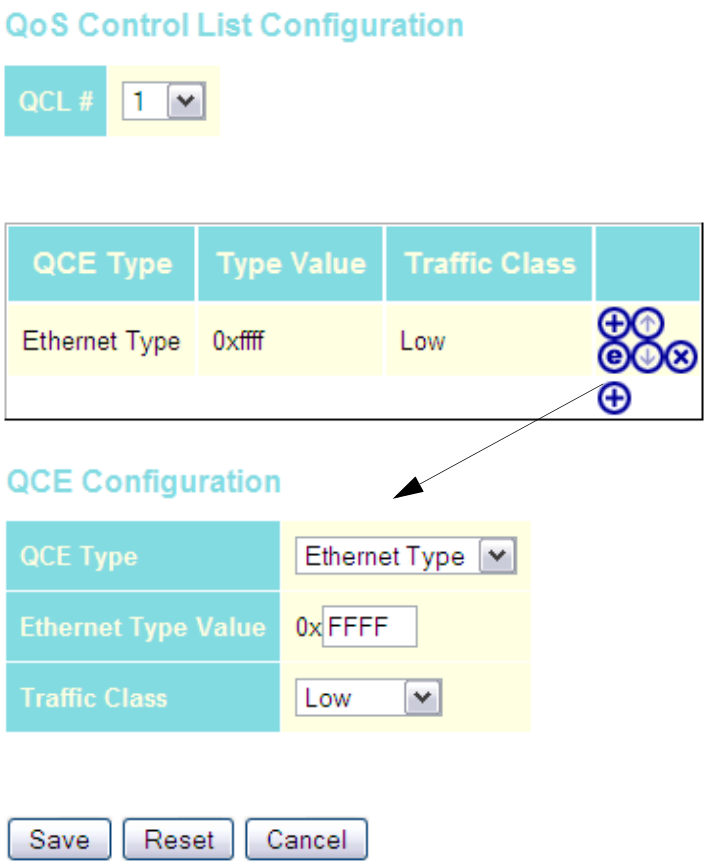
- **Traffic Class** - Output queue buffer. (Range: Low, Normal, Medium and High, where High is the highest CoS priority queue)

WEB INTERFACE

To configure QoS Control Lists:

1. Click Configuration, QoS, Control Lists.
2. Click the ⊕ button to add a new QCL, or use the other QCL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).
3. When editing an entry on the QCE Configuration page, select the QCE type, specify the relevant criteria to be matched for this type, and set the traffic class to which traffic matching this criteria will be assigned.
4. Click Save.

Figure 27: QoS Control List Configuration



CONFIGURING RATE LIMITING

Rate limiting controls the maximum rate for traffic transmitted or received on an interface. Rate limiting can be configured on interfaces at the edge of a network to form part of the customer service package by limiting traffic into or out of the switch. Packets that exceed the acceptable amount of traffic are dropped, while conforming traffic is forwarded without any changes.

PARAMETERS

The following parameters are displayed on the Rate Limit Configuration page:

- **Port** - Port identifier.

Ingress Limits

- **Policer Enabled** - Enables or disables ingress rate limiting. (Default: Disabled)
- **Policer Rate** - Configure the rate for the port policer. (Range: 500-1000000 kbps, or 1-1000 Mbps; Default: 500 kbps)
- **Policer Unit** - Sets the unit of measure for the port policer. (Options: kbps, Mbps; Default: kbps)

Egress Limits

- **Shaper Enabled** - Enables or disables egress rate limiting. (Default: Disabled)
- **Shaper Rate** - Configures the rate for the port shaper. (Range: 500-1000000 kbps, or 1-1000 Mbps; Default: 500 kbps)
- **Shaper Unit** - Sets the unit of measure for the port shaper. (Options: kbps, Mbps; Default: kbps)

WEB INTERFACE

To configure Rate Limits:

1. Click Configuration, QoS, Rate Limiters.
2. To set an rate limit on ingress traffic, check Policer Enabled box next to the required port, set the rate limit in the Policer Rate field, and select the unit of measure for the traffic rate.
3. To set an rate limit on egress traffic, check Shaper Enabled box next to the required port, set the rate limit in the Shaper Rate field, and select the unit of measure for the traffic rate.
4. Click Save.

Figure 28: Rate Limit Configuration

Rate Limit Configuration

Port	Policer Enabled	Policer Rate	Policer Unit	Shaper Enabled	Shaper Rate	Shaper Unit
1	☐	500	kbps	☐	500	kbps
2	☐	500	kbps	☐	500	kbps
3	☑	600	kbps	☐	600	kbps
4	☐	500	kbps	☐	500	kbps
5	☐	500	kbps	☐	500	kbps
6	☐	500	kbps	☐	500	kbps
7	☐	500	kbps	☐	500	kbps
8	☐	500	kbps	☐	500	kbps
9	☐	500	kbps	☐	500	kbps
10	☐	500	kbps	☐	500	kbps

CONFIGURING STORM CONTROL

You can configure limits on broadcast, multicast and unknown unicast traffic to control traffic storms which may occur when a network device is malfunctioning, the network is not properly configured, or application programs are not well designed or properly configured. Traffic storms caused by any of these problems can severely degrade performance or bring your network to a complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast, or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped. Note that the limit specified on this page applies to each port.

PARAMETERS

The following parameters are displayed on the Storm Control Configuration page:

- **Frame Type** - Specifies broadcast, multicast or unknown unicast traffic.
- **Status** - Enables or disables storm control. (Default: Disabled)
- **Rate** (pps) - The threshold above which packets are dropped. This limit can be set by specifying a value of 2^n packets per second (pps), or by selecting one of the options in Kpps (i.e., marked with the suffix "K"). (Options: 2^n pps where n = 1, 2, 4, 8, 16, 32, 64, 128, 256, 512; or 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024 Kpps; Default: 2 pps)

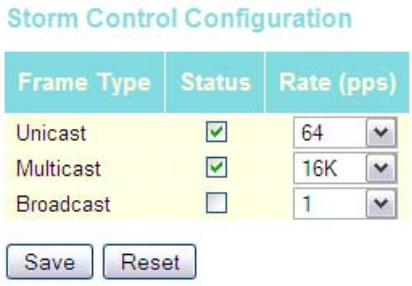
  Due to an ASIC limitation, the enforced rate limits are slightly less than the listed options. For example: 1 Kpps translates into an enforced threshold of 1002.1 pps.

WEB INTERFACE

To configure Storm Control:

1. Click Configuration, QoS, Storm Control.
2. Enable storm control for unknown unicast, broadcast, or multicast traffic by marking the Status box next to the required frame type.
3. Select the control rate as a function of 2^n pps (i.e., a value with no suffix for the unit of measure) or a rate in Kpps (i.e., a value marked with the suffix "K").
4. Click Save.

Figure 29: Storm Control Configuration



ACCESS CONTROL LISTS

An Access Control List (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 packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

ASSIGNING ACL POLICIES AND RESPONSES

The ACL Port Configuration page can be used to define a port to which matching frames are copied, enable logging, or shut down a port when a matching frame is seen. Note that rate limiting (configured with the Rate Limiter menu, page 111) is implemented regardless of whether or not a matching packet is seen.

PARAMETERS

The following options are displayed on the ACL Port Configuration page:

- **Port** - Port Identifier.

- **Policy ID** - An ACL policy configured on the ACE Configuration page (page 114). (Range: 1-8; Default: 1, which is undefined)
- **Action** - Permits or denies a frame based on whether it matches a rule defined in the assigned policy. (Default: Permit)
- **Rate Limiter ID** - Specifies a rate limiter (page 111) to apply to the port. (Range: 1-14; Default: Disabled)
- **Port Copy** - Defines a port to which matching frames are copied. (Range: 1-28; Default: Disabled)
- **Shutdown** - Shuts down a port when a macthing frame is seen. (Default: Disabled)
- **Counter** - The number of frames which have matched any of the rules defined in the selected policy.

WEB INTERFACE

To configure ACL policies and responses for a port:

1. Click Configuration, ACL, Ports.
2. Assign an ACL policy configured on the ACE Configuration page, specify the responses to invoke when a matching frame is seen, including the filter mode, copying matching frames to another port, or shutting down the port. Note that the setting for rate limiting is implemented regardless of whether or not a matching packet is seen.
3. Repeat the preceding step for each port to which an ACL will be applied.
4. Click Save.

Figure 30: ACL Port Configuration

ACL Ports Configuration

Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Shutdown	Counter
1	1	Permit	Disabled	Disabled	Disabled	0
2	1	Permit	Disabled	Disabled	Disabled	0
3	1	Permit	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	Disabled	0
8	1	Permit	Disabled	Disabled	Disabled	0
9	1	Permit	Disabled	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	Disabled	0

CONFIGURING RATE LIMITERS

The ACL Rate Limiter Configuration page is used to define the rate limits applied to a port (as configured either through the ACL Ports Configuration menu (page 110) or the Access Control List Configuration menu (page 112).

PARAMETERS

The following options are displayed on the ACL Rate Limiter Configuration page:

- **Rate Limiter ID** - Rate limiter identifier. (Range: 0-14; Default: 1)
- **Rate** (pps) - The threshold above which packets are dropped. (Options: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, 1024K pps; Default: 1 pps)

  Due to an ASIC limitation, the enforced rate limits are slightly less than the listed options. For example: 1 Kpps translates into an enforced threshold of 1002.1 pps.

WEB INTERFACE

To configure rate limits which can be applied to a port:

1. Click Configuration, ACL, Rate Limiters.
2. For any of the rate limiters, select the maximum ingress rate that will be supported on a port once a match has been found in an assigned ACL.
3. Click Save.

Figure 31: ACL Rate Limiter Configuration

CONFIGURING ACCESS CONTROL LISTS

The Access Control List Configuration page is used to define filtering rules for an ACL policy, for a specific port, or for all ports. Rules applied to a port

take effect immediately, while those defined for a policy must be mapped to one or more ports using the ACL Ports Configuration menu (page 110).

USAGE GUIDELINES

- Rules within an ACL are checked in the configured order, from top to bottom. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted.
- The maximum number of ACL rules that can be configured on the switch is 128.
- The maximum number of ACL rules that can be bound to a port is 10.
- ACLs provide frame filtering based on any of the following criteria:
  - Any frame type (based on MAC address, VLAN ID, VLAN priority)
  - Ethernet type (based on Ethernet type value, MAC address, VLAN ID, VLAN priority)
  - ARP (based on ARP/RARP type, request/reply, sender/target IP, hardware address matches ARP/RARP MAC address, ARP/RARP hardware address length matches protocol address length, matches this entry when ARP/RARP hardware address is equal to Ethernet, matches this entry when ARP/RARP protocol address space setting is equal to IP (0x800)
  - IPv4 frames (based on destination MAC address, protocol type, TTL, IP fragment, IP option flag, source/destination IP, VLAN ID, VLAN priority)

PARAMETERS

The following options are displayed on the Access Control List Configuration page:

ACCESS CONTROL LIST CONFIGURATION

- **Ingress Port** - Any port, port identifier, or policy.
- **Frame Type** - The type of frame to match.
- **Action** - Shows whether a frame is permitted or denied when it matches an ACL rule.
- **Rate Limiter** - Shows if rate limiting will be enabled or disabled when matching frames are found.
- **Port Copy** - Shows the port to which matching frames are copied.
- **Logging** - Shows if logging of matching frames to the system log is enabled or disabled.

Open the System Log Information menu (page 137) to view any entries stored in the system log for this entry. Related entries will be displayed under the "Info" or "All" logging levels.

- **Shutdown** - Shows if a port is shut down when a macthing frame is found.
- **Counter** - Shows he number of frames which have matched any of the rules defined for this ACL.

The following buttons are used to edit or move the ACL entry (ACE):

Table 11: QCE Modification Buttons

Button	Description
	Inserts a new ACE before the current row.
	Edits the ACE.
	Moves the ACE up the list.
	Moves the ACE down the list.
	Deletes the ACE.
	The lowest plus sign adds a new entry at the bottom of the list.

ACE CONFIGURATION

Ingress Port and Frame Type

- **Ingress Port** - Any port, port identifier, or policy. (Options: Any port, Port 1-28, Policy 1-8; Default: Any)
- **Frame Type** - The type of frame to match. (Options: Any, Ethernet, ARP, IPv4; Default: Any)

Filter Criteria Based on Selected Frame Type

- Any frame type:

  MAC Parameters

  - **DMAC Filter** - The type of destination MAC address. (Options: Any, MC - multicast, BC - broadcast, UC - unicast; Default: Any)

- Ethernet:

  MAC Parameters

  - **SMAC Filter** - The type of source MAC address. (Options: Any, MC - multicast, BC - broadcast, UC - unicast, Specific - user defined; Default: Any)

- **DMAC Filter** - The type of destination MAC address. (Options: Any, MC - multicast, BC - broadcast, UC - unicast, Specific - user defined; Default: Any)

Ethernet Type Parameters

- **EtherType Filter** - This option can only be used to filter Ethernet II formatted packets. (Options: Any, Specific (600-ffff hex); Default: Any)

  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).

◆ ARP:

MAC Parameters

- **SMAC Filter** - The type of source MAC address. (Options: Any, MC - multicast, BC - broadcast, UC - unicast, Specific - user defined; Default: Any)

- **DMAC Filter** - The type of destination MAC address. (Options: Any, MC - multicast, BC - broadcast, UC - unicast; Default: Any)

ARP Parameters

- **ARP/RARP** - Specifies the type of ARP packet. (Options: Any - no ARP/RARP opcode flag is specified, ARP - frame must have ARP/RARP opcode set to ARP, RARP - frame must have ARP/RARP opcode set to RARP, Other - frame has unknown ARP/RARP opcode flag; Default: Any)

- **Request/Reply** - Specifies whether the packet is an ARP request, reply, or either type. (Options: Any - no ARP/RARP opcode flag is specified, Request - frame must have ARP Request or RARP Request opcode flag set, Reply - frame must have ARP Reply or RARP Reply opcode flag; Default: Any)

- **Sender IP Filter** - Specifies the sender's IP address. (Options: Any - no sender IP filter is specified, Host - specifies the sender IP address in the SIP Address field, Network - specifies the sender IP address and sender IP mask in the SIP Address and SIP Mask fields; Default: Any)

- **Target IP Filter** - Specifies the destination IP address. (Options: Any - no target IP filter is specified, Host - specifies the target IP address in the Target IP Address field, Network - specifies the target IP address and target IP mask in the Target IP Address and Target IP Mask fields; Default: Any)

- **ARP SMAC Match** - Specifies whether frames can be matched according to their sender hardware address (SHA) field settings. (0ptions: Any - any value is allowed, 0 - ARP frames where SHA is

not equal to the SMAC address, 1 - ARP frames where SHA is equal to the SMAC address; Default: Any)

- **RARP DMAC Match** - Specifies whether frames can be matched according to their target hardware address (THA) field settings. (Options: Any - any value is allowed, 0 - RARP frames where THA is not equal to the DMAC address, 1 - RARP frames where THA is equal to the DMAC address; Default: Any)

- **IP/Ethernet Length** - Specifies whether frames can be matched according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. (Options: Any - any value is allowed, 0 - ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry, 1 - ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry; Default: Any)

- **IP** - Specifies whether frames can be matched according to their ARP/RARP hardware address space (HRD) settings. (Options: Any - any value is allowed, 0 - ARP/RARP frames where the HRD is equal to Ethernet (1) must not match this entry, 1 - ARP/RARP frames where the HRD is equal to Ethernet (1) must match this entry; Default: Any)

- **Ethernet** - Specifies whether frames can be matched according to their ARP/RARP protocol address space (PRO) settings. (Options: Any - any value is allowed, 0 - ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry, 1 - ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry; Default: Any)

◆ IPv4:

MAC Parameters

- **DMAC Filter** - The type of destination MAC address. (Options: Any, MC - multicast, BC - broadcast, UC - unicast; Default: Any)

IP Parameters

- **IP Protocol Filter** - Specifies the IP protocol to filter for this rule. (Options: Any, ICMP, UDP, TCP, Other; Default: Any)

  The following additional fields are displayed when these protocol filters are selected.

  ICMP Parameters

  - **ICMP Type Filter** - Specifies the type of ICMP packet to filter for this rule. (Options: Any, Specific: 0-255; Default: Any)

- **ICMP Code Filter** - Specifies the ICMP code of an ICMP packet to filter for this rule. (Options: Any, Specific (0-255); Default: Any)

UDP Parameters

- **Source Port Filter** - Specifies the UDP source filter for this rule. (Options: Any, Specific (0-65535), Range (0-65535); Default: Any)

- **Dest. Port Filter** - Specifies the UDP destination filter for this rule. (Options: Any, Specific (0-65535), Range (0-65535); Default: Any)

TCP Parameters

- **Source Port Filter** - Specifies the TCP source filter for this rule. (Options: Any, Specific (0-65535), Range (0-65535); Default: Any)

- **Dest. Port Filter** - Specifies the TCP destination filter for this rule. (Options: Any, Specific (0-65535), Range (0-65535); Default: Any)

- **TCP FIN** - Specifies the TCP "No more data from sender" (FIN) value for this rule. (Options: Any - any value is allowed, 0 - TCP frames where the FIN field is set must not match this entry, 1 - TCP frames where the FIN field is set must match this entry; Default: Any)

- **TCP SYN** - Specifies the TCP "Synchronize sequence numbers" (SYN) value for this rule. (Options: Any - any value is allowed, 0 - TCP frames where the SYN field is set must not match this entry, 1 - TCP frames where the SYN field is set must match this entry; Default: Any)

- **TCP RST** - Specifies the TCP "Reset the connection" (RST) value for this rule. (Options: Any - any value is allowed, 0 - TCP frames where the RST field is set must not match this entry, 1 - TCP frames where the RST field is set must match this entry; Default: Any)

- **TCP PSH** - Specifies the TCP "Push Function" (PSH) value for this rule. (Options: Any - any value is allowed, 0 - TCP frames where the PSH field is set must not match this entry, 1 - TCP frames where the PSH field is set must match this entry; Default: Any)

- **TCP ACK** - Specifies the TCP "Acknowledgment field significant" (ACK) value for this rule. (Options: Any - any value is allowed, 0 - TCP frames where the ACK field is set must not match this entry, 1 - TCP frames where the ACK field is set must match this entry; Default: Any)

- **TCP URG** - Specifies the TCP "Urgent Pointer field significant" (URG) value for this rule. (Options: Any - any value is allowed, 0 - TCP frames where the URG field is set must not match this entry, 1 - TCP frames where the URG field is set must match this entry; Default: Any)

- **IP TTL** - Specifies the time-to-Live settings for this rule. (Options: Any - any value is allowed, Non-zero - IPv4 frames with a TTL field greater than zero must match this entry, Zero - IPv4 frames with a TTL field greater than zero must not match this entry; Default: Any)

- **IP Fragment** - Specifies the fragment offset settings for this rule. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. (Options: Any - any value is allowed, Yes - IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must match this entry, No - IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not match this entry; Default: Any)

- **IP Option** - Specifies the options flag setting for this rule. (Options: Any - any value is allowed, Yes - IPv4 frames where the options flag is set must match this entry, No - IPv4 frames where the options flag is set must not match this entry; Default: Any)

- **SIP Filter** - Specifies the source IP filter for this rule. (Options: Any - no source IP filter is specified, Host - specifies the source IP address in the SIP Address field, Network - specifies the source IP address and source IP mask in the SIP Address and SIP Mask fields; Default: Any)

- **DIP Filter** - Specifies the destination IP filter for this rule. (Options: Any - no destination IP filter is specified, Host - specifies the destination IP address in the DIP Address field, Network - specifies the destination IP address and destination IP mask in the DIP Address and DIP Mask fields; Default: Any)

Response to take when a rule is matched

- **Action** - Permits or denies a frame based on whether it matches an ACL rule. (Default: Permit)

- **Rate Limiter** - Specifies a rate limiter (page 111) to apply to the port. (Range: 1-14; Default: Disabled)

- **Port Copy** - Defines a port to which matching frames are copied. (Range: 1-28; Default: Disabled)

- **Logging** - Enables logging of matching frames to the system log. (Default: Disabled)

  Open the System Log Information menu (page 137) to view any entries stored in the system log for this entry. Related entries will be displayed under the "Info" or "All" logging levels.

- **Shutdown** - Shuts down a port when a macthing frame is seen. (Default: Disabled)

- **Counter** - Shows he number of frames which have matched any of the rules defined for this ACL.

VLAN Parameters

- **VLAN ID Filter** - Specifies the VLAN to filter for this rule. (Options: Any, Specific (1-4095); Default: Any)

- **Tag Priority** - Specifies the User Priority value found in the VLAN tag (3 bits as defined by IEEE 802.1p) to match for this rule. (Options: Any, Specific (1-7); Default: Any)

WEB INTERFACE

To configure an Access Control List for a port or a policy:

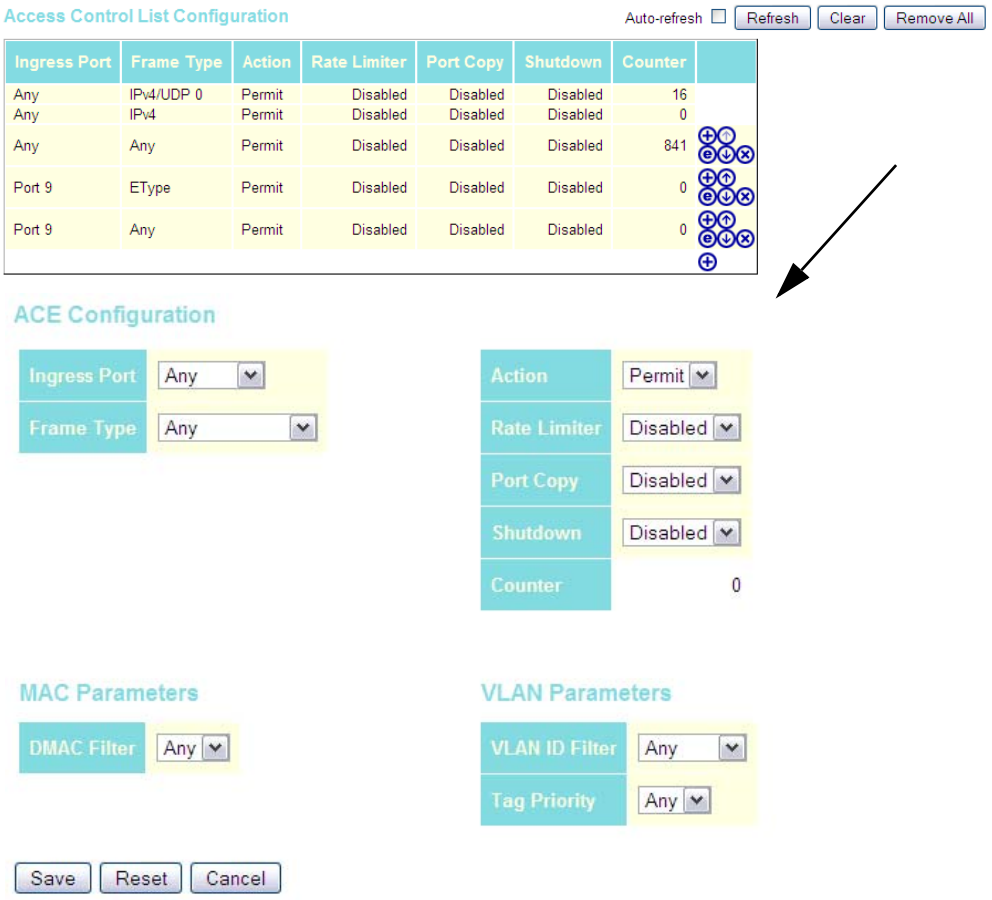
1. Click Configuration, ACL, Access Control List.

2. Click the  button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).

3. When editing an entry on the ACE Configuration page, note that the items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

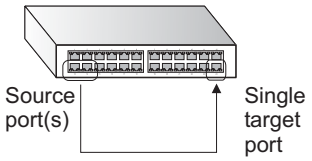
4. Click Save.

Figure 32: Access Control List Configuration



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.



PARAMETERS

The following parameters are displayed on the Mirror Configuration page:

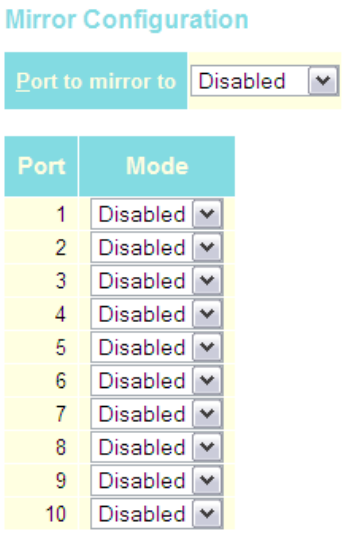
- **Port to mirror to** - The destination port that will mirror the traffic from the source port. All mirror sessions must share the same destination port. (Default: Disabled)
- **Port** - The port whose traffic will be monitored.
- **Mode** - Specifies which traffic to mirror to the target port. (Options: Disabled, Enabled (receive and transmit), Rx only (receive), Tx only (transmit); Default: Disabled)

WEB INTERFACE

To configure port mirroring:

1. Click Configuration, Mirroring. Then click Next.
2. Select the destination port to which all mirrored traffic will be sent.
3. Set the mirror mode on any of the source ports to be monitored.
4. Click Save.

Figure 33: Mirror Configuration



SIMPLE NETWORK MANAGEMENT PROTOCOL

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

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

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as HP OpenView. 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 12: SNMP Security Models and Levels

Model	Level	Community String	Group	Read View	Write View	Security
v1	noAuth NoPriv	public	default_ro_group	default_view	none	Community string only
v1	noAuth NoPriv	private	default_rw_group	default_view	default_view	Community string only
v1	noAuth NoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v2c	noAuth NoPriv	public	default_ro_group	default_view	none	Community string only
v2c	noAuth NoPriv	private	default_rw_group	default_view	default_view	Community string only
v2c	noAuth NoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v3	noAuth NoPriv	*user defined*	default_rw_group	default_view	default_view	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.

CONFIGURING SNMP SYSTEM AND TRAP SETTINGS

To manage the switch through SNMP, you must first enable the protocol and configure the basic access parameters. To issue trap messages, the trap function must also be enabled and the destination host specified.

PARAMETERS

The following parameters are displayed on the SNMP System Configuration page:

SNMP System Configuration

- **Mode** - Enables or disables SNMP service. (Default: Disabled)
- **Version** - Specifies the SNMP version to use. (Options: SNMP v1, SNMP v2c, SNMP v3; Default: SNMP v2c)
- **Read Community** - The community used for read-only access to the SNMP agent. (Range: 0-255 characters, ASCII characters 33-126 only; Default: public)

  This parameter only applies to SNMPv1 and SNMPv2c. SNMPv3 uses the User-based Security Model (USM) for authentication and privacy. This community string is associated with SNMPv1 or SNMPv2 clients in the SNMPv3 Communities table (page 126).
- **Write Community** - The community used for read/write access to the SNMP agent. (Range: 0-255 characters, ASCII characters 33-126 only; Default: private)

  This parameter only applies to SNMPv1 and SNMPv2c. SNMPv3 uses the User-based Security Model (USM) for authentication and privacy. This community string is associated with SNMPv1 or SNMPv2 clients in the SNMPv3 Communities table (page 126).
- **Engine ID** - The SNMPv3 engine ID. (Range: 10-64 hex digits, excluding a string of all 0's or all F's; Default: 800007e5017f000001)

  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 local SNMP users will be cleared. You will need to reconfigure all existing users.

SNMP Trap Configuration

- **Trap Mode** - Enables or disables SNMP traps. (Default: Disabled)

  You should enable SNMP traps so that key events are reported by this switch to your management station. Traps indicating status changes can be issued by the switch to the specified trap manager by sending authentication failure messages and other trap messages.

- **Trap Version** - Indicates if the target user is running SNMP v1, v2c, or v3. (Default: SNMP v1)

- **Trap Community** - Specifies the community access string to use when sending SNMP trap packets. (Range: 0-255 characters, ASCII characters 33-126 only; Default: public)

- **Trap Destination Address** - IPv4 address of the management station to receive notification messages.

- **Trap Destination IPv6 Address** - IPv6 address of the management station to receive notification messages. An IPv6 address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.

- **Trap Authentication Failure** - Issues a notification message to specified IP trap managers whenever authentication of an SNMP request fails. (Default: Enabled)

- **Trap Link-up and Link-down** - Issues a notification message whenever a port link is established or broken. (Default: Enabled)

- **Trap Inform Mode** - Enables or disables sending notifications as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)

  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.

- **Trap Inform Timeout** - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147 seconds; Default: 1 second)

- **Trap Inform Retry Times** - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 5)

- **Trap Probe Security Engine ID** (SNMPv3) - Specifies whether or not to use the engine ID of the SNMP trap probe in trap and inform messages. (Default: Enabled)

- **Trap Security Engine ID** (SNMPv3) - Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this

field is used. (Range: 10-64 hex digits, excluding a string of all 0's or all F's)

NOTE: The Trap Probe Security Engine ID must be disabled before an engine ID can be manually entered in this field.

- **Trap Security Name** (SNMPv3) - Indicates the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when SNMPv3 traps or informs are enabled.

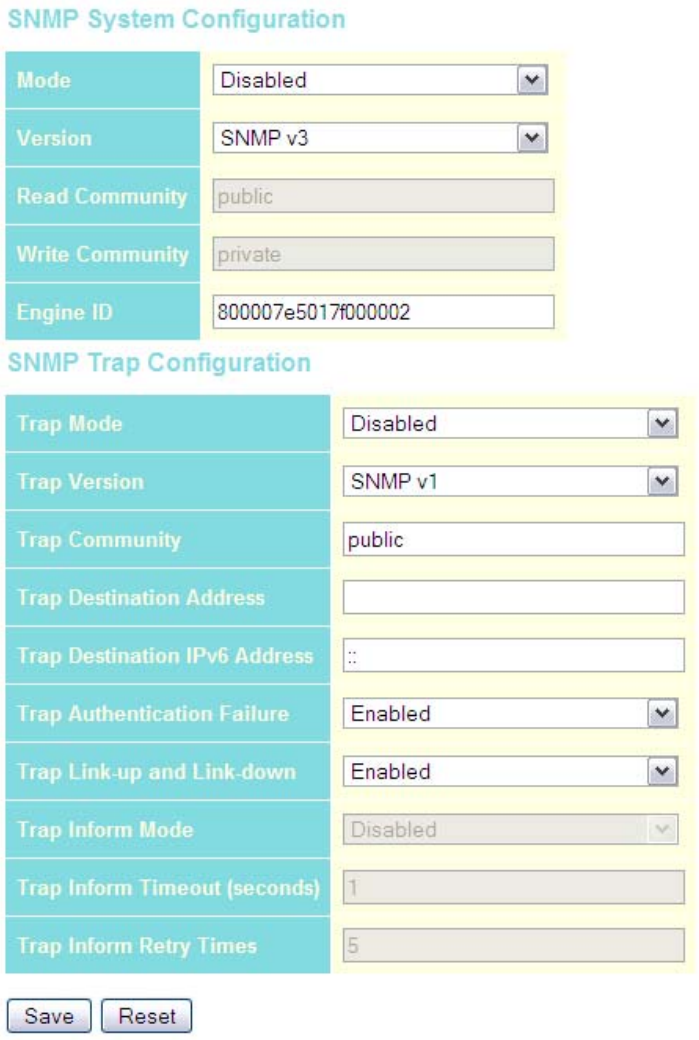
NOTE: To select a name from this field, first enter an SNMPv3 user with the same Trap Security Engine ID in the SNMPv3 Users Configuration menu (see "Configuring SNMPv3 Users" on page 127).

WEB INTERFACE

To configure SNMP system and trap settings:

1. Click Configuration, SNMP, System. Then click Next.
2. In the SNMP System Configuration table, set the Mode to Enabled to enable SNMP service on the switch, specify the SNMP version to use, change the community access strings if required, and set the engine ID if SNMP version 3 is used.
3. In the SNMP Trap Configuration table, enable the Trap Mode to allow the switch to send SNMP traps. Specify the trap version, trap community, and IP address of the management station that will receive trap messages either as an IPv4 or IPv6 address. Select the trap types to issue, and set the trap inform settings for SNMP v2c or v3 clients. For SNMP v3 clients, configure the security engine ID and security name used in v3 trap and inform messages.
4. Click Save.

Figure 34: SNMP System Configuration



SETTING SNMPV3 COMMUNITY ACCESS STRINGS

All community strings used to authorize access by SNMP v1 and v2c clients should be listed in the SNMPv3 Communities Configuration table. For security reasons, you should consider removing the default strings.

PARAMETERS

The following parameters are displayed on the SNMPv3 Communities Configuration page:

- **Community** - Specifies the community strings which allow access to the SNMP agent. (Range: 1-32 characters, ASCII characters 33-126 only; Default: public, private)

  For SNMPv3, these strings are treated as a Security Name, and are mapped as an SNMPv1 or SNMPv2 community string in the SNMPv3 Groups Configuration table (see "Configuring SNMPv3 Groups" on page 129).

- **Source IP** - Specifies the source address of an SNMP client.
- **Source Mask** - Specifies the address mask for the SNMP client.

WEB INTERFACE

To configure SNMP community access strings:

1. Click Configuration, SNMP, Communities.
2. Set the IP address and mask for the default community strings. Otherwise, you should consider deleting these strings for security reasons.
3. Add any new community strings required for SNMPv1 or v2 clients that need to access the switch, along with the source address and address mask for each client.
4. Click Save.

Figure 35: SNMPv3 Communities Configuration

CONFIGURING SNMPV3 USERS

Each SNMPv3 user is defined by a unique name and remote engine ID. Users must be configured with a specific security level, and the types of authentication and privacy protocols to use.

NOTE: Any user assigned through this page is associated with the group assigned to the USM Security Model on the SNMPv3 Groups Configuration page (page 129), and the views assigned to that group in the SNMPv3 Access Configuration page (page 131).

PARAMETERS

The following parameters are displayed on the SNMPv3 Users Configuration page:

- **Engine ID** - The engine identifier for the SNMP agent on the remote device where the user resides. (Range: 10-64 hex digits, excluding a string of all 0's or all F's)

  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 "Configuring SNMP System and Trap Settings" on page 123.)

- **User Name** - The name of user connecting to the SNMP agent. (Range: 1-32 characters, ASCII characters 33-126 only)

- **Security Level** - The security level assigned to the user:
  - **NoAuth, NoPriv** - There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
  - **Auth, NoPriv** - SNMP communications use authentication, but the data is not encrypted.
  - **Auth, Priv** - SNMP communications use both authentication and encryption.

- **Authentication Protocol** - The method used for user authentication. (Options: None, MD5, SHA; Default: MD5)

- **Authentication Password** - A plain text string identifying the authentication pass phrase. (Range: 1-32 characters for MD5, 8-40 characters for SHA)

- **Privacy Protocol** - The encryption algorithm use for data privacy; only 56-bit DES is currently available. (Options: None, DES; Default: DES)

- **Privacy Password** - A string identifying the privacy pass phrase. (Range: 8-40 characters, ASCII characters 33-126 only)

WEB INTERFACE

To configure SNMPv3 users:

1. Click Configuration, SNMP, Users.
2. Click Add New User to configure a user name.
3. Enter a remote Engine ID of up to 64 hexadecimal characters
4. Define the user name, security level, authentication and privacy settings.
5. Click Save.

Figure 36: SNMPv3 Users Configuration

CONFIGURING SNMPV3 GROUPS

An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read and write views as defined on the SNMPv3 Access Configuration page (page 131). You can use the pre-defined default groups, or create a new group and the views authorized for that group.

PARAMETERS

The following parameters are displayed on the SNMPv3 Groups Configuration page:

- **Security Model** - The user security model. (Options: SNMP v1, v2c, or the User-based Security Model – usm).
- **Security Name** - The name of user connecting to the SNMP agent. (Range: 1-32 characters, ASCII characters 33-126 only)

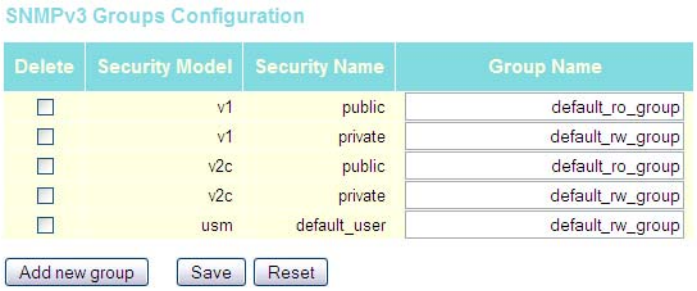
  The options displayed for this parameter depend on the selected Security Model. For SNMP v1 and v2c, the switch displays the names configured on the SNMPv3 Communities Configuration menu (see page 126). For USM (or SNMPv3), the switch displays the names configured with the local engine ID in the SNMPv3 Users Configuration menu (see page 127). To modify an entry for USM, the current entry must first be deleted.
- **Group Name** - The name of the SNMP group. (Range: 1-32 characters, ASCII characters 33-126 only)

WEB INTERFACE

To configure SNMPv3 groups:

1. Click Configuration, SNMP, Groups.
2. Click Add New Group to set up a new group.
3. Select a security model.
4. Select the security name. For SNMP v1 and v2c, the security names displayed are based on the those configured in the SNMPv3 Communities menu. For USM, the security names displayed are based on the those configured in the SNMPv3 Users Configuration menu.
5. Enter a group name. Note that the views assigned to a group must be specified on the SNMP Accesses Configuration menu (see page 131).
6. Click Save.

Figure 37: SNMPv3 Group Configuration



CONFIGURING SNMPV3 VIEWS

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

PARAMETERS

The following parameters are displayed on the SNMPv3 Views Configuration page:

- **View Name** - The name of the SNMP view. (Range: 1-32 characters, ASCII characters 33-126 only)
- **View Type** - Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view. Generally, if the view type of an entry is "excluded," another entry of view type "included" should exist and its OID subtree should overlap the "excluded" view entry.
- **OID Subtree** - Object identifiers of branches within the MIB tree. Note that the first character must be a period (.). Wild cards can be used to

mask a specific portion of the OID string using an asterisk. (Length: 1-128)

WEB INTERFACE

To configure SNMPv3 views:

1. Click Configuration, SNMP, Views.
2. Click Add New View to set up a new view.
3. Enter the view name, view type, and OID subtree.
4. Click Save.

Figure 38: SNMPv3 View Configuration

CONFIGURING SNMPV3 GROUP ACCESS RIGHTS

Use the SNMP Accesses Configuration menu to assign portions of the MIB tree to which each SNMPv3 group is granted access. You can assign more than one view to a group to specify access to different portions of the MIB tree.

PARAMETERS

The following parameters are displayed on the SNMPv3 Access Configuration page:

- **Group Name** - The name of the SNMP group. (Range: 1-32 characters, ASCII characters 33-126 only)
- **Security Model** - The user security model. (Options: any, v1, v2c, or the User-based Security Model – usm; Default: any)
- **Security Level** - The security level assigned to the group:
  - **NoAuth, NoPriv** - There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
  - **Auth, NoPriv** - SNMP communications use authentication, but the data is not encrypted.
  - **Auth, Priv** - SNMP communications use both authentication and encryption.
- **Read View Name** - The configured view for read access. (Range: 1-32 characters, ASCII characters 33-126 only)

- **Write View Name** - The configured view for write access. (Range: 1-32 characters, ASCII characters 33-126 only)

WEB INTERFACE

To configure SNMPv3 group access rights:

1. Click Configuration, SNMP, Accesses.
2. Click Add New Access to create a new entry.
3. Specify the group name, security settings, read view, and write view.
4. Click Save.

Figure 39: SNMPv3 Access Configuration

CONFIGURING UPNP

Universal Plug and Play (UPnP) is a set of protocols that allows devices to connect seamlessly and simplifies the deployment of home and office networks. UPnP achieves this by issuing UPnP device control protocols designed upon open, Internet-based communication standards.

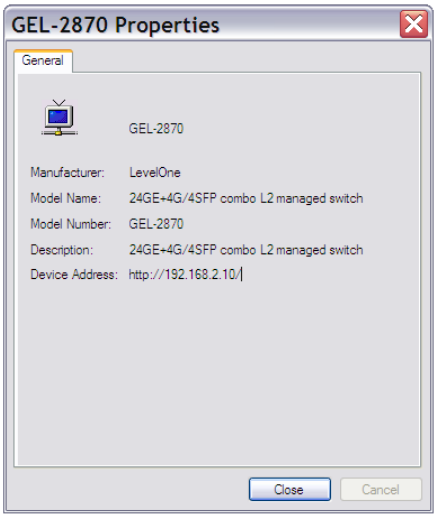
The first step in UPnP networking is discovery. When a device is added to the network, the UPnP discovery protocol allows that device to broadcast its services to control points on the network. Similarly, when a control point is added to the network, the UPnP discovery protocol allows that control point to search for UPnP enabled devices on the network.

Once a control point has discovered a device its next step is to learn more about the device and its capabilities by retrieving 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, it can send actions to the 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).

When a device is known to the control point, periodic event notification messages are sent. 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.

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.

Using UPnP under Windows XP - To access or manage the switch with the aid of UPnP under Windows XP, open My Network Places in the Explore file manager. An entry for "GEL-2870" will appear in the list of discovered devices. Double-click on this entry to access the switch's web management interface. Or right-click on the entry and select "Properties" to display a list of device attributes advertised through UPnP.



PARAMETERS

The following parameters are displayed on the UPnP Configuration page:

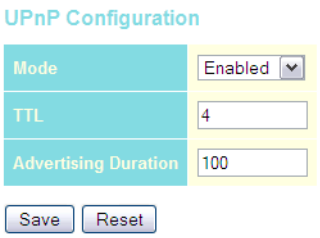
- **Mode** - Enables/disables UPnP on the device. (Default: Disabled)
- **TTL** - Sets the time-to-live (TTL) value for UPnP messages transmitted by the switch. (Range: 4-255; Default: 4)
- **Advertising Duration** - The duration, carried in Simple Service Discover Protocol (SSDP) packets, which informs a control point or control points how often it or they should receive a SSDP advertisement message from this switch. Due to the unreliable nature of UDP, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. (Range: 100-86400 seconds; Default: 100 seconds)

WEB INTERFACE

To configure UPnP:

1. Click Configuration, UPnP.
2. Enable or disable UPnP, then set the TTL and advertisement values.
3. Click Save.

Figure 40: UPnP Configuration



CONFIGURING DHCP RELAY AND OPTION 82 INFORMATION

The switch supports DHCP relay service for attached host devices. If a subnet does not include a DHCP server, you can relay DHCP client requests to a DHCP server on another subnet.

When DHCP relay is enabled and the switch sees a DHCP request broadcast, it inserts its own IP address into the request (so that the DHCP server knows the subnet of the client), then forwards the packet to the DHCP server. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the switch. The switch then broadcasts the DHCP response to the client.

DHCP also provides a 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.

Using DHCP Relay Option 82, clients can be identified by the VLAN and 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 drop packets that already contain Option 82 information, keep the existing information, or replace it with the switch's relay information.

PARAMETERS

The following parameters are displayed on the DHCP Relay Configuration page:

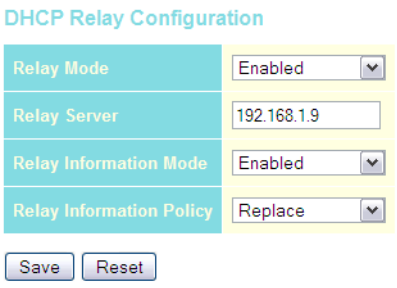
- **Relay Mode** - Enables or disables the DHCP relay function. (Default: Disabled)
- **Relay Server** - IP address of DHCP server to be used by the switch's DHCP relay agent.
- **Relay Information Mode** - Enables or disables the DHCP Relay Option 82 support. Note that Relay Mode must also be enabled for Relay Information Mode to take effect. (Default: Disabled)
- **Relay Information Policy** - Sets the DHCP relay policy for DHCP client packets that include Option 82 information.
  - **Replace** - Overwrites the DHCP client packet information with the switch's relay information. (This is the default.)
  - **Keep** - Retains the client's DHCP information.
  - **Drop** - Drops the packet when it receives a DHCP message that already contains relay information.

WEB INTERFACE

To configure DHCP Relay:

1. Click Configuration, DHCP, Relay.
2. Enable the DHCP relay function, specify the DHCP server's IP address, enable Option 82 information mode, and set the policy by which to handle relay information found in client packets.
3. Click Save.

Figure 41: DHCP Relay Configuration



5 MONITORING THE SWITCH

This chapter describes how to monitor all of the basic functions, configure or view system logs, and how to view traffic status or the address table.

DISPLAYING BASIC INFORMATION ABOUT THE SYSTEM

You can use the Monitor/System menu to display a basic description of the switch, log messages, or statistics on traffic used in managing the switch.

DISPLAYING SYSTEM INFORMATION

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

PARAMETERS

These parameters are displayed on the System Information page:

System - To configure the following items see "Configuring System Information" on page 50.

- **Contact** – Administrator responsible for the system.
- **Name** – Name assigned to the switch system.
- **Location** – Specifies the system location.

Hardware

- **MAC Address** – The physical layer address for this switch.

Time

- **System Date** – The current system time and date. The time is obtained through an SNTP Server if configured (see "Setting an IP Address" on page 51).
- **System Uptime** – Length of time the management agent has been up.

Software

- **Software Version** – Version number of runtime code.
- **Software Date** – Release date of the switch software.

WEB INTERFACE

To view System Information in the web interface, click Monitor, System, Information.

Figure 42: System Information

System Information

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-01-c1-00-00-e1
Time	
System Date	1970-01-01 06:37:57 +0000
System Uptime	0d 06:37:57
Software	
Software Version	GEL-2870 Managed (standalone) v1.0.1
Software Date	2009-10-26 14:21:26 +0800

DISPLAYING LOG MESSAGES

Use the System Log Information page to scroll through the logged system and event messages.

PARAMETERS

These parameters are displayed on the System Log Information page:

Display Filter

- **Level** – Specifies the type of log messages to display.
  - Info – Informational messages only.
  - Warning – Warning conditions.
  - Error – Error conditions.
  - All – All levels.
- Start from ID – The error ID from which to start the display.
- with # entries per page – The number of entries to display per page.

Table Headings

- **ID** – Error ID.
- **Level** – Error level as described above.
- **Time** – The time of the system log entry.
- **Message** – The message text of the system log entry.

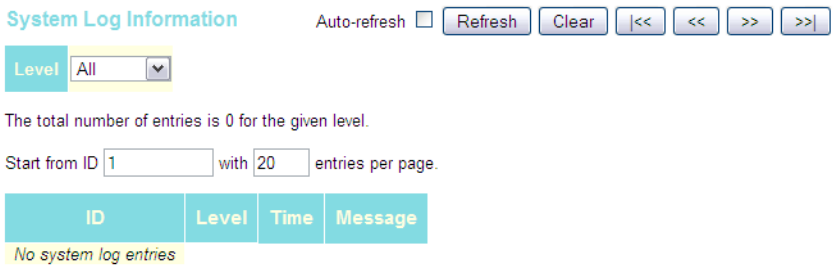
WEB INTERFACE

To display the system log:

1. Click Monitor, System, Log.
2. Specify the message level to display, the starting message ID, and the number of messages to display per page.
3. Use Auto-refresh to automatically refresh the page at regular intervals, Refresh to update system log entries starting from the current entry ID, or Clear to flush all system log entries.

   Use the arrow buttons to scroll through the log messages. |<< updates the system log entries, starting from the first available entry ID, << updates the system log entries, ending at the last entry currently displayed, >> updates the system log entries, starting from the last entry currently displayed, and >>| updates the system log entries, ending at the last available entry ID.

Figure 43: System Log Information



DISPLAYING LOG DETAILS

Use the Detailed Log page to view the full text of specific log messages.

WEB INTERFACE

To display the text of a specific log message, click Monitor, System, Detailed Log.

Figure 44: Detailed System Log Information

DISPLAYING ACCESS MANAGEMENT STATISTICS

Use the Access Management Statistics page to view statistics on traffic used in managing the switch.

USAGE GUIDELINES

Statistics will only be displayed on this page if access management is enabled on the Access Management Configuration menu (see page 56), and traffic matching one of the entries is detected.

PARAMETERS

These parameters are displayed on the Access Management Statistics page:

- **Interface** – Network protocols used to manage the switch. (Protocols: HTTP, HTTPS, SNMP, TELNET, SSH)
- **Receive Packets** – The number of management packets received.
- **Allow Packets** – The number of management packets accepted.
- **Discard Packets** – The number of management packets discarded.

WEB INTERFACE

To display the information on management packets, click Monitor, System, Access Management Statistics.

Figure 45: Access Management Statistics

Access Management Statistics

Auto-refresh ☐ Refresh Clear

Interface	Receive Packets	Allow Packets	Discard Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

DISPLAYING INFORMATION ABOUT PORTS

You can use the Monitor/Port menu to display a graphic image of the front panel which indicates the connection status of each port, basic statistics on the traffic crossing each port, the number of packets processed by each service queue, or detailed statistics on port traffic.

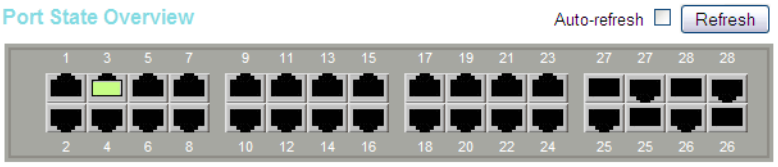
DISPLAYING PORT STATUS ON THE FRONT PANEL

Use the Port State Overview page to display an image of the switch's ports. Clicking on the image of a port opens the Detailed Port Statistics page as described on page 142.

WEB INTERFACE

To display an image of the switch's ports, click Monitor, Ports, State.

Figure 46: Port State Overview



DISPLAYING AN OVERVIEW OF PORT STATISTICS

Use the Port Statistics Overview page to display a summary of basic information on the traffic crossing each port.

PARAMETERS

These parameters are displayed on the Port Statistics Overview page:

- **Packets Receive/Transmit** – The number of packets received and transmitted.
- **Bytes Receive/Transmit** – The number of bytes received and transmitted.
- **Errors Receive/Transmit** – The number of frames received with errors and the number of incomplete transmissions.
- **Drops Receive/Transmit** – The number of frames discarded due to ingress or egress congestion
- **Filtered Receive** – The number of received frames filtered by the forwarding process.

WEB INTERFACE

To display a summary of port statistics, click Monitor, Ports, Traffic Overview.

Figure 47: Port Statistics Overview

Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	97	606	35037	96358	8	0	8	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0

DISPLAYING QOS STATISTICS

Use the QoS Statistics page to display the number of packets processed by each service queue.

PARAMETERS

These parameters are displayed on the Queuing Counters page:

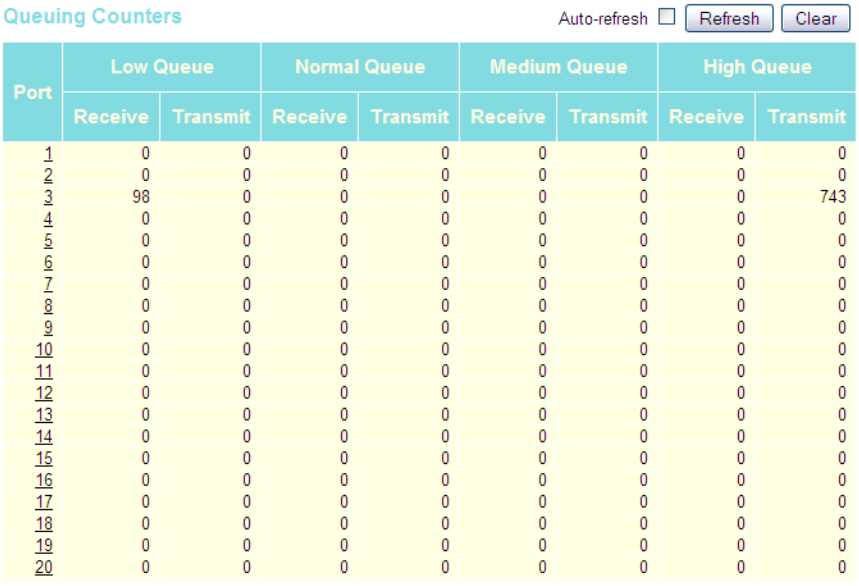
- **Low Queue Receive/Transmit** – The number of packets received and transmitted through the low-priority queue.

- **Normal Queue Receive/Transmit** – The number of packets received and transmitted through the normal-priority queue.
- **Medium Queue Receive/Transmit** – The number of packets received and transmitted through the medium-priority queue.
- **High Queue Receive/Transmit** – The number of packets received and transmitted through the high-priority queue.

WEB INTERFACE

To display the queue counters, click Monitor, Ports, QoS Statistics.

Figure 48: Queuing Counters



Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	98	0	0	0	0	0	0	743
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0

DISPLAYING DETAILED PORT STATISTICS

Use the Detailed Port Statistics page to display detailed statistics on network traffic. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading).

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.

PARAMETERS

These parameters are displayed on the Detailed Port Statistics page:

- **Receive/Transmit Total**
  - **Packets** – The number of received and transmitted packets (good and bad).
  - **Octets** – The number of received and transmitted bytes (good and bad), including Frame Check Sequence, but excluding framing bits.

- **Unicast** – The number of received and transmitted unicast packets (good and bad).
- **Multicast** – The number of received and transmitted multicast packets (good and bad).
- **Broadcast** – The number of received and transmitted broadcast packets (good and bad).
- **Pause** – A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

- **Receive/Transmit Size Counters** - The number of received and transmitted packets (good and bad) split into categories based on their respective frame sizes.

- **Receive/Transmit Queue Counters** - The number of received and transmitted packets per input and output queue.

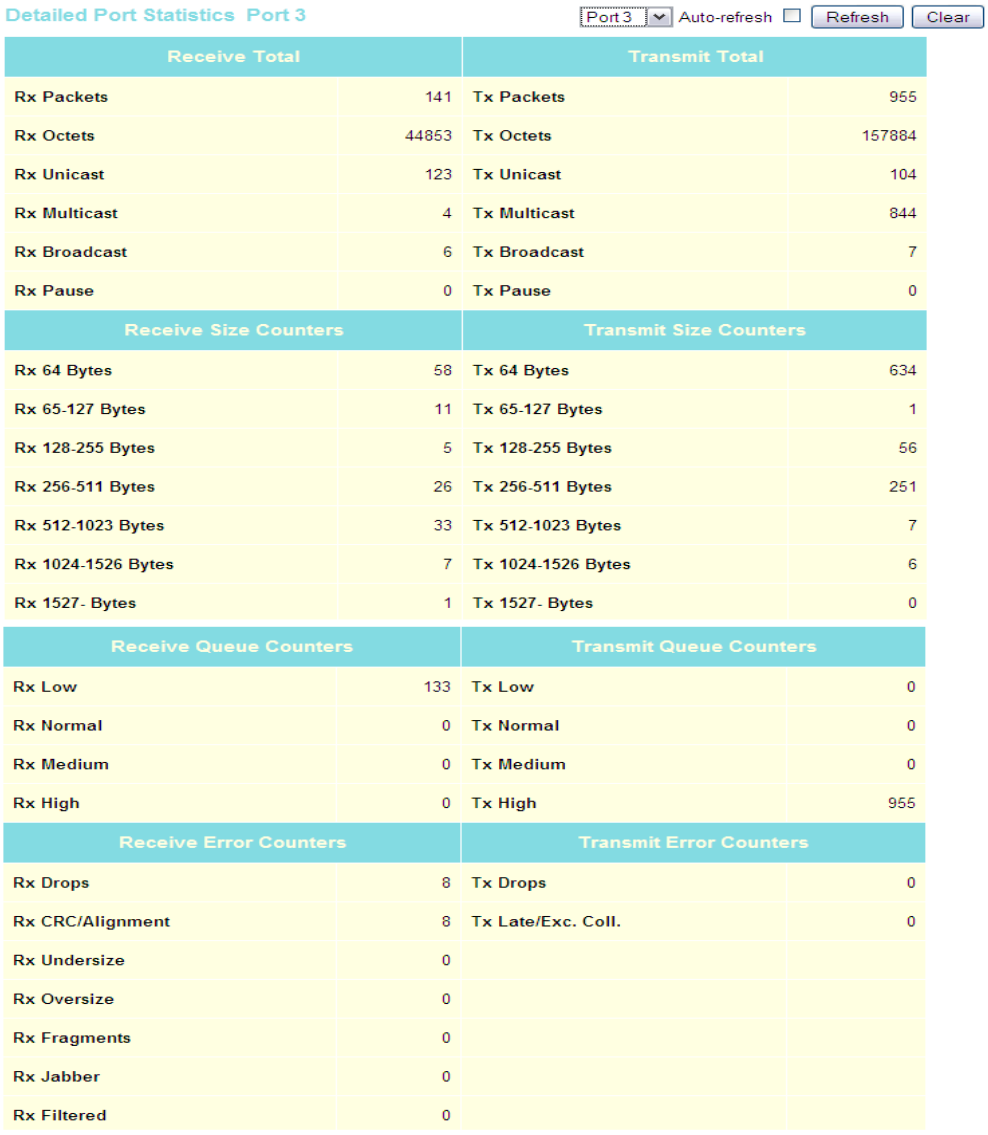
- **Receive Error Counters**
  - **Rx Drops** - The number of inbound packets which were discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
  - **Rx CRC/Alignment** - The number of frames received with CRC or alignment errors.
  - **Rx Undersize** - 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.
  - **Rx Oversize** - The total number of frames received that were longer than the configured maximum frame length for this port (excluding framing bits, but including FCS octets) and were otherwise well formed.
  - **Rx 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.
  - **Rx Jabber** - The total number of frames received that were longer than the configured maximum frame length for this port (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
  - **Rx Filtered** - The number of received frames filtered by the forwarding process.

- **Transmit Error Counters**
  - **Tx Drops** – The number of frames dropped due to output buffer congestion.
  - **Tx Late/Exc. Coll.** – The number of frames dropped due to late or excessive collisions.

WEB INTERFACE

To display the detailed port statistics, click Monitor, Ports, Detailed Statistics.

Figure 49: Detailed Port Statistics



Receive Total		Transmit Total	
Rx Packets	141	Tx Packets	955
Rx Octets	44853	Tx Octets	157884
Rx Unicast	123	Tx Unicast	104
Rx Multicast	4	Tx Multicast	844
Rx Broadcast	6	Tx Broadcast	7
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	58	Tx 64 Bytes	634
Rx 65-127 Bytes	11	Tx 65-127 Bytes	1
Rx 128-255 Bytes	5	Tx 128-255 Bytes	56
Rx 256-511 Bytes	26	Tx 256-511 Bytes	251
Rx 512-1023 Bytes	33	Tx 512-1023 Bytes	7
Rx 1024-1526 Bytes	7	Tx 1024-1526 Bytes	6
Rx 1527- Bytes	1	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Low	133	Tx Low	0
Rx Normal	0	Tx Normal	0
Rx Medium	0	Tx Medium	0
Rx High	0	Tx High	955
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	8	Tx Drops	0
Rx CRC/Alignment	8	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

DISPLAYING INFORMATION ON AUTHENTICATION SERVERS

Use the Monitor/Authentication pages to display information on RADIUS authentication and accounting servers, including the IP address and statistics for each server.

DISPLAYING A LIST OF AUTHENTICATION SERVERS

Use the RADIUS Overview page to display a list of configured authentication and accounting servers.

PARAMETERS

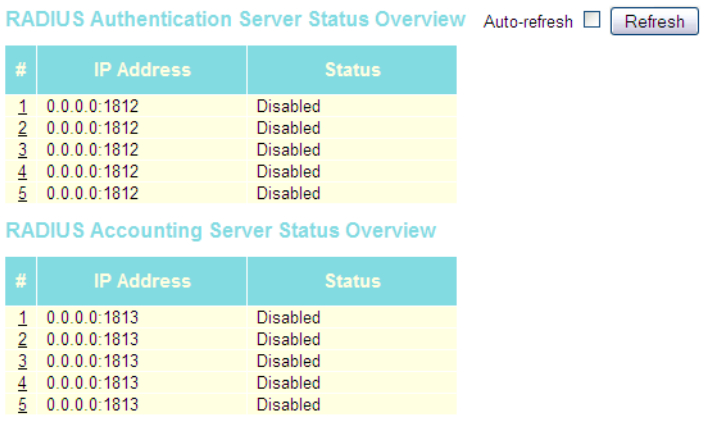
These parameters are displayed on the RADIUS Overview page:

- **IP Address** - The IP address and UDP port number of this server.
- **Status** - The current state of the server. This field takes one of the following values:
  - **Disabled** - The server is disabled.
  - **Not Ready** - The server is enabled, but IP communication is not yet up and running.
  - **Ready** - The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
  - **Dead** (X seconds left) - Access attempts were made to this server, but it did not reply within the configured timeout. The server has been temporarily disabled, but will be re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses.

WEB INTERFACE

To display a list of configured authentication and accounting servers, click Monitor, Authentication, RADIUS Overview.

Figure 50: RADIUS Overview



DISPLAYING STATISTICS FOR CONFIGURED AUTHENTICATION SERVERS

Use the RADIUS Details page to display statistics for configured authentication and accounting servers. The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

PARAMETERS

These parameters are displayed on the RADIUS Details page:

RADIUS Authentication Statistics

- **Receive Packets**
  - **Access Accepts** - The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
  - **Access Rejects** - The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
  - **Access Challenges** - The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
  - **Malformed Access Responses** - The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
  - **Bad Authenticators** - The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from this server.
  - **Unknown Types** - The number of RADIUS packets of unknown type that were received from this server on the authentication port.
  - **Packets Dropped** - The number of RADIUS packets that were received from this server on the authentication port and dropped for some other reason.
- **Transmit Packets**
  - **Access Requests** - The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
  - **Access Retransmissions** - The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
  - **Pending Requests** - The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

- **Timeouts** - The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

◆ **Other Info**

- **State** - The current state of the server. This field takes one of the following values:
  - **Disabled** - The server is disabled.
  - **Not Ready** - The server is enabled, but IP communication is not yet up and running.
  - **Ready** - The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
  - **Dead** (X seconds left) - Access attempts were made to this server, but it did not reply within the configured timeout. The server has been temporarily disabled, but will be re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses.
- **Round-Trip Time** - The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics

◆ **Receive Packets**

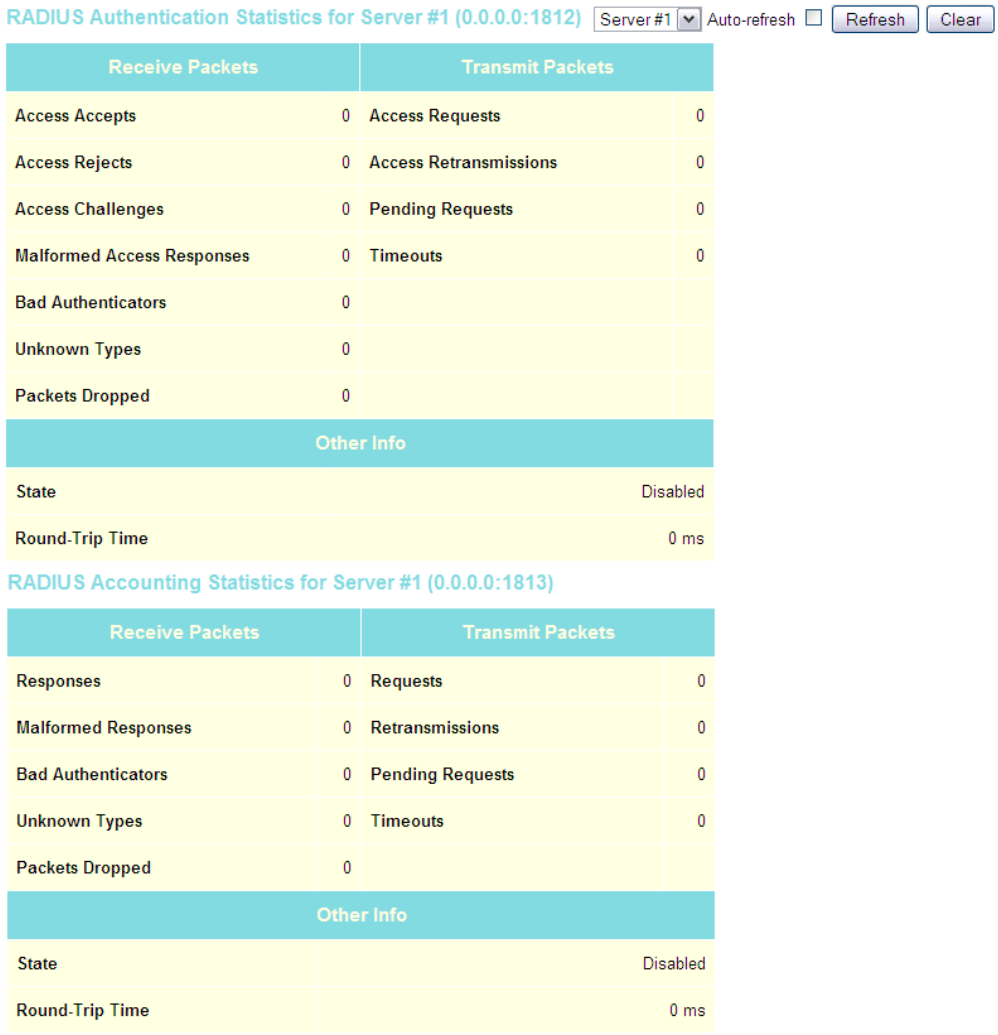
- **Responses** - The number of RADIUS packets (valid or invalid) received from the server.
- **Malformed Responses** - The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
- **Bad Authenticators** - The number of RADIUS packets containing invalid authenticators received from the server.
- **Unknown Types** - The number of RADIUS packets of unknown types that were received from the server on the accounting port.
- **Packets Dropped** - The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

- **Transmit Packets**
  - **Requests** - The number of RADIUS packets sent to the server. This does not include retransmissions.
  - **Retransmissions** - The number of RADIUS packets retransmitted to the RADIUS accounting server.
  - **Pending Requests** - The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
  - **Timeouts** - The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
- **Other Info**
  - **State** - The current state of the server. It takes one of the following values:
    - **Disabled** - The server is disabled.
    - **Not Ready** - The server is enabled, but IP communication is not yet up and running.
    - **Ready** - The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
    - **Dead** (X seconds left) - Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
  - **Round-Trip Time** - The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

WEB INTERFACE

To display statistics for configured authentication and accounting servers, click Monitor, Authentication, RADIUS Details.

Figure 51: RADIUS Details



DISPLAYING INFORMATION ON LACP

Use the monitor pages for LACP to display information on LACP configuration settings, the functional status of participating ports, and statistics on LACP control packets.

DISPLAYING AN OVERVIEW OF LACP GROUPS

Use the LACP System Status page to display an overview of LACP groups.

PARAMETERS

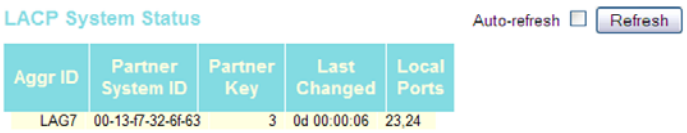
These parameters are displayed on the LACP System Status page:

- **Aggr ID** - The Aggregation ID associated with this Link Aggregation Group (LAG).
- **Partner System ID** - LAG partner's system ID (MAC address).
- **Partner Key** - The Key that the partner has assigned to this LAG.
- **Last Changed** - The time since this LAG changed.
- **Local Ports** - Shows the local ports that are a part of this LAG.

WEB INTERFACE

To display an overview of LACP groups active on this switch, click Monitor, LACP, System Status.

Figure 52: LACP System Status



DISPLAYING LACP PORT STATUS

Use the LACP Port Status page to display information on the LACP groups active on each port.

PARAMETERS

These parameters are displayed on the LACP Port Status page:

- **Port** - Port Identifier.
- **LACP** - Shows LACP status:
  - **Yes** - LACP is enabled and the port link is up.
  - **No** - LACP is not enabled or the port link is down.

- **Backup** - The port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

- **Key** - Current operational value of the key for the aggregation port. Note that only ports with the same key can aggregate together.
- **Aggr ID** - The Aggregation ID assigned to this LAG.
- **Partner System ID** - LAG partner's system ID assigned by the LACP protocol (i.e., its MAC address).
- **Partner Port** - The partner port connected to this local port.

WEB INTERFACE

To display LACP status for local ports this switch, click Monitor, LACP, Port Status.

Figure 53: LACP Port Status

LACP Status

Auto-refresh ☐ Refresh

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	Yes	3	LLAG7	00-13-f7-32-6f-63	18
19	Yes	3	LLAG7	00-13-f7-32-6f-63	19
20	No	-	-	-	-

DISPLAYING LACP PORT STATISTICS

Use the LACP Port Statistics page to display statistics on LACP control packets crossing on each port.

PARAMETERS

These parameters are displayed on the LACP Port Statistics page:

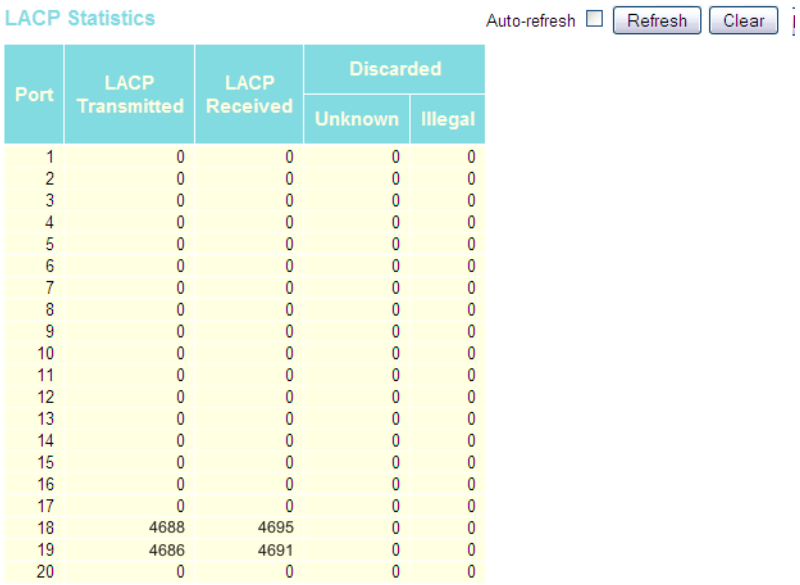
- **Port** - Port Identifier.
- **LACP Transmitted** - The number of LACP frames sent from each port.
- **LACP Received** - The number of LACP frames received at each port.

- **Discarded** - The number of unknown or illegal LACP frames that have been discarded at each port.

WEB INTERFACE

To display LACP statistics for local ports this switch, click Monitor, LACP, Port Statistics.

Figure 54: LACP Port Statistics



Port	LACP Transmitted	LACP Received	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	4688	4695	0	0
19	4686	4691	0	0
20	0	0	0	0

DISPLAYING INFORMATION ON THE SPANNING TREE

Use the monitor pages for Spanning Tree to display information on spanning tree bridge status, the functional status of participating ports, and statistics on spanning tree protocol packets.

DISPLAYING BRIDGE STATUS FOR STA

Use the Bridge Status page to display RSTP information on the global bridge (i.e., this switch) and individual ports.

PARAMETERS

These parameters are displayed on the Spanning Tree Bridge Status page:

RSTP Bridge Status

- **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).

- **Root ID** - 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 Cost** - The path cost from the root port on this switch to the root device. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.

- **Topology Flag** - The current state of the Topology Change Notification flag (TCN) for this bridge instance.

- **Topology Change Count** - The number of times the Spanning Tree has been reconfigured (during a one-second interval).

- **Topology Change Last** - Time since the Spanning Tree was last reconfigured.

Physical Ports & Aggregations State

- **Port** - Port Identifier.

- **Port ID** - The port identifier as used by the RSTP protocol. This consists of the priority part and the logical port index of the bridge 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.

- **State** - Displays the current state of this port within the Spanning Tree:
  - **Blocking** - 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.

- **Path Cost** - The contribution of this port to the path cost of paths towards the spanning tree root which include this port. This will either be a value computed from the Auto setting, or any explicitly configured value.

- **Edge** - The current RSTP port (operational) Edge Flag. An Edge Port is a switch port to which no bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transitions directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

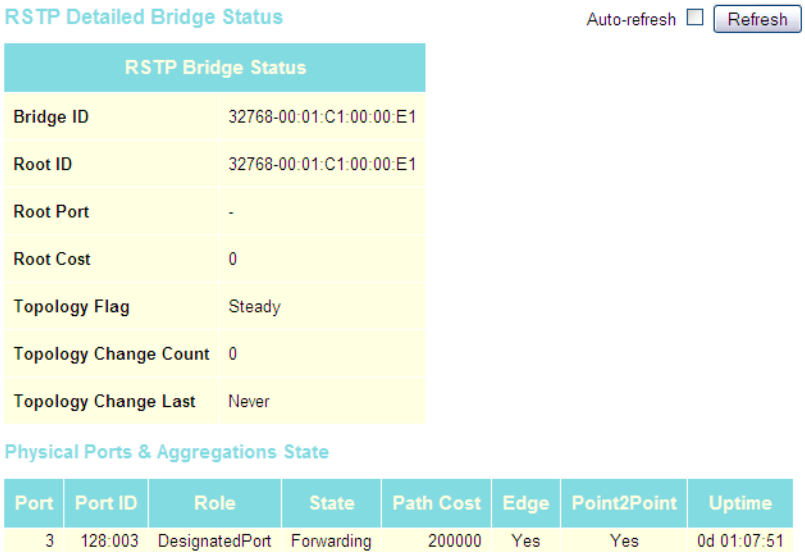
- **Point2Point** - Indicates a connection to exactly one other bridge. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transition RSTP states.

- **Uptime** - The time since the bridge port was last initialized.

WEB INTERFACE

To display information on spanning tree bridge and port status, click Monitor, Spanning Tree, Bridge Status.

Figure 55: Spanning Tree Bridge Status



DISPLAYING PORT STATUS FOR STA

Use the Port Status page to display the RSTP functional status of participating ports.

PARAMETERS

These parameters are displayed on the RSTP Port Status page:

- **Port** - Port Identifier.

- **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.

- **State** - Displays current state of this port within the Spanning Tree:
  - **Blocking** - Port receives STA configuration messages, but does not forward packets.

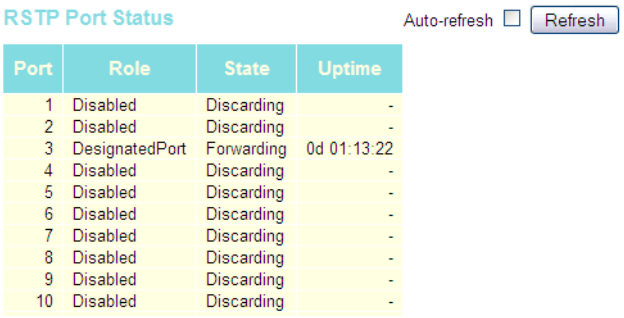
- **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
- **Forwarding** - Port forwards packets, and continues learning addresses.

- **Uptime** - The time since the bridge port was last initialized.

WEB INTERFACE

To display information on spanning tree port status, click Monitor, Spanning Tree, Port Status.

Figure 56: Spanning Tree Port Status



Port	Role	State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	DesignatedPort	Forwarding	0d 01:13:22
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-

DISPLAYING PORT STATISTICS FOR STA

Use the Port Statistics page to display statistics on spanning tree protocol packets crossing each port.

packets crossing each port.

PARAMETERS

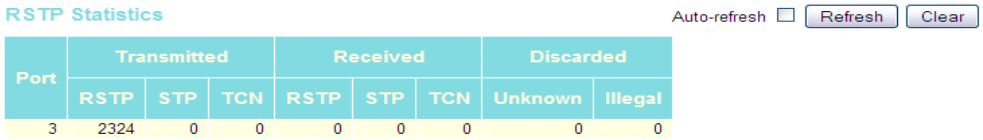
These parameters are displayed on the RSTP Port Statistics page:

- **Port** - Port Identifier.
- **RSTP** - The number of RSTP Configuration BPDU's received/transmitted on a port.
- **STP** - The number of legacy STP Configuration BPDU's received/ transmitted on a port.
- **TCN** - The number of (legacy) Topology Change Notification BPDU's received/transmitted on a port.
- **Discarded Unknown** - The number of unknown Spanning Tree BPDU's received (and discarded) on a port.
- **Discarded Illegal** - The number of illegal Spanning Tree BPDU's received (and discarded) on a port.

WEB INTERFACE

To display information on spanning port statistics, click Monitor, Spanning Tree, Port Statistics.

Figure 57: Spanning Tree Port Statistics



DISPLAYING PORT SECURITY INFORMATION

Use the monitor pages for Port Security to display the IEEE 802.1X authentication state, statistics, and protocol information for each port.

DISPLAYING PORT SECURITY STATUS

Use the Port Security Status page to display the authentication state and related information for each port.

PARAMETERS

These parameters are displayed on the Port Security Status page:

- **Port** - Port Identifier.
- **State** - The current state of the port:
  - **Disabled** - 802.1X and MAC-based authentication are globally disabled.
  - **Link Down** - 802.1X or MAC-based authentication is enabled, but there is no link on the port.
  - **Authorized** - The port is authorized. This state exists when 802.1X authentication is enabled, the port has a link, the Admin State is "802.1X," and the supplicant is authenticated, or when the Admin State is "Authorized."
  - **Unauthorized** - The port is unauthorized. This state exists when 802.1X authentication is enabled, the port has a link, and the Admin State is "Auto," but the supplicant is not (or not yet) authenticated, or when the Admin State is "Unauthorized."
  - X **Auth**/Y **Unauth** - X clients are currently authorized and Y are unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to "MAC-Based."
- **Last Source** - The source MAC address carried in the most recently received EAPOL frame for port-based authentication, and the most

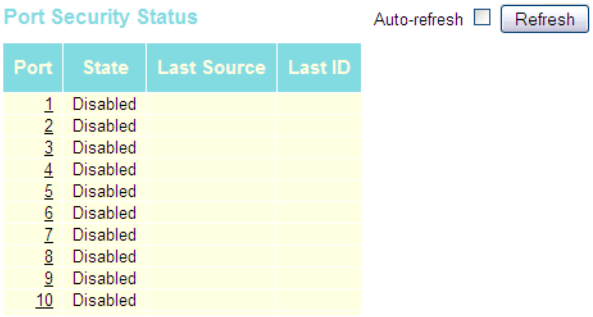
recently received frame from a new client for MAC-based authentication.

- **Last ID** - The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame for port-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

WEB INTERFACE

To display the authentication state and related information for each port, click Monitor, Port Security, Status.

Figure 58: Port Security Status



DISPLAYING PORT SECURITY STATISTICS

Use the Port Security Statistics page to display IEEE 802.1X statistics and protocol information for each port. It provides detailed IEEE 802.1X statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows only selected backend server (RADIUS Authentication Server) statistics.

PARAMETERS

These parameters are displayed on the 802.1X Statistics page:

- **Port** - Port Identifier.

Receive EAPOL Counters

- **Total** - The number of valid EAPOL frames of any type that have been received by the switch.
- **Response ID** - The number of valid EAP Resp/ID frames that have been received by the switch.
- **Responses** - The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.
- **Start** - The number of EAPOL Start frames that have been received by the switch.
- **Logoff** - The number of valid EAPOL logoff frames that have been received by the switch.

- **Invalid Type** - The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
- **Invalid Length** - The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.

Transmit EAPOL Counters

- **Total** - The number of EAPOL frames of any type that have been transmitted by the switch.
- **Request ID** - The number of EAP initial request frames that have been transmitted by the switch.
- **Requests** - The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.

Receive Backend Server Counters - For MAC-based ports there are two tables containing backend server counters. The left-most shows a summary of all backend server counters on this port. The right-most shows backend server counters for the currently selected client, or dashes if no client is selected or available. A client can be selected from the list of authorized/unauthorized clients below the two counter tables.

There are slight differences in the interpretation of the counters between port- and MAC-based authentication as shown below.

- **Access Challenges**

  For port-based authentication, this field counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. It indicates that the backend server has communications with the switch.

  For MAC-based authentication, this field counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).

- **Other Requests** - For port-based authentication, this field counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. It indicates that the backend server chose an EAP-method. For MAC-based authentication, this field is not applicable.
- **Auth. Successes** - For both port- and MAC-based authentication, this field counts the number of times that the switch receives a success indication. It indicates that the supplicant/client has successfully authenticated to the backend server.
- **Auth. Failures** - For both port-based and MAC-based authentication, this field counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.

Transmit Backend Server Counters

- **Responses**

  For port-based authentication, this field counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. This indicates that the switch has attempted

communication with the backend server. Possible retransmissions are not counted.

For MAC-based authentication, this field counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

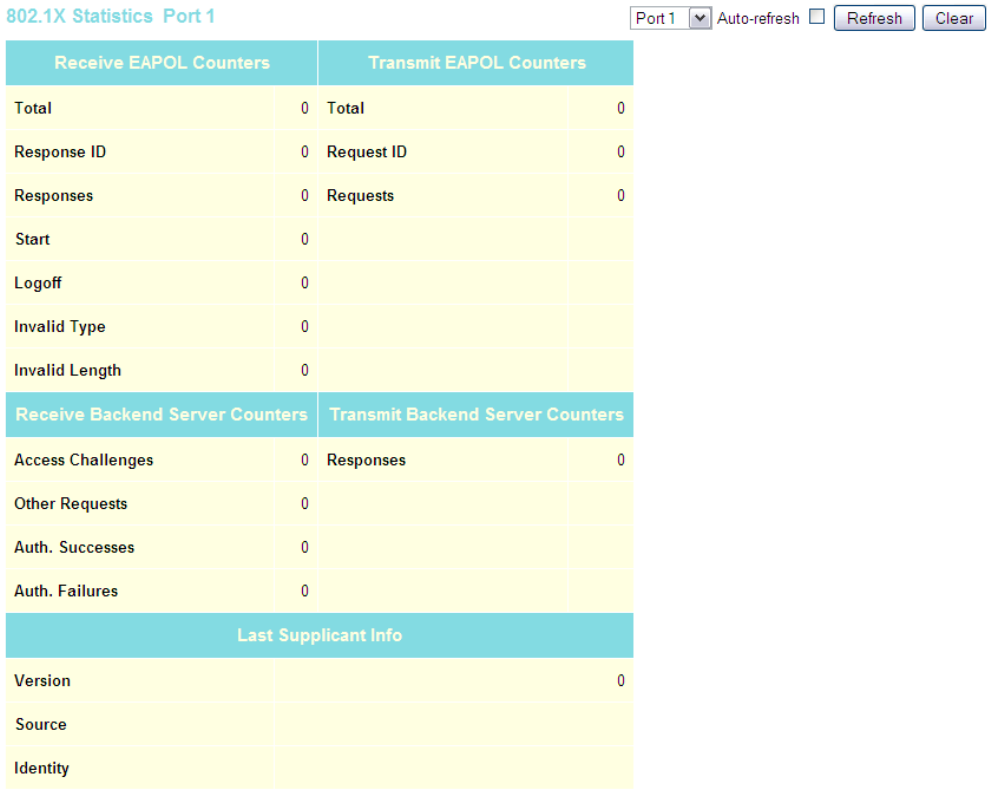
Last Supplicant Info

- **Version** - For port-based authentication, this field indicates the protocol version number carried in the most recently received EAPOL frame. For MAC-based authentication, this field is not applicable.
- **Source** - For port-based authentication, this field indicates the source MAC address carried in the most recently received EAPOL frame. For MAC-based authentication, this field is not applicable.
- **Identity** - For port-based authentication, this field shows the user name (supplicant identity) carried in the most recently received Resp/ ID EAPOL frame. For MAC-based authentication, this field shows the MAC address of the last client that attempted to authenticate (left-most table), or the MAC address of the currently selected client (right-most table).

WEB INTERFACE

To display IEEE 802.1X statistics and protocol information for each port, click Monitor, Port Security, Statistics.

Figure 59: Port Security Statistics



SHOWING IGMP SNOOPING INFORMATION

Use the IGMP Snooping page to display IGMP querier status and snooping statistics for each VLAN, the port members of each service group, and the ports connected to an upstream multicast router/switch.

PARAMETERS

These parameters are displayed on the IGMP Snooping Status page:

Statistics

- **VLAN ID** - VLAN Identifier.
- **Querier Status** - Shows the Querier status as "ACTIVE" or "IDLE." When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic.
- **Querier Transmit** - The number of transmitted Querier messages.
- **Querier Receive** - The number of received Querier messages.
- **V1 Reports Receive** - The number of received IGMP Version 1 reports.
- **V2 Reports Receive** - The number of received IGMP Version 2 reports.
- **V3 Reports Receive** - The number of received IGMP Version 3 reports.

- **V2 Leave Receive** - The number of received IGMP Version 2 leave reports.

IGMP Groups

- **VLAN ID** - VLAN Identifier.
- **Groups** - The IP address for a specific multicast service.
- **Port Members** - The ports assigned to the listed VLAN which propagate a specific multicast service.

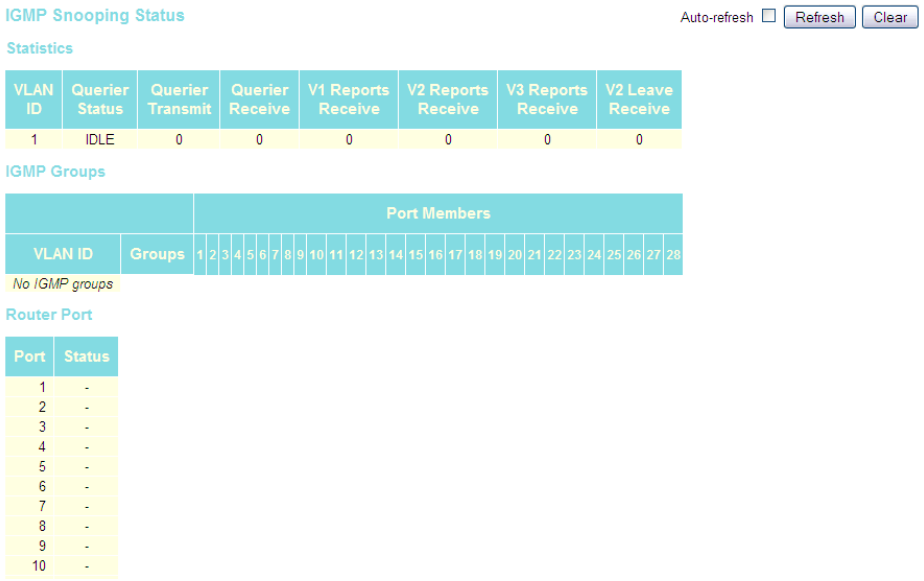
Router Port

- **Port** - Port Identifier.
- **Status** - Ports connected to multicast routers may be dynamically discovered by this switch or statically assigned to an interface on this switch.

WEB INTERFACE

To display information for IGMP snooping, click Monitor, IGMP Snooping.

Figure 60: IGMP Snooping Status



DISPLAYING LLDP INFORMATION

Use the monitor pages for LLDP to display information advertised by LLDP neighbors and statistics on LLDP control frames.

DISPLAYING LLDP NEIGHBOR INFORMATION

Use the LLDP Neighbor Information page to display information about devices connected directly to the switch's ports which are advertising information through LLDP.

PARAMETERS

These parameters are displayed on the LLDP Neighbor Information page:

- **Local Port** - The local port to which a remote LLDP-capable device is attached.
- **Chassis ID** - An octet string indicating the specific identifier for the particular chassis in this system.
- **Remote Port ID** - A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **System Name** - A string that indicates the system's assigned name.
- **Port Description** - A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **System Capabilities** - The capabilities that define the primary function(s) of the system as shown in the following table:

Table 13: System Capabilities

ID Basis	Reference
Other	–
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
Station only	IETF RFC 2011

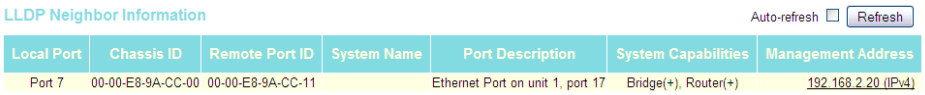
When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

- **Management Address** - The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

WEB INTERFACE

To display information about LLDP neighbors, click Monitor, LLDP, Neighbors.

Figure 61: LLDP Neighbor Information



DISPLAYING LLDP PORT STATISTICS

Use the LLDP Port Statistics page to display statistics on LLDP global counters and control frames.

PARAMETERS

These parameters are displayed on the LLDP Port Statistics page:

Global Counters

- **Neighbor entries were last changed at** - The time the LLDP neighbor entry list was last updated. It also shows the time elapsed since last change was detected.
- **Total Neighbors Entries Added** - Shows the number of new entries added since the switch was rebooted, and for which the remote TTL has not yet expired.
- **Total Neighbors Entries Deleted** - The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.
- **Total Neighbors Entries Dropped** - The number of times which the remote database on this switch dropped an LLDPDU because the entry table was full.
- **Total Neighbors Entries Aged Out** - The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

LLDP Statistics

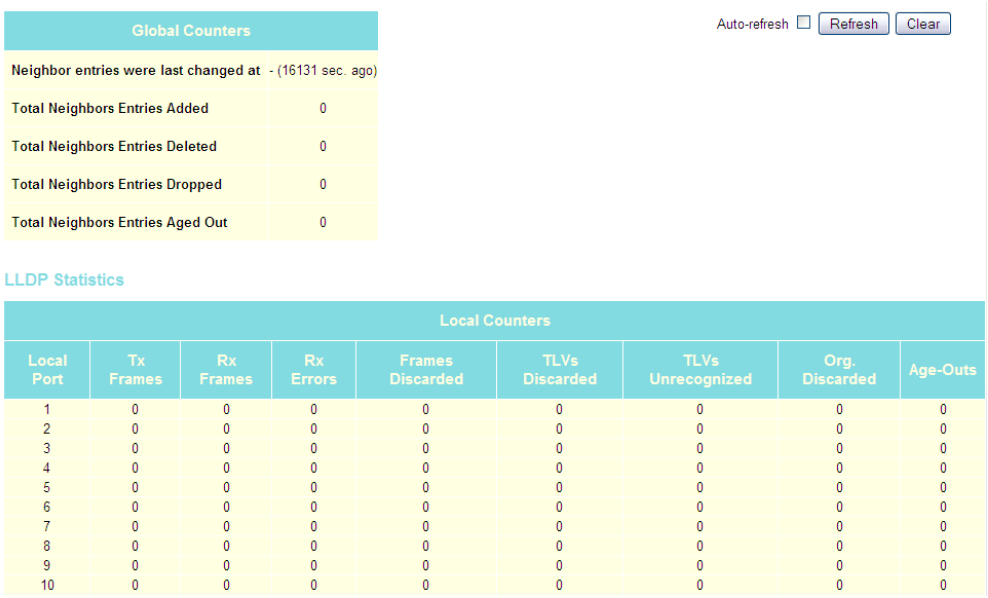
- **Local Port** - Port Identifier.
- **Tx Frames** - Number of LLDP PDUs transmitted.
- **Rx Frames** - Number of LLDP PDUs received.
- **Rx Errors** - The number of received LLDP frames containing some kind of error.

- **Frames Discarded** - Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular Type Length Value (TLV).
- **TLVs Discarded** - Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded.
- **TLVs Unrecognized** - The number of well-formed TLVs, but with an unknown type value.
- **Org. Discarded** - The number of organizational TLVs discarded.
- **Age-Outs** - Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age-out time, the LLDP information is removed, and the Age-Out counter is incremented.

WEB INTERFACE

To display statistics on LLDP global counters and control frames, click Monitor, LLDP, Port Statistics.

Figure 62: LLDP Port Statistics



Auto-refresh ☐ Refresh Clear

Global Counters	
Neighbor entries were last changed at	- (16131 sec. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics

Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

DISPLAYING DHCP RELAY STATISTICS

Use the DHCP Relay Statistics page to display statistics for the DHCP relay service supported by this switch and DHCP relay clients.

PARAMETERS

These parameters are displayed on the DHCP Relay Statistics page:

Server Statistics

- **Transmit to Server** - The number of packets relayed from the client to the server.
- **Transmit Error** - The number of packets containing errors that were sent to clients.
- **Receive from Server** - The number of packets received from the server.
- **Receive Missing Agent Option** - The number of packets that were received without agent information options.
- **Receive Missing Circuit ID** - The number of packets that were received with the Circuit ID option missing.
- **Receive Missing Remote ID** - The number of packets that were received with the Remote ID option missing.
- **Receive Bad Circuit ID** - The number of packets with a Circuit ID option that did not match a known circuit ID.
- **Receive Bad Remote ID** - The number of packets with a Remote ID option that did not match a known remote ID.

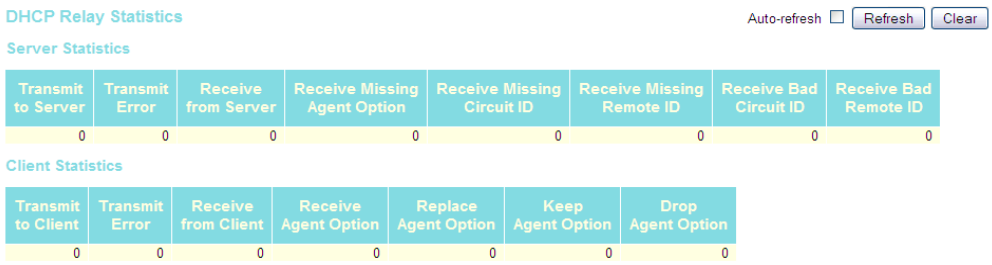
Client Statistics

- **Transmit to Client** - The number of packets that were relayed from the server to a client.
- **Transmit Error** - The number of packets containing errors that were sent to servers.
- **Receive from Client** - The number of packets received from clients.
- **Receive Agent Option** - The number of packets received where the switch.
- **Replace Agent Option** - The number of packets received where the DHCP client packet information was replaced with the switch's relay information.
- **Keep Agent Option** - The number of packets received where the DHCP client packet information was retained.
- **Drop Agent Option** - The number of packets that were dropped because they already contained relay information.

WEB INTERFACE

To display DHCP relay statistics, click Monitor, DHCP, Relay Statistics.

Figure 63: DHCP Relay Statistics



DISPLAYING THE MAC ADDRESS TABLE

Use the MAC Address Table to display dynamic and static address entries associated with the CPU and each port.

PARAMETERS

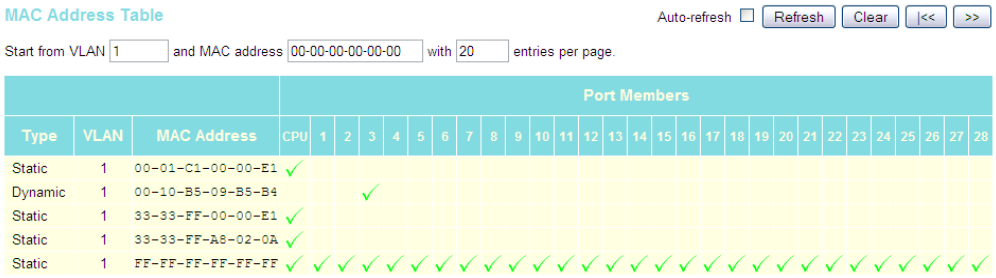
These parameters are displayed on the MAC Address Table:

- **Start from VLAN # and MAC address # with # entries per page** - These input fields allow you to select the starting point in the table.
- **Type** - Indicates whether the entry is static or dynamic. Dynamic MAC addresses are learned by monitoring the source address for traffic entering the switch. To configure static addresses, refer to "Configuring the MAC Address Table" on page 92.
- **VLAN** - The VLAN containing this entry.
- **MAC Address** - Physical address associated with this interface.
- **Port Members** - The ports associated with this entry.

WEB INTERFACE

To display the address table, click Monitor, MAC Address Table.

Figure 64: MAC Address Table



6 PERFORMING BASIC DIAGNOSTICS

This chapter describes how to test network connectivity using Ping for IPv4 or IPv6, and how to test network cables.

PINGING AN IPV4 OR IPV6 ADDRESS

The Ping page is used to send ICMP echo request packets to another node on the network to determine if it can be reached.

PARAMETERS

These parameters are displayed on the Ping page:

- **IP Address** – IPv4 or IPv6 address of the host.

  An IPv4 address consists of 4 numbers, 0 to 255, separated by periods.

  An IPv6 address consists of 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- **Ping Size** – The payload size of the ICMP packet.
  (Range: 8- 1400 bytes)

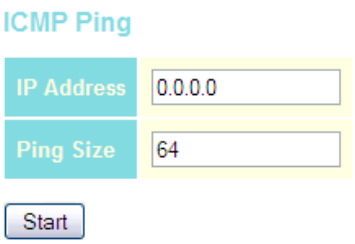
WEB INTERFACE

To ping another device on the network:

1. Click Diagnostics, Ping.
2. Enter the IP address of the target device.
3. Specify the packet size.
4. Click Start.

After you press Start, five ICMP packets are transmitted, and the sequence number and round-trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Figure 65: ICMP Ping



RUNNING CABLE DIAGNOSTICS

The VeriPHY page is used to perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open, etc.) and report the cable length.

PARAMETERS

These parameters are displayed on the VeriPHY Cable Diagnostics page:

- **Port** – Diagnostics can be performed on all ports or on a specific port.
- **Cable Status** – Shows the cable length, operating conditions and isolates a variety of common faults that can occur on Category 5 twisted pair cabling.

WEB INTERFACE

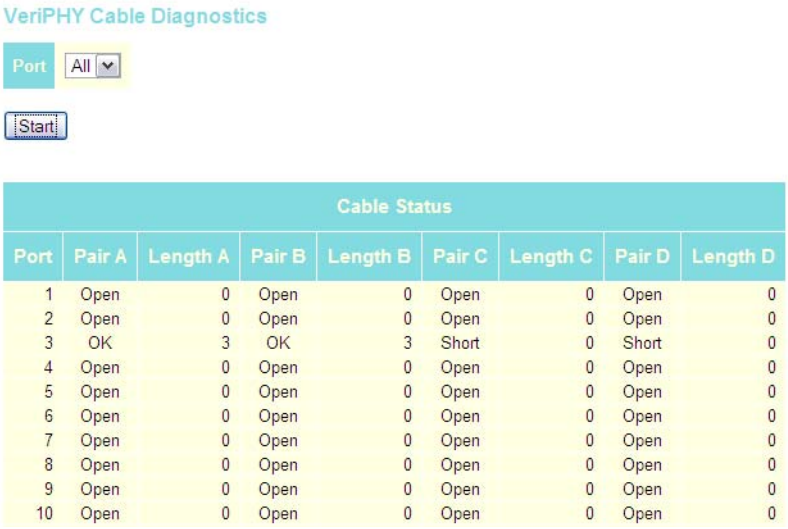
To run cable diagnostics:

1. Click Diagnostics, VeriPHY.
2. Select all ports or indicate a specific port for testing.
3. Click Start.

If a specific port is selected, the test will take approximately 5 seconds. If all ports are selected, it can run approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables 7 - 140 meters long.

Ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a management port will cause the switch to stop responding until testing is completed.

Figure 66: VeriPHY Cable Diagnostics



VeriPHY Cable Diagnostics

Port All

Start

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	Open	0	Open	0	Open	0	Open	0
2	Open	0	Open	0	Open	0	Open	0
3	OK	3	OK	3	Short	0	Short	0
4	Open	0	Open	0	Open	0	Open	0
5	Open	0	Open	0	Open	0	Open	0
6	Open	0	Open	0	Open	0	Open	0
7	Open	0	Open	0	Open	0	Open	0
8	Open	0	Open	0	Open	0	Open	0
9	Open	0	Open	0	Open	0	Open	0
10	Open	0	Open	0	Open	0	Open	0

7 PERFORMING SYSTEM MAINTENANCE

This chapter describes how to perform basic maintenance tasks including upgrading software, restoring or saving configuration settings, and resetting the switch.

RESETTING THE SWITCH

Use the Reset Device page to restart the switch.

WEB INTERFACE

To restart the switch

1. Click Maintenance, Reset Device.
2. Click Yes.

The reset will be complete when the user interface displays the login page.

Figure 67: Reset Device

RESTORING FACTORY DEFAULTS

Use the Factory Defaults page to restore the original factory settings. Note that the LAN IP Address, Subnet Mask and Gateway IP Address will be reset to their factory defaults.

WEB INTERFACE

To restore factory defaults:

1. Click Maintenance, Factory Defaults.
2. Click Yes.

The factory defaults are immediately restored, which means that no reboot is necessary.

Figure 68: Factory Defaults

UPGRADING FIRMWARE

Use the Software Upload page to upgrade the switch's system firmware by specifying a file provided by Transition Networks. You can download firmware files for your switch from the Support section of the Transition Networks web site at www.transition.com.

WEB INTERFACE

To upgrade firmware:

1. Click Maintenance, Software Upload.
2. Click the Browse button, and select the firmware file.
3. Click the Upload button to upgrade the switch's firmware.

After the software image is uploaded, a page announces that the firmware update has been initiated. After about a minute, the firmware is updated and the switch is rebooted.

CAUTION: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off at a frequency of 10 Hz while the firmware update is in progress. Do not reset or power off the device at this time or the switch may fail to function afterwards.

Figure 69: Software Upload

REGISTERING THE PRODUCT

Use the Register Product page to register your switch online if you have not already done so. The Register Product page provides a convenient link to the Transition Networks web site for this purpose.

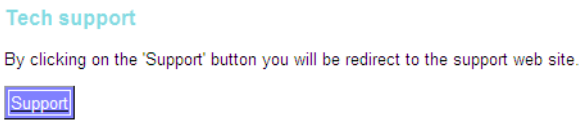
WEB INTERFACE

To register your switch:

1. Click Maintenance, Register Product.
2. Click the Register Now button.

Once you have selected your country, you will be directed to the main page where you can click on SUPPORT to register your product.

Figure 70: Register Product



MANAGING CONFIGURATION FILES

Use the Maintenance Configuration pages to save the current configuration to a file on your computer, or to restore previously saved configuration settings to the switch.

SAVING CONFIGURATION SETTINGS

Use the Configuration Save page to save the current configuration settings to a file on your local management station.

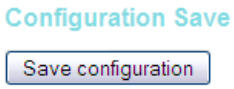
WEB INTERFACE

To save your current configuration settings:

1. Click Maintenance, Configuration, Save.
2. Click the “Save configuration” button.
3. Specify the directory and name of the file under which to save the current configuration settings.

The configuration file is in XML format. The configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire configuration including syntax descriptions is included in the file. The file may be modified using an editor and loaded to a switch.

Figure 71: Configuration Save



RESTORING CONFIGURATION SETTINGS

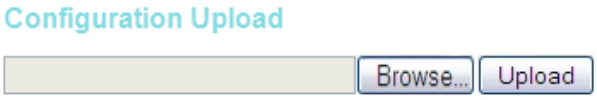
Use the Configuration Upload page to restore previously saved configuration settings to the switch from a file on your local management station.

WEB INTERFACE

To restore your current configuration settings:

1. Click Maintenance, Configuration, Upload.
2. Click the Browse button, and select the configuration file.
3. Click the Upload button to restore the switch's settings.

Figure 72: Configuration Upload



SECTION III

COMMAND LINE INTERFACE

This section provides a detailed description of the Command Line Interface, along with examples for all of the commands.

This section includes these chapters:

- "Using the Command Line Interface" on page 177
- "System Commands" on page 185
- "IP Commands" on page 195
- "Authentication Commands" on page 205
- "Port Commands" on page 215
- "Link Aggregation Commands" on page 224
- "LACP Commands" on page 229
- "RSTP Commands" on page 235
- "IEEE 802.1X Commands" on page 246
- "IGMP Commands" on page 255
- "LLDP Commands" on page 264
- "MAC Commands" on page 271
- "VLAN Commands" on page 276
- "PVLAN Commands" on page 282
- "QoS Commands" on page 285
- "ACL Commands" on page 296
- "Mirror Commands" on page 304
- "Config Commands" on page 306

- "SNMP Commands" on page 308
- "HTTPS Commands" on page 329
- "SSH Commands" on page 332
- "UPnP Commands" on page 334
- "DHCP Commands" on page 337
- "Firmware Commands" on page 341

8 USING THE COMMAND LINE INTERFACE

This chapter describes how to use the Command Line Interface (CLI).

ACCESSING THE CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet or Secure Shell connection (SSH), the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

CONSOLE CONNECTION

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user name is "admin" with password "admin". When the administrator's user name and password are entered, the CLI displays the ">" prompt.
2. Enter the necessary commands to complete your desired tasks.
3. When finished, exit the session with the "logout" command.

After connecting to the system through the console port, the login screen displays:

```
Username: admin
Password:
Login in progress...
Welcome to Command Line Interface.
Type 'help' or '?' to get help.

Port Numbers:

+------------------------------------------------------------+
| +--+--+--+--+ +--+--+--+--+ +--+--+--+--+   +----+   +----+ |
| | 1| 3| 5| 7| | 9|11|13|15| |17|19|21|23|   | 27 |   | 28 | |
| +--+--+--+--+ +--+--+--+--+ +--+--+--+--+   +----+   +----+ |
| | 2| 4| 6| 8| |10|12|14|16| |18|20|22|24|   | 25 |   | 26 | |
| +--+--+--+--+ +--+--+--+--+ +--+--+--+--+   +----+   +----+ |
+------------------------------------------------------------+
>
```

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,

```
>ip setup 192.168.0.10 255.255.255.0 192.168.0.1 1
>
```

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 ">" prompt for the administrator.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the "logout" command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:
Login in progress...
Welcome to LevelOne Command Line Interface.
Type 'help' or '?' to get help.

Port Numbers:

+------------------------------------------------------------+
| +--+--+--+--+ +--+--+--+--+ +--+--+--+--+   +----+   +----+ |
| | 1| 3| 5| 7| | 9|11|13|15| |17|19|21|23|   | 27 |   | 28 | |
| +--+--+--+--+ +--+--+--+--+ +--+--+--+--+   +----+   +----+ |
| | 2| 4| 6| 8| |10|12|14|16| |18|20|22|24|   | 25 |   | 26 | |
| +--+--+--+--+ +--+--+--+--+ +--+--+--+--+   +----+   +----+ |
+------------------------------------------------------------+
>
```

You can open up to four sessions to the device via Telnet.

NOTE: When SSH is enabled, Telnet can't be used.

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. Commands are organized into functional groups. You can enter the full command from the main level command prompt ">," or enter the name of a command group (e.g., port) and then enter the required command without the group name prefix.

For example, in the command "port configuration 5," **port configuration** are keywords, and **5** specifies the 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:

  >**port**
  Port>**configuration 5**

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

  >**system password admin**

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.

GETTING HELP ON COMMANDS

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the "?" character to list keywords or parameters.

SHOWING COMMANDS

If you enter a "?" at the command prompt, the system will display the first level of keywords or command groups. You can also display a list of valid keywords for a specific command. For example, the command "**system ?**" displays a list of possible system commands:

```
>help
General Commands:
-----------------
Help/?: Get help on a group or a specific command
Up    : Move one command level up
Logout: Exit CLI

Command Groups:
---------------
System  : System settings and reset options
IP      : IP configuration and Ping
Auth    : Authentication
Port    : Port management
Aggr    : Link Aggregation
LACP    : Link Aggregation Control Protocol
RSTP    : Rapid Spanning Tree Protocol
Dot1x   : IEEE 802.1X port authentication
IGMP    : Internet Group Management Protocol snooping
LLDP    : Link Layer Discovery Protocol
MAC     : MAC address table
VLAN    : Virtual LAN
PVLAN   : Private VLAN
QoS     : Quality of Service
ACL     : Access Control List
Mirror  : Port mirroring
Config  : Load/Save of configuration via TFTP
SNMP    : Simple Network Management Protocol
HTTPS    : Hypertext Transfer Protocol over Secure Socket Layer
SSH     : Secure Shell
UPnP    : Universal Plug and Plug
DHCP    : Dynamic Host Configuration Protocol
Firmware: Download of firmware via TFTP
Debug   : Switch debug facilities
```

```
Type '<group>' to enter command group, e.g. 'port'.
Type '<group> ?' to get list of group commands, e.g. 'port ?'.
Type '<command> ?' to get help on a command, e.g. 'port mode ?'.
Commands may be abbreviated, e.g. 'po co' instead of 'port configuration'.
>
```

The command "**system ?**" will display the following information:

```
>system ?
Available Commands:

System Configuration [all] [<port_list>]
System Reboot
System Restore Default [keep_ip]
System Contact [<contact>]
System Name [<name>]
System Location [<location>]
System Password [<password>]
System Timezone [<offset>]
System Log [<log_id>] [all|info|warning|error] [clear]
System Access Configuration
System Access Mode [enable|disable]
System Access Add <access_id> <start_ip_addr> <end_ip_addr> [web|snmp|telnet]
System Access Ipv6 Add <access_id> <start_ipv6_addr> <end_ipv6_addr>
  [web|snmp|telnet]
System Access Delete <access_id>
System Access Lookup <access_id>
System Access Clear
System Access Statistics [clear]
>
```

PARTIAL KEYWORD LOOKUP

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember to leave a space between the command and question mark.) For example "**m ?**" shows all the keywords starting with "m."

```
>m ?
Available Commands:

MAC Configuration [<port_list>]
MAC Add <mac_addr> <port_list> [<vid>]
MAC Delete <mac_addr> [<vid>]
MAC Lookup <mac_addr> [<vid>]
MAC Agetime [<age_time>]
MAC Learning [<port_list>] [auto|disable|secure]
MAC Dump [<mac_max>] [<mac_addr>] [<vid>]
MAC Statistics [<port_list>]
MAC Flush
Mirror Configuration [<port_list>]
Mirror Port [<port>|disable]
Mirror Mode [<port_list>] [enable|disable|rx|tx]
>
```

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.

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 14: Keystroke Commands

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Delete key or backspace key	Erases a mistake when entering a command.

CLI COMMAND GROUPS

The system commands can be broken down into the functional groups shown below.

Table 15: Command Group Index

Command Group	Description	Page
System	Configures general system settings, including descriptive information, user name and password, rebooting the system, setting the time zone, configuring the log levels to display, and filtering management access to the switch through specified IP addresses.	185
IP	Configures IP settings, including IPv4 or IPv6 addresses, DHCP, DNS, DNS proxy, as well as SNTP	195
Auth	Controls management access through RADIUS or TACACS+ authentication servers	205
Port	Configures connection parameters for ports, power saving mode, and cable testing	215
Aggr	Configures static port aggregation, including member assignment, and load balancing methods	224
LACP	Configures Link Aggregation Control Protocol	229
RSTP	Configures Rapid Spanning Tree Protocol	235
Dot1x	Configures IEEE 802.1X Port Authentication	246
IGMP	Configures IGMP snooping, query, throttling, and filtering	255
LLDP	Configures Link Layer Discovery Protocol	264
MAC	Configures the MAC address table, including learning mode, aging time, and setting static addresses	271
VLAN	Configures VLAN port members and port attributes	276
PVLAN	Configures private VLANs and isolated ports	282
QoS	Configures quality of service parameters, including default port queue, default tag assigned to untagged frames, input rate limiting, output shaping, queue mode, queue weight, quality control lists, storm control, DSCP remarking, and DSCP queue mapping	285
ACL	Configures access control lists, including policies, responses, and rate limiters	296
Mirror	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	304
Config	Saves or restores configuration settings	306
SNMP	Configures SNMP community strings, trap managers, and basic settings for SNMPv3	308
HTTPS	Enables or disables HTTPS, or automatically redirects management access from HTTP connections to HTTPS	329
SSH	Enables or disables management access via SSH	332
UPnP	Configures UPnP protocol settings	334
DHCP	Configures DHCP Relay and Option 82 Information	337

Table 15: Command Group Index

Command Group	Description	Page
Firmware	Upgrades firmware via a TFTP server	341
Debug	Displays debugging information for all key functions These commands are not described in this manual. Please refer to the prompt messages included in the CLI interface.	

9 SYSTEM COMMANDS

This section describes commands used to configure information that uniquely identifies the switch, set the user name and password, reboot the system, set the time zone, configure the log levels to display, and filter management access to the switch through specified IP addresses.

Table 16: System Commands

Command	Function
system configuration	Displays information that uniquely identifies the switch
system reboot	Restarts the system
system restore default	Restore factory default settings
system contact	Sets the name of the administrator responsible for the system
system name	Displays or sets the name assigned to the switch system
system location	Displays or sets the system location
system password	Displays or sets the administrator password
system timezone	Displays or sets the time zone for the switch's internal clock
system log	Displays log entries, configures the log levels to display, or clears the log table
system access configuration	Displays the access mode and the number of authorized addresses
system access mode	Shows or sets the access mode
system access add	Adds IPv4 addresses that are allowed management access
system access ipv6 add	Adds IPv6 addresses that are allowed management access
system access delete	Deletes an access management entry
system access lookup	Displays specified access management entry
system access clear	Clears all access management entries
system access statistics	Displays or clears access management statistics

system configuration

This command displays a brief summary of information that uniquely identifies the switch, or a full list of all configuration settings for all ports or for a specified port or port range.

SYNTAX

system configuration [**all** [*port-list*]]

all - Displays a full list of all configuration settings.

port-list - Displays a full list of configuration settings for a specified port or for a range of ports. (Range: 1-28, or **all**)

EXAMPLE

```
System>configuration
System Contact :
System Name    :
System Location:
System Password:
Timezone Offset: 0
MAC Address    : 00-01-c1-00-00-e1
System Time    : 1970-01-01 03:39:06 +0000
System Uptime  : 03:39:06
Software Version: GEL-2870 Managed (standalone) GEL-2870-LevelOne-0_4
Software Date   : 2009-06-12 14:32:38 +0200
System>
```

system reboot

This command restarts the system.

SYNTAX

system reboot

COMMAND USAGE

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.

EXAMPLE

This example shows how to reset the switch:

```
System>reboot
System will reset in a few seconds
⋮
Username:
```

system restore default

This command restores the original factory settings. Note that the LAN IP Address, Subnet Mask and Gateway IP Address will be reset to their factory defaults.

SYNTAX

system restore default [**keep_ip**]

all - Displays a full list of all configuration settings.

DEFAULT SETTING

Restores all settings

EXAMPLE

This example shows how to restore all factory defaults.

```
System>restore default
System>
```

system contact

This command displays or sets the system contact.

SYNTAX

system contact [*contact*]

contact - String that describes the system contact information. (Maximum length: 255 characters)

DEFAULT SETTING

None

COMMAND USAGE

No blank spaces are permitted as part of the contact string.

EXAMPLE

```
System>contact Maggie
System>
```

system name

This command displays or sets the name assigned to the switch system.

SYNTAX

system name [*name*]

name - The name of this switch. (Maximum length: 255 characters)

DEFAULT SETTING
None

COMMAND USAGE
No blank spaces are permitted as part of the name string.

EXAMPLE

```
System>name RD
System>
```

system location

This command displays or sets the system location.

SYNTAX

system location [*location*]

location - String that describes the system location. (Maximum length: 255 characters)

DEFAULT SETTING
None

COMMAND USAGE
No blank spaces are permitted as part of the location string.

EXAMPLE

```
System>location WC5
System>
```

system password

This command displays or sets the administrator password.

SYNTAX

system password [[*password*] | [**clear**]]

password - The authentication password for the administrator. (Maximum length: 8 characters plain text, case sensitive)

clear - Removes the administrator password.

DEFAULT SETTING
None

COMMAND USAGE
The administrator has read/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

EXAMPLE

```
System>password admin
System>
```

system timezone

This command displays or sets the time zone for the switch's internal clock.

SYNTAX

system timezone [*offset*]

offset - Number of minutes before/after UTC. (Range: -720 minutes before to 720 minutes after)

DEFAULT SETTING

no offset

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 minutes your time zone is east (before) or west (after) of UTC.

EXAMPLE

```
System>time -240
System>
```

system log

This command displays log entries, configures the log levels to display, or clears the log table.

SYNTAX

system log [*log-id*] [**all** | **info** | **warning** | **error**] [**clear**]

log-id - System log ID or range of IDs.

all - Shows all levels.

info - Shows informational messages only.

warning - Shows warning conditions.

error - Shows error conditions.

clear - Clears log messages.

DEFAULT SETTING

Displays all entries
Displays all message levels

EXAMPLE

```
System>log all
.
.
 590  Info    1970-01-01 02:22:38 +0000  Frame of 202 bytes received on port 4
 591  Info    1970-01-01 02:22:41 +0000  Frame of 202 bytes received on port 3
 592  Info    1970-01-01 02:23:09 +0000  Frame of 202 bytes received on port 4
 593  Info    1970-01-01 02:23:12 +0000  Frame of 202 bytes received on port 3
 594  Info    1970-01-01 02:23:40 +0000  Frame of 202 bytes received on port 4
 595  Info    1970-01-01 02:23:43 +0000  Frame of 202 bytes received on port 3
 596  Info    1970-01-01 02:23:56 +0000  Frame of 243 bytes received on port 1
 597  Info    1970-01-01 02:23:56 +0000  Frame of 243 bytes received on port 0
System>
```

system access configuration

This command displays the access mode and the number of authorized addresses.

SYNTAX

system access configuration

EXAMPLE

```
System/Access>configuration
System Access Mode : Enabled
System Access number of entries: 1
Idx Start IP Address                End IP Address                  WEB  SNMP TELNET
--- ------------------------------- ------------------------------- ---- ---- -----
1   192.168.1.19                    192.168.1.19                     Yes  NO    NO
System/Access>
```

system access mode

This command shows or sets the management access mode.

SYNTAX

system access mode [**enable** | **disable**]

enable - Enables access management.

disable - Disables access management.

DEFAULT SETTING

Disabled

EXAMPLE

```
System>access mode enable
System>
```

system access add

This command adds IPv4 addresses that are allowed management access to the switch through various protocols.

SYNTAX

system access add *access-id start-ip-addr end-ip-addr* [**web** | **snmp** | **telnet**]

access-id - Entry index. (Range: 1-16)

start-ip-addr - The starting IPv4 address of a range.

end-ip-addr - The ending IPv4 address of a range.

web - Adds IP address(es) to the web group.

snmp - Adds IP address(es) to the SNMP group.

telnet - Adds IP address(es) to the Telnet group.

DEFAULT SETTING

None

COMMAND USAGE

- To set a single address for a entry, enter the same address for both the start and end of a range.
- 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.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.

EXAMPLE

```
System/Access>add 1 192.168.1.0 192.168.2.0 web
System/Access>
```

system access ipv6 add

This command adds IPv6 addresses that are allowed management access to the switch through various protocols.

SYNTAX

system access ipv6 add *access-id start-ip-addr end-ip-addr* [**web** | **snmp** | **telnet**]

access-id - Entry index. (Range: 1-16)

start-ip-addr - The starting IPv6 address of a range.

end-ip-addr - The ending IPv6 address of a range.

web - Adds IP address(es) to the web group.

snmp - Adds IP address(es) to the SNMP group.

telnet - Adds IP address(es) to the Telnet group.

DEFAULT SETTING

None

COMMAND USAGE

- An IPv6 address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.
- To set a single address for a entry, enter the same address for both the start and end of a range.
- 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.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.

EXAMPLE

```
System>access ipv6 add 1 2001:DB8:2222:7272::72 2001:DB8:2222:7272::72 web
System>
```

system access delete

This command deletes an access management entry.

SYNTAX

system access delete *access-id*

access-id - Entry index. (Range: 1-16)

EXAMPLE

```
System/Access>delete 1
System/Access>
```

system access lookup

This command displays specified access management entry.

SYNTAX

system access lookup *access-id*

access-id - Entry index. (Range: 1-16)

EXAMPLE

```
System/Access>lookup 1
Idx Start IP Address                End IP Address                  WEB  SNMP TELNET
--- ------------------------------- ------------------------------- ---- ---- -----
1   192.168.1.0                     192.168.2.0                      Yes  NO    NO
System/Access>
```

system access clear

This command clears all access management entries.

SYNTAX

system access clear

EXAMPLE

```
System/Access>clear
System/Access>
```

system access statistics

This command displays or clears access management statistics.

SYNTAX

system access statistics [**clear**]

clear - Clears all access management statistics.

EXAMPLE

```
System/Access>statistics

Access Management Statistics:
-----------------------------
HTTP     Receive:          3    Allow:          0    Discard:          0
HTTPS    Receive:          0    Allow:          0    Discard:          0
SNMP     Receive:          0    Allow:          0    Discard:          0
TELNET   Receive:          0    Allow:          0    Discard:          0
SSH      Receive:          0    Allow:          0    Discard:          0
System/Access>
```

10 IP COMMANDS

This section describes commands used to configure IP settings, including IPv4 or IPv6 addresses, DHCP, DNS, DNS proxy, as well as SNTP.

Table 17: IP Commands

Command	Function
ip configuration	Displays all settings for IPv4 and IPv6 and related functions
ip dhcp	Displays or sets the DHCP client mode
ip setup	Displays or sets the switch's IPv4 address and gateway for the specified VLAN
ip ping	Sends ICMP echo request packets to another node on the network
ip dns	Displays or sets a DNS server to which client requests for mapping host names to IP addresses are forwarded
ip dns_proxy	Displays or sets DNS proxy mode which can maintain a local database based on previous responses to DNS queries forwarded on behalf of attached clients
ip sntp	Displays or sets the IP address for a time server
ip ipv6 autoconfig	Displays or sets stateless autoconfiguration of IPv6 addresses on an interface and IPv6 functionality on the interface
ip ipv6 setup	Displays or sets the switch's IPv6 address and gateway for the specified VLAN
ip ipv6 ping6	Sends ICMP echo request packets to another node on the network
ip ipv6 sntp	Displays or sets the IP address for a time server

ip configuration

This command displays all settings for IPv4 and IPv6 and related functions.

SYNTAX

ip configuration

EXAMPLE

The default settings are shown in the following example.

```
IP>configuration
DHCP Client        : Enabled
IP Address         : 192.168.1.1
IP Mask            : 255.255.255.0
IP Router          : 0.0.0.0
DNS Server         : 0.0.0.0
VLAN ID            : 1
DNS Proxy          : Disabled
IPv6 AUTOCONFIG mode  : Disabled
IPv6 Link-Local Address: fe80::2e1:ff:fe00:0
```

```
IPv6 Address      : ::192.168.1.10
IPv6 Prefix       : 96
IPv6 Router       : ::
IPv6 VLAN ID      : 1
SNTP Server       :
IPv6 SNTP Server  : ::

Active Configuration:
IP Address        : 192.168.1.1
IP Mask           : 255.255.255.0
IP Router         : 0.0.0.0
DNS Server        : 0.0.0.0
SNTP Server       :
IP>
```

ip dhcp

This command displays or sets the DHCP client mode.

SYNTAX

ip dhcp [**enable** | **disable**]

enable - Enables or renews the switches IP address through DHCP.

disable - Disables DHCP client mode.

DEFAULT SETTING

Enabled

COMMAND USAGE

NOTE: An IPv4 address for this switch is obtained via DHCP by default. If the switch does not receive a response from a DHCP server, it will default to the IP address 192.168.1.1 and subnet mask 255.255.255.0.

- This switch supports both IP Version 4 and Version 6, and can be managed simultaneously through either of these address types. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a DHCP server when it is powered on.
- The IPv4 address for the switch is obtained via DHCP by default for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network using the ip setup command (page 197). You may also need to a establish a default gateway between the switch and management stations that exist on another network segment using the ip setup command.
- If DHCP is enabled, the system will immediately start broadcasting service requests. 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). If the switch does not receive a response from a DHCP server, it will default to the IP address 192.168.1.1 and subnet mask 255.255.255.0.

- If the IP DHCP option is enabled, the switch will start broadcasting service requests as soon as it is powered on.

EXAMPLE

```
IP>dhcp enable
IP>dhcp
DHCP Client       : Enabled

Active Configuration:
IP Address        : 192.168.0.3
IP Mask           : 255.255.255.0
IP Router         : 0.0.0.0
DNS Server        : 0.0.0.0
SNTP Server       :
IP>
```

ip setup

This command displays or sets the switch's IPv4 address and gateway for the specified VLAN.

SYNTAX

ip setup [*ip-addr*] [*network-mask*] [*gateway*] [*vlan-id*]

ip-addr - IPv4 address.

network-mask - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

gateway - IP address of the default gateway.

vlan-id - VLAN to which the management address is assigned. (Range: 1-4095)

DEFAULT SETTING

IP Address: 192.168.1.1
Network Mask: 255.255.255.0
Gateway: none
VLAN: 1

COMMAND USAGE

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.

- You must assign an IP address to this device to gain management access over the network or to connect the switch to existing IP subnets. You can manually configure a specific IP address, or direct the device to obtain an address from a DHCP server using the ip dhcp command (page 196). 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.

- A gateway must be defined if the management station is located in a different IP segment.
- An default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.
- The attributes for this command must be entered in the sequence shown for command syntax.

EXAMPLE

In the following example, the device is assigned an address in VLAN 1.

```
IP>setup 192.168.0.9 255.255.255.0 192.168.0.1
IP>setup
IP Address        : 192.168.0.9
IP Mask           : 255.255.255.0
IP Router         : 192.168.0.1
DNS Server        : 0.0.0.0
VLAN ID           : 1
IP>
```

ip ping

This command sends ICMP echo request packets to another node on the network.

SYNTAX

ip ping *ip-addr* [*packet-size*]

ip-addr - IP address or IP alias of the host. An IPv4 address consists of 4 numbers, 0 to 255, separated by periods.

packet-size - The payload size of the ICMP packet. (Range: 8-1400 bytes) The actual packet size excludes MAC, IP and ICMP headers.

DEFAULT SETTING

Packet Size: 60 bytes
Count: 5

COMMAND USAGE

- When you enter the ping command, five ICMP packets are transmitted, and the sequence number and round-trip time are displayed upon reception of a reply.
- The following are some results of the ping command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.

- *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.
- *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
- *Network or host unreachable* - The gateway found no corresponding entry in the route table.

◆ When pinging a host name, be sure the DNS server address has been configured with the ip dns command.

EXAMPLE

```
IP>ping 192.168.1.1
PING server 192.168.1.1
60 bytes from 192.168.1.1: icmp_seq=0, time=0ms
60 bytes from 192.168.1.1: icmp_seq=1, time=0ms
60 bytes from 192.168.1.1: icmp_seq=2, time=0ms
60 bytes from 192.168.1.1: icmp_seq=3, time=0ms
60 bytes from 192.168.1.1: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
IP>
```

ip dns

This command displays or sets a DNS server to which client requests for mapping host names to IP addresses are forwarded.

SYNTAX

ip dns [*ip-addr*]

ip-addr - IP address of domain-name server. An IPv4 address consists of 4 numbers, 0 to 255, separated by periods.

DEFAULT SETTING

None

EXAMPLE

```
IP>dns 192.168.1.55
IP>
```

ip dns_proxy

This command displays or sets DNS proxy mode which can maintain a local database based on previous responses to DNS queries forwarded on behalf of attached clients.

SYNTAX

ip dns_proxy [**enable** | **disable**]

enable - Enables DNS proxy service.

disable - Disables DNS proxy service.

DEFAULT SETTING
Disabled

COMMAND USAGE
If enabled, the switch maintains a local database based on previous responses to DNS queries forwarded on behalf of attached clients. If the required information is not in the local database, the switch forwards the DNS query to a DNS server, stores the response in its local cache for future reference, and passes the response back to the client.

EXAMPLE

```
IP>dns_proxy enable
IP>
```

ip sntp

This command displays or sets the IP address for a time server.

SYNTAX

ip sntp [*ip-addr*]

ip-addr - IP address or IP alias of a time server (NTP or SNTP). An IPv4 address consists of 4 numbers, 0 to 255, separated by periods.

DEFAULT SETTING
None

COMMAND USAGE
The switch attempts to periodically update the time from the specified server. The polling interval is fixed at 15 minutes.

EXAMPLE

```
IP>sntp 192.168.1.19
IP>
```

ip ipv6 autoconfig

This command displays or sets stateless autoconfiguration of IPv6 addresses on an interface and IPv6 functionality on the interface.

SYNTAX

ip ipv6 autoconfig [**enable** | **disable**]

enable - Enables IPv6 autoconfiguration mode.

disable - Disables IPv6 autoconfiguration mode.

DEFAULT SETTING
Disabled

COMMAND USAGE

- To connect to a larger network with multiple subnets, you must configure a global unicast address. This address can be automatically configured using this command, or it can be manually configured using the ip ipv6 setup command (page 201).

- When autoconfiguration is enabled, the network portion of the address is based on prefixes received in IPv6 router advertisement messages observed on the local interface, and the host portion is automatically generated using the modified EUI-64 form of the interface identifier; i.e., the switch's MAC address.

EXAMPLE

```
IP/IPv6>autoconfig enable
IP/IPv6>autoconfig
IPv6 AUTOCONFIG mode  : Enabled
IPv6 Link-Local Address: fe80::2e1:ff:fe00:0
IPv6 Address      : ::192.168.1.1
IPv6 Prefix       : 96
IPv6 Router       : ::
IPv6 VLAN ID      : 1
IP/IPv6>
```

ip ipv6 setup

This command displays or sets the switch's IPv6 address and gateway for the specified VLAN.

SYNTAX

ip ipv6 setup [*ipv6-addr*] [*ipv6-prefix*] [*ipv6-gateway*] [*vlan-id*]

ipv6-addr - The full IPv6 address of the switch including the network prefix and host address bits.

ipv6-prefix - A decimal value indicating how many contiguous bits (starting at the left) of the address comprise the prefix.

ipv6-gateway - The IPv6 address of the default next hop router to use when the management station is located on a different network segment

vlan-id - VLAN to which the management address is assigned. (Range: 1-4095)

DEFAULT SETTING

IPv6 Address: ::192.168.1.1
Prefix: 96 bits – The default prefix length specifies that the first six colon-separated values comprise the network portion of the address.

COMMAND USAGE

- All IPv6 addresses must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- To connect to a larger network with multiple subnets, you must configure a global unicast address. This address can be manually configured with this command, or it can be automatically configured using the ip ipv6 autoconfig command (page 200).
- When configuring a link-local address, the prefix length is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier (i.e., the physical MAC address). You can manually configure a link-local address by entering the full address with the network prefix FE80.
- An IPv6 default gateway must be defined if the management station is located in a different IPv6 segment. An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

EXAMPLE

This example specifies the IPv6 address, the prefix length, the IPv6 gateway, and the VLAN to which the address is assigned.

```
IP/IPv6>setup 2001:DB8:2222:7272::72 96 FE80::269:3EF9:FE19:6780 1
IP/IPv6>setup
IPv6 AUTOCONFIG mode  : Enabled
IPv6 Link-Local Address: fe80::2e1:ff:fe00:0
IPv6 Address      : 2001:db8:2222:7272::72
IPv6 Prefix       : 96
IPv6 Router       : fe80::269:3ef9:fe19:6780
IPv6 VLAN ID      : 1
IP/IPv6>
```

ip ipv6 ping6

This command sends ICMP echo request packets to another node on the network.

SYNTAX

ip ipv6 ping6 *ipv6-addr* [*packet-size*]

ipv6-addr - IP address of the host. An IPv6 address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

packet-size - The payload size of the ICMP packet. (Range: 8-1400 bytes) The actual packet size excludes MAC, IP and ICMP headers.

DEFAULT SETTING

Packet Size: 68 bytes
Count: 5

COMMAND USAGE

- An IPv6 address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.
- When you enter the ping command, five ICMP packets are transmitted, and the sequence number and round-trip time are displayed upon reception of a reply.
- The following are some results of the ping command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.

EXAMPLE

```
IP/IPv6>ping6 ::192.168.1.19
PING6 server ::192.168.1.19
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
Sent 5 packets, received 0 OK, 0 bad
IP/IPv6>
```

ip ipv6 sntp

This command displays or sets the IP address for a time server.

SYNTAX

ip ipv6 sntp [*ipv6-addr*]

ipv6-addr - The IP address for a time server (NTP or SNTP). An IPv6 address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

DEFAULT SETTING

None

COMMAND USAGE

The switch attempts to periodically update the time from the specified server. The polling interval is fixed at 15 minutes.

EXAMPLE

```
IP/IPv6>sntp ::129.6.15.28
IP/IPv6>
```

11 AUTHENTICATION COMMANDS

This section describes commands used to controls management access through RADIUS or TACACS+ authentication servers.

Table 18: Authentication Commands

Command	Function
auth configuration	Displays settings for authentication servers and the authentication methods used for each access protocol
auth timeout	Displays or sets the time the switch waits for a reply from an authentication server before it resends the request
auth deadtime	Displays or sets the time after which the switch considers an authentication server to be dead if it does not reply
auth radius	Displays or sets RADIUS authentication server settings
auth acct_radius	Displays or sets RADIUS accounting server settings
auth tacacs+	Displays or sets TACACS+ authentication server settings
auth client	Displays or sets the authentication methods used for each management access protocol
auth statistics	Displays statistics for configured authentication and accounting servers

auth configuration

This command displays the settings for authentication servers and the authentication methods used for each access protocol.

SYNTAX

auth configuration

EXAMPLE

The default settings are shown in the following example.

```
Auth>configuration

Server Timeout    : 15 seconds

Server Dead Time : 300 seconds

RADIUS Authentication Server Configuration:
===========================================
Server  Mode      IP Address       Secret                          Port
------  --------  ---------------  ------------------------------  -----
1       Disabled                                                    1812
2       Disabled                                                    1812
3       Disabled                                                    1812
4       Disabled                                                    1812
5       Disabled                                                    1812
```

```
RADIUS Accounting Server Configuration:
=======================================
Server  Mode      IP Address       Secret                          Port
------  --------  ---------------  ------------------------------  -----
1       Disabled                                                    1813
2       Disabled                                                    1813
3       Disabled                                                    1813
4       Disabled                                                    1813
5       Disabled                                                    1813

TACACS+ Authentication Server Configuration:
============================================
Server  Mode      IP Address       Secret                          Port
------  --------  ---------------  ------------------------------  -----
1       Disabled                                                      49
2       Disabled                                                      49
3       Disabled                                                      49
4       Disabled                                                      49
5       Disabled                                                      49

Client Configuration:
=====================
Client   Authentication Method   Local Authentication Fallback
-------  ----------------------  -----------------------------
console  local                   Disabled
telnet   local                   Disabled
ssh      local                   Disabled
web      local                   Disabled
Auth>
```

auth timeout

This command displays or sets the time the switch waits for a reply from an authentication server before it resends the request.

SYNTAX

auth timeout [*timeout*]

timeout - The time the switch waits for a reply from an authentication server before it resends the request. (Range: 3-3600 seconds).

DEFAULT SETTING

15 seconds

EXAMPLE

```
Auth>timeout 10
Auth>
```

auth deadtime

This command displays or sets the time after which the switch considers an authentication server to be dead if it does not reply.

SYNTAX

auth deadtime [*dead-time*]

dead-time - The time after which the switch considers an authentication server to be dead if it does not reply. (Range: 0-3600 seconds)

DEFAULT SETTING

300 seconds

COMMAND USAGE

Setting the dead time to a value greater than 0 (zero) will cause the authentication server to be ignored until the dead time has expired. However, if only one server is enabled, it will never be considered dead.

EXAMPLE

```
Auth>deadtime 400
Auth>
```

auth radius

This command displays or sets RADIUS authentication server settings.

SYNTAX

auth radius [*server-index*] [**enable** | **disable**] [*ip-addr*] [*secret*] [*server-port*]

server-index - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.

enable - Enables the specified RADIUS authentication server.

disable - Disables the specified RADIUS authentication server.

ip-addr - IP address or IP alias of authentication server. An IPv4 address consists of 4 numbers, 0 to 255, separated by periods.

secret - Encryption key used to authenticate logon access for the client. (Maximum length: 29 characters)

server-port - Network (UDP) port of authentication server used for authentication messages. (Range: 0-65535, where 0 means that the switch will use the default port 1812)

To set an empty secret, use two quotes (“”). To use spaces in the secret, enquote the secret. Quotes in the secret are not allowed.

DEFAULT SETTING

Authentication: Disabled
Server Port: 1812

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 method and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via Telnet, SSH, or a web browser.

- When using RADIUS logon authentication, the user name and password must be configured on the authentication server. The encryption methods used for the authentication process must also be configured or negotiated between the authentication server and logon client. This switch can pass authentication messages between the server and client that have been encrypted using MD5 (Message-Digest 5), TLS (Transport Layer Security), or TTLS (Tunneled Transport Layer Security).

NOTE: This guide assumes that RADIUS servers have already been configured to support AAA. The configuration of RADIUS server software is beyond the scope of this guide. Refer to the documentation provided with the RADIUS and server software.

EXAMPLE

```
Auth>radius 1 enable 192.168.0.19 greenhills
Auth>radius

RADIUS Authentication Server Configuration:
=========================================
Server  Mode      IP Address       Secret                          Port
------  --------  ---------------  ------------------------------  -----
1       Enabled   192.168.0.19     **********                       1812
2       Disabled                                                    1812
3       Disabled                                                    1812
4       Disabled                                                    1812
5       Disabled                                                    1812
Auth>
```

auth acct_radius

This command displays or sets RADIUS accounting server settings.

SYNTAX

auth acct_radius [*server-index*] [**enable | disable**] [*ip-addr*] [*secret*] [*server-port*]

server-index - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.

enable - Enables the specified RADIUS accounting server.

disable - Disables the specified RADIUS accounting server.

ip-addr - IP address or IP alias of accounting server. An IPv4 address consists of 4 numbers, 0 to 255, separated by periods.

secret - Encryption key shared between the accounting server and the switch. (Maximum length: 29 characters)

server-port - Network (UDP) port of accounting server used for accounting messages. (Range: 0-65535, where 0 means that the switch will use the default port 1813)

To set an empty secret, use two quotes (“”). To use spaces in the secret, enquote the secret. Quotes in the secret are not allowed.

DEFAULT SETTING

Accounting: Disabled
Server Port: 1813

COMMAND USAGE

The switch supports the following accounting services:

- Accounting for users that access the Telnet, SSH or web management interfaces on the switch.
- Accounting for IEEE 802.1X authenticated users that access the network through the switch. This accounting can be used to provide reports, auditing, and billing for services that users have accessed.

EXAMPLE

```
Auth>acct_radius 1 enable 192.168.0.29 bluebird
Auth>acct_radius

RADIUS Accounting Server Configuration:
=======================================
Server  Mode      IP Address       Secret                          Port
------  --------  ---------------  ------------------------------  -----
1       Enabled   192.168.0.29     ********                         1813
2       Disabled                                                    1813
3       Disabled                                                    1813
4       Disabled                                                    1813
5       Disabled                                                    1813
Auth>
```

auth tacacs+

This command displays or sets TACACS+ authentication server settings.

SYNTAX

auth tacacs+ [*server-index*] [**enable | disable**] [*ip-addr*] [*secret*] [*server-port*]

server-index - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.

enable - Enables the specified TACACS+ authentication server.

disable - Disables the specified TACACS+ authentication server.

ip-addr - IP address or IP alias of authentication server. An IPv4 address consists of 4 numbers, 0 to 255, separated by periods.

secret - Encryption key used to authenticate logon access for the client. (Maximum length: 29 characters)

server-port - Network (UDP) port of authentication server used for authentication messages. (Range: 0-65535, where 0 means that the switch will use the default port 1812)

To set an empty secret, use two quotes (“”). To use spaces in the secret, enquote the secret. Quotes in the secret are not allowed.

DEFAULT SETTING

Authentication: Disabled
Server Port: 49

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 method and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via Telnet, SSH, or a web browser.

- When using TACACS+ logon authentication, the user name and password must be configured on the authentication server. The encryption methods used for the authentication process must also be configured or negotiated between the authentication server and logon client. This switch can pass authentication messages between the server and client that have been encrypted using MD5 (Message-Digest 5), TLS (Transport Layer Security), or TTLS (Tunneled Transport Layer Security).

NOTE: This guide assumes that RADIUS servers have already been configured to support AAA. The configuration of TACACS+ server software is beyond the scope of this guide. Refer to the documentation provided with the RADIUS and server software.

EXAMPLE

```
Auth>tacacs+ 1 enable 192.168.0.39 "no problem"
Auth>tacacs+

TACACS+ Authentication Server Configuration:
=============================================
Server  Mode      IP Address       Secret                          Port
------  --------  ---------------  ------------------------------  -----
1       Enabled   192.168.0.39     **********                        49
2       Disabled                                                    49
3       Disabled                                                    49
4       Disabled                                                    49
5       Disabled                                                    49
Auth>
```

auth client

This command displays or sets the authentication methods used for each management access protocol.

SYNTAX

auth client [**console** | **telnet** | **ssh** | **web**] [**none** | **local** | **radius** | **tacacs+**] [**enable** | **disable**]

console - Settings for console port.

telnet - Settings for Telnet.

ssh - Settings for SSH.

web - Settings for HTTP or HTTPS.

none - Disables access for the specified management protocol.

local - Authenticates through the local database.

radius - Authenticates through RADIUS.

tacacs+ - Authenticates through TACACS+.

enable - Enables fallback to local authentication if remote authentication fails. If authentication fallback is enabled, the switch uses the local user database for authentication if none of the configured authentication servers are alive. This is only possible if the authentication method is set to something else than **none** or **local**.

disable - Disables fallback local authentication if remote authentication fails.

DEFAULT SETTING

Authentication Method: local
Local Authentication Fallback: disabled

EXAMPLE

```
Auth>client telnet radius enable
Auth>client

Client Configuration:
=====================
Client   Authentication Method   Local Authentication Fallback
-------  ----------------------  -----------------------------
console  local                   Disabled
telnet   RADIUS                  Enabled
ssh      local                   Disabled
web      local                   Disabled
Auth>
```

auth statistics

This command displays statistics for configured authentication and accounting servers. The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

SYNTAX

auth statistics

COMMAND USAGE

For a description of the items displayed, refer to "Displaying Statistics for Configured Authentication Servers" on page 146.

EXAMPLE

```
Auth>statistics

Server #1 (0.0.0.0:1812) RADIUS Authentication Statistics:
Rx Access Accepts:                    0   Tx Access Requests:                0
Rx Access Rejects:                    0   Tx Access Retransmissions:         0
Rx Access Challenges:                 0   Tx Pending Requests:               0
Rx Malformed Acc. Responses:          0   Tx Timeouts:                       0
Rx Bad Authenticators:                0
Rx Unknown Types:                     0
Rx Packets Dropped:                   0
State:                         Disabled
Round-Trip Time:                      0 ms

Server #1 (192.168.0.29:1813) RADIUS Accounting Statistics:
Rx Responses:                         0   Tx Requests:                       0
Rx Malformed Responses:               0   Tx Retransmissions:                0
Rx Bad Authenticators:                0   Tx Pending Requests:               0
Rx Unknown Types:                     0   Tx Timeouts:                       0
Rx Packets Dropped:                   0
State:                           Ready
Round-Trip Time:                      0 ms

Server #2 (0.0.0.0:1812) RADIUS Authentication Statistics:
Rx Access Accepts:                    0   Tx Access Requests:                0
Rx Access Rejects:                    0   Tx Access Retransmissions:         0
Rx Access Challenges:                 0   Tx Pending Requests:               0
Rx Malformed Acc. Responses:          0   Tx Timeouts:                       0
Rx Bad Authenticators:                0
Rx Unknown Types:                     0
Rx Packets Dropped:                   0
```

```
State:                          Disabled
Round-Trip Time:                       0 ms

Server #2 (0.0.0.0:1813) RADIUS Accounting Statistics:
Rx Responses:                          0   Tx Requests:                       0
Rx Malformed Responses:                0   Tx Retransmissions:                0
Rx Bad Authenticators:                 0   Tx Pending Requests:               0
Rx Unknown Types:                      0   Tx Timeouts:                       0
Rx Packets Dropped:                    0
State:                          Disabled
Round-Trip Time:                       0 ms

Server #3 (0.0.0.0:1812) RADIUS Authentication Statistics:
Rx Access Accepts:                     0   Tx Access Requests:                0
Rx Access Rejects:                     0   Tx Access Retransmissions:         0
Rx Access Challenges:                  0   Tx Pending Requests:               0
Rx Malformed Acc. Responses:           0   Tx Timeouts:                       0
Rx Bad Authenticators:                 0
Rx Unknown Types:                      0
Rx Packets Dropped:                    0
State:                          Disabled
Round-Trip Time:                       0 ms

Server #3 (0.0.0.0:1813) RADIUS Accounting Statistics:
Rx Responses:                          0   Tx Requests:                       0
Rx Malformed Responses:                0   Tx Retransmissions:                0
Rx Bad Authenticators:                 0   Tx Pending Requests:               0
Rx Unknown Types:                      0   Tx Timeouts:                       0
Rx Packets Dropped:                    0
State:                          Disabled
Round-Trip Time:                       0 ms

Server #4 (0.0.0.0:1812) RADIUS Authentication Statistics:
Rx Access Accepts:                     0   Tx Access Requests:                0
Rx Access Rejects:                     0   Tx Access Retransmissions:         0
Rx Access Challenges:                  0   Tx Pending Requests:               0
Rx Malformed Acc. Responses:           0   Tx Timeouts:                       0
Rx Bad Authenticators:                 0
Rx Unknown Types:                      0
Rx Packets Dropped:                    0
State:                          Disabled
Round-Trip Time:                       0 ms

Server #4 (0.0.0.0:1813) RADIUS Accounting Statistics:
Rx Responses:                          0   Tx Requests:                       0
Rx Malformed Responses:                0   Tx Retransmissions:                0
Rx Bad Authenticators:                 0   Tx Pending Requests:               0
Rx Unknown Types:                      0   Tx Timeouts:                       0
Rx Packets Dropped:                    0
State:                          Disabled
Round-Trip Time:                       0 ms

Server #5 (0.0.0.0:1812) RADIUS Authentication Statistics:
Rx Access Accepts:                     0   Tx Access Requests:                0
Rx Access Rejects:                     0   Tx Access Retransmissions:         0
Rx Access Challenges:                  0   Tx Pending Requests:               0
Rx Malformed Acc. Responses:           0   Tx Timeouts:                       0
Rx Bad Authenticators:                 0
Rx Unknown Types:                      0
Rx Packets Dropped:                    0
State:                          Disabled
Round-Trip Time:                       0 ms

Server #5 (0.0.0.0:1813) RADIUS Accounting Statistics:
Rx Responses:                          0   Tx Requests:                       0
Rx Malformed Responses:                0   Tx Retransmissions:                0
```

```
Rx Bad Authenticators:                0   Tx Pending Requests:                0
Rx Unknown Types:                     0   Tx Timeouts:                        0
Rx Packets Dropped:                   0
State:                           Disabled
Round-Trip Time:                      0 ms
Auth>
```

12 PORT COMMANDS

This section describes commands used to configure connection parameters for ports, power saving mode, and cable testing.

Table 19: Port Commands

Command	Function
port configuration	Displays configuration settings
port state	Displays or sets administrative state to enabled or disabled
port mode	Displays or sets port speed and duplex mode
port flow control	Displays or sets flow control mode
port maxframe	Displays or sets the maximum frame size
port power	Displays or sets the power provided to ports based on the length of the cable used to connect to other devices
port excessive	Displays or sets the response to take when excessive transmit collisions are detected on a port
port statistics	Displays port statistics
port veriphy	Performs cable diagnostics
port numbers	Shows port numbering

port configuration

This command displays the configuration settings for all ports, a specific port, or a range of ports.

SYNTAX

port configuration [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

DEFAULT SETTING

All ports

COMMAND USAGE

The fields shown by this command are described below:

Table 20: Port Configuration

Field	Description
Port	Port index
State	Administrative state (Enabled or Disabled)
Mode	Port speed and duplex mode (speed/duplex mode or Auto)

Table 20: Port Configuration (Continued)

Field	Description
Flow Control	Flow control mode (Enabled or Disabled)
MaxFrame	Maximum frame size
Power	Power saving mode (Enabled or Disabled)
Excessive	Response to take when excessive transmit collisions are detected on a port (Discard frame or Restart backoff algorithm)
Link	Link status (connection speed/duplex mode or down)

EXAMPLE

```
Port>configuration

Port  State     Mode    Flow Control  MaxFrame  Power     Excessive  Link
----  --------  ------  ------------  --------  --------  ---------  ----
1     Enabled   Auto    Disabled      9600      Disabled  Discard    100fdx
2     Enabled   Auto    Disabled      9600      Disabled  Discard    100fdx
3     Enabled   1Gfdx   Disabled      9600      Disabled  Discard    Down
4     Enabled   Auto    Disabled      9600      Disabled  Discard    Down
5     Enabled   Auto    Disabled      9600      Disabled  Discard    Down
6     Enabled   Auto    Disabled      9600      Disabled  Discard    Down
7     Enabled   Auto    Disabled      9600      Disabled  Discard    Down
8     Enabled   Auto    Disabled      9600      Disabled  Discard    Down
9     Enabled   Auto    Disabled      9600      Disabled  Discard    Down
10    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
11    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
12    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
13    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
14    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
15    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
16    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
17    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
18    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
19    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
20    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
21    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
22    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
23    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
24    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
25    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
26    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
27    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
28    Enabled   Auto    Disabled      9600      Disabled  Discard    Down
Port>
```

port state

This command displays the administrative state, or sets it enabled or disabled.

SYNTAX

port state [*port-list*] [**enable** | **disable**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

enable - Enables the specified ports.

disable - Disables the specified ports.

DEFAULT SETTING

Enabled

COMMAND USAGE

This command allows you to disable a port due to abnormal behavior (e.g.,excessive collisions), and then re-enable it after the problem has been resolved. You may also want to disable a port for security reasons.

EXAMPLE

```
Port>state 5 disable
Port>
```

port mode

This command displays or sets port speed and duplex mode of a port.

SYNTAX

port mode [*port-list*] [**10hdx** | **10fdx** | **100hdx** | **100fdx** | **1000fdx** | **auto**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

10hdx - Supports 10 Mbps half-duplex operation

10fdx - Supports 10 Mbps full-duplex operation

100hdx - Supports 100 Mbps half-duplex operation

100fdx - Supports 100 Mbps full-duplex operation

1000fdx - Supports 1 Gbps full-duplex operation

auto - Enables auto-negotiation. When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities.

DEFAULT SETTING

Auto-negotiation

COMMAND USAGE

NOTE: The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.

EXAMPLE

```
Port>mode 5 100hdx
Port>mode 5

Port  Mode    Link
----  ------  ----
5     100hdx  Down
Port>
```

port flow control

This command displays or sets the flow control mode.

SYNTAX

port flow control [*port-list*] [**enable | disable**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

enable - Enables flow control.

disable - Disables flow control.

DEFAULT SETTING

Disabled

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 802.3-2005 (formally IEEE 802.3x) for full-duplex operation.

- When auto-negotiation is used, this parameter indicates the flow control capability advertised to the link partner. When the speed and duplex mode are manually set, the Rx Pause field indicates whether pause frames are obeyed by this port, and the Tx Pause field indicates if pause frames are transmitted from this port (as shown in the following example).

- 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

```
Port>flow control 5 enable
Port>flow control 5

Port  Flow Control  Rx Pause  Tx Pause
----  ------------  --------  --------
5     Enabled       Enabled   Enabled

Port>
```

port maxframe

This command displays or sets the maximum frame size allowed for a port.

SYNTAX

port maxframe [*port-list*] [*max-frame*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

max-frame - The maximum transfer unit for traffic crossing a port. (Range: 9600-1518 bytes)

DEFAULT SETTING

9600 bytes

EXAMPLE

```
Port>maxframe 5 1518
Port>
```

port power

This command displays or sets the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements.

SYNTAX

port power [*port-list*] [**enable** | **disable** | **actiphy** | **perfectreach**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

enable - Both link up and link down power savings enabled.

disable - All power savings mechanisms disabled.

actiphy - Link down power savings enabled.

perfectreach - Link up power savings enabled.

DEFAULT SETTING

Disabled

COMMAND USAGE

IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters.

Enabling power saving mode can significantly reduce power used for cable lengths of 20 meters or less, and continue to ensure signal integrity.

EXAMPLE

This example indicates that power usage for port 5 is 41% of normal.

```
Port>power 5 enable
Port>power 5

Port  Power     Usage
----  --------  -----
5     Enabled   41 %
Port>
```

port excessive

This command displays or sets the response to take when excessive transmit collisions are detected on a port.

SYNTAX

port excessive [*port-list*] [**discard** | **restart**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

discard - Discards a frame after 16 collisions.

restart - Restarts the backoff algorithm after 16 collisions.

DEFAULT SETTING

Discard

EXAMPLE

```
Port>excessive 5 restart
Port>
```

port statistics

This command displays port statistics.

SYNTAX

port statistics [*port-list*] [**clear**] [*statistic*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

clear - Clears port statistics

statistic - Specifies the statistics to display.

packets - The number of packets received and transmitted.

bytes - The number of bytes received and transmitted.

errors - The number of frames received with errors and the number of incomplete transmissions.

discards - The number of frames discarded due to ingress or egress congestion.

filtered - The number of received frames filtered by the forwarding process.

low - The number of packets received and transmitted through the low-priority queue.

normal - The number of packets received and transmitted through the normal-priority queue.

medium - The number of packets received and transmitted through the medium-priority queue.

high - The number of packets received and transmitted through the high-priority queue.

DEFAULT SETTING

Displays all statistics for all ports.

EXAMPLE

```
Port>statistics 1
Port 1 Statistics:

Rx Packets:                      38   Tx Packets:                     751
Rx Octets:                     5503   Tx Octets:                    49003
Rx Unicast:                       0   Tx Unicast:                       0
Rx Multicast:                    18   Tx Multicast:                   734
Rx Broadcast:                    17   Tx Broadcast:                    17
Rx Pause:                         0   Tx Pause:                         0

Rx 64:                           18   Tx 64:                          736
Rx 65-127:                       12   Tx 65-127:                       12
Rx 128-255:                       5   Tx 128-255:                       3
Rx 256-511:                       0   Tx 256-511:                       0
Rx 512-1023:                      3   Tx 512-1023:                      0
Rx 1024-1526:                     0   Tx 1024-1526:                     0
Rx 1527-    :                     0   Tx 1527-    :                     0

Rx Low:                          17   Tx Low:                          17
Rx Normal:                        0   Tx Normal:                        0
Rx Medium:                        0   Tx Medium:                        0
```

```
Rx High:                          18   Tx High:                         734

Rx Drops:                          2   Tx Drops:                          0
Rx CRC/Alignment:                  3   Tx Late/Exc. Coll.:                0
Rx Undersize:                      0
Rx Oversize:                       0
Rx Fragments:                      0
Rx Jabbers:                        0
Rx Filtered:                       0
Port>
```

port veriphy

This command performs cable diagnostics to diagnose any cable faults (short, open, etc.) and report the cable length.

SYNTAX

port veriphy [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

DEFAULT SETTING

Performs diagnostics for all ports.

COMMAND USAGE

- If a specific port is selected, the test will take approximately 5 seconds. If all ports are selected, it can run approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables 7 - 140 meters long.
- Potential conditions which may be listed by the diagnostics include:
  - OK : Correctly terminated pair
  - Open : Open pair, no link partner
  - Short : Short pair,
  - Abnormal : Terminating Impedance is not in the reference range.
  - Short x : Cross-pair short to pair x
  - Cross x : Abnormal cross-pair coupling, pair x
- Ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a management port will cause the switch to stop responding until testing is completed.

EXAMPLE

This example shows the cable length, operating conditions and isolates a variety of common faults that can occur on Category 5 twisted pair cabling.

```
Port>veriphy 1-10
Starting VeriPHY, please wait
Port   Pair A   Length   Pair B   Length   Pair C   Length   Pair D   Length
-----  -------  -------  -------  -------  -------  -------  -------  ------
1      OK       3        OK       3        Open     2        Open     2
2      OK       14       OK       14       Abnormal 3        Abnormal 3
3      Open     0        Open     0        Short    0        Short    0
4      Open     0        Open     0        Open     0        Open     0
5      Open     0        Open     0        Open     0        Open     0
6      Open     0        Open     0        Open     0        Open     0
7      Open     0        Open     0        Open     0        Open     0
8      Open     0        Open     0        Open     0        Open     0
9      Open     0        Open     0        Open     0        Open     0
10     Open     0        Open     0        Open     0        Open     0
Port>
```

port numbers

This command shows the port numbering on the front panel of the switch.

SYNTAX

port numbers

EXAMPLE

```
Port>numbers
Port Numbers:

+-------------------------------------------------------------+
| +--+--+--+--+ +--+--+--+--+ +--+--+--+--+   +----+   +----+ |
| | 1| 3| 5| 7| | 9|11|13|15| |17|19|21|23|   | 27 |   | 28 | |
| +--+--+--+--+ +--+--+--+--+ +--+--+--+--+   +----+   +----+ |
| | 2| 4| 6| 8| |10|12|14|16| |18|20|22|24|   | 25 |   | 26 | |
| +--+--+--+--+ +--+--+--+--+ +--+--+--+--+   +----+   +----+ |
+-------------------------------------------------------------+
Port>
```

13 LINK AGGREGATION COMMANDS

This section describes commands used to configures static port aggregation, including member assignment, and load balancing methods.

Table 21: Link Aggregation Commands

Command	Function
aggr configuration	Displays configuration settings for all link aggregation groups
aggr add	Adds or modifies member ports for a link aggregation group
aggr delete	Deletes a link aggregation group
aggr lookup	Displays information on the specified link aggregation group
aggr mode	Selects the load-balance method to apply to all link aggregation groups on the switch

USAGE GUIDELINES

- 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 switches.

- 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.

- 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, configure 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 14 trunks on a switch, with up to 16 ports per trunk.

  - The ports at both ends of a connection must be configured as trunk ports.

- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

aggr configuration

This command displays configuration settings for all link aggregation groups.

SYNTAX

aggr configuration

EXAMPLE

```
Aggr>configuration
Aggregation Mode:

SMAC  : Enabled
DMAC  : Disabled
IP    : Enabled
Port  : Enabled

Aggr ID  Name    Type    Configured Ports  Aggregated Ports
-------  ------  ------  ----------------  ----------------
1        LLAG1   Static  4-7               4,5
Aggr>
```

aggr add

This command adds or modifies member ports for a link aggregation group.

SYNTAX

aggr add *port-list* [*aggr-id*]

port-list - A specific port or a range of ports. (Range: 1-28)

aggr-id - Trunk identifier. If not specified, the next available aggregation ID is used. (Range: 1-14)

DEFAULT SETTING

The next available aggregation ID is used if not specified.

COMMAND USAGE

To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports.

EXAMPLE

```
Aggr>add 4-8 1
Aggr>configuration
Aggregation Mode:

SMAC  : Enabled
DMAC  : Disabled
IP    : Enabled
Port  : Enabled

Aggr ID  Name    Type    Configured Ports  Aggregated Ports
-------  ------  ------  ----------------  ----------------
1        LLAG1   Static  4-8               4,5
Aggr>
```

aggr delete

This command deletes a link aggregation group.

SYNTAX

aggr delete *aggr-id*

aggr-id - Trunk identifier. (Range: 1-14)

COMMAND USAGE

To avoid creating a loop in the network, be sure you disconnect the ports before removing a static trunk via the configuration interface.

EXAMPLE

```
Aggr>delete 2
Aggr>
```

aggr lookup

This command displays information on the specified link aggregation group.

SYNTAX

aggr lookup [*aggr-id*]

aggr-id - Trunk identifier. (Range: 1-14)

DEFAULT SETTING

Displays information for all link aggregation groups.

EXAMPLE

```
Aggr>lookup 2

Aggr ID  Name    Type    Configured Ports  Aggregated Ports
-------  ------  ------  ----------------  ----------------
2        LLAG2   Static  9,10              None
Aggr>
```

aggr mode

This command selects the load-balance method to apply to all link aggregation groups on the switch. If more than one option is selected, each factor is used in the hash algorithm to determine the port member within the trunk to which a frame will be assigned.

SYNTAX

aggr mode [**smac** | **dmac** | **ip** | **port**] [**enable** | **disable**]

smac (Source MAC Address) - All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts.

dmac (Destination MAC Address) - All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.

ip (IP Address) - All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.

port (TCP/UDP Port Number) - All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk. Avoid using his mode as a lone option. It may overload a single port member of the trunk for application traffic of a specific type, such as web browsing. However, it can be used effectively in combination with the IP Address option.

enable - Enables the specified methods for traffic distribution.

disable - Disables the specified methods for traffic distribution.

DEFAULT SETTING

Source MAC Address
IP Address
TCP/UDP Port Number

COMMAND USAGE

When incoming data frames are forwarded through the switch to a trunk, the switch must determine to which port link in the trunk an outgoing frame should be sent. To maintain the frame sequence of various traffic flows between devices in the network, the switch also needs to ensure that frames in each "conversation" are mapped to the same trunk link. To achieve this requirement and to distribute a balanced load across all links in a trunk, the switch uses a hash algorithm to calculate an output link number in the trunk. However, depending on the device to which a trunk is connected and the traffic flows in the network, this load-balance algorithm may result in traffic being distributed mostly on one port in a trunk. To ensure that the switch traffic load is distributed evenly across all links in a trunk, the hash method used in the load-balance calculation can be selected to provide the best result for trunk connections.

EXAMPLE

```
Aggr>mode port disable
Aggr>mode
Aggregation Mode:

SMAC  : Enabled
DMAC  : Disabled
IP    : Enabled
Port  : Disabled
Aggr>
```

14 LACP COMMANDS

This section describes commands used to configures the Link Aggregation Control Protocol.

Table 22: LACP Commands

Command	Function
lacp configuration	Displays LACP configuration settings for specified ports
lacp mode	Displays or sets LACP mode for specified ports
lacp key	Displays or sets the LACP administration key for specified ports
lacp role	Displays or sets the LACP initiation mode for specified ports
lacp status	Displays the operational status for specified ports
lacp statistics	Displays LACP statistics for specified ports

USAGE GUIDELINES

- 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 switches.

- The switch supports dynamic Link Aggregation Control Protocol (LACP). 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 to use LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured to use LACP, the switch and the other device will negotiate a trunk between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

- 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, configure the trunk on the devices at both ends. When using a port trunk, take note of the following points:

  - 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.

  - You can create up to 12 trunks on a switch, with up to 28 ports per trunk.

- The ports at both ends of a connection must be configured as trunk ports.
- 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.
- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

◆ 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, either by forced mode or auto-negotiation.

◆ Ports assigned to a common link aggregation group (LAG) must meet the following criteria:

- Ports must have the same LACP administration key. Using auto-configuration of the administration key will avoid this problem.
- One of the ports at either the near end or far end must be set to active initiation mode.

lacp configuration

This command displays the LACP configuration settings for specified ports.

SYNTAX

lacp configuration [*port-list*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

EXAMPLE

In the following example, Key refers to the LACP administration key, and Role to the protocol initiation mode.

```
LACP>configuration 1-10

Port  Mode      Key   Role
----  --------  ----  ------
1     Disabled  Auto  Active
2     Disabled  Auto  Active
3     Disabled  Auto  Active
4     Enabled   Auto  Active
5     Enabled   Auto  Active
6     Enabled   Auto  Active
7     Enabled   Auto  Active
8     Disabled  Auto  Active
9     Disabled  Auto  Active
10    Disabled  Auto  Active
LACP>
```

lacp mode

This command displays or sets the LACP mode for specified ports.

SYNTAX

lacp mode *port-list* [**enable** | **disable**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

enable - Enables LACP.

disable - Disables LACP.

DEFAULT SETTING

Disabled

COMMAND USAGE

This command controls whether LACP is enabled a switch port. LACP will form an aggregation when two or more ports are connected to the same partner. LACP can form up to 12 LAGs per switch.

EXAMPLE

```
LACP>mode 4-7 enable
LACP>mode 1-10

Port  Mode
----  --------
1     Disabled
2     Disabled
3     Disabled
4     Enabled
5     Enabled
6     Enabled
7     Enabled
8     Disabled
9     Disabled
10    Disabled
LACP>
```

lacp key

This command displays or sets the LACP administration key for specified ports.

SYNTAX

lacp key [*port-list*] [*key*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

key - LACP administration key. The key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535, or auto)

DEFAULT SETTING

auto - A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.

EXAMPLE

```
LACP>key 11-15 5
LACP>
```

lacp role

This command displays or sets the LACP initiation mode for specified ports.

SYNTAX

lacp role [*port-list*] [**active** | **passive**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

active - Sends LACP negotiation packets (once each second).

passive - Waits until it receives an LACP protocol packet from a partner before starting negotiations,

DEFAULT SETTING
Active

EXAMPLE

```
LACP>role 11-15 passive
LACP>
```

lacp status

This command displays the operational status for specified ports.

SYNTAX

lacp status [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

EXAMPLE

```
LACP>status 1-10
Aggr ID  Partner System ID  Partner Key  Last Changed   Ports
-------  -----------------  -----------  -------------  -----
1        00-30-fc-12-34-56  3            01:34:46       4,5

Port  Mode      Key    Aggr ID  Partner System ID  Partner Port
----  --------  -----  -------  -----------------  ------------
1     Disabled  2      -        -                  -
2     Disabled  2      -        -                  -
3     Disabled  1      -        -                  -
4     Enabled   2      1        00-30-fc-12-34-56  2
5     Enabled   2      1        00-30-fc-12-34-56  1
6     Disabled  1      -        -                  -
7     Disabled  1      -        -                  -
8     Disabled  1      -        -                  -
9     Disabled  1      -        -                  -
10    Disabled  1      -        -                  -
LACP>
```

lacp statistics

This command displays LACP statistics for specified ports.

SYNTAX

lacp status [*port-list*] [clear]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

clear - Clears LACP statistics.

EXAMPLE

This example shows the number of LACP frames received and transmitted, as well as the number of unknown or illegal LACP frames that have been discarded.

```
LACP>statistics 4-5

Port  Rx Frames   Tx Frames   Rx Unknown  Rx Illegal
----  ----------  ----------  ----------  ----------
4     5942        6136        0           0
5     5942        6136        0           0
LACP>
```

15 RSTP COMMANDS

This section describes commands used to configure the Rapid Spanning Tree Protocol.

Table 23: RSTP Commands

Command	Function
rstp configuration	Displays RSTP configuration settings for specified interfaces
rstp sysprio	Displays or sets RSTP system priority
rstp age	Displays or sets RSTP maximum age
rstp delay	Displays or sets RSTP forward delay
rstp txhold	Displays or sets RSTP Transmit Hold Count
rstp version	Displays or sets RSTP protocol version (RSTP or STP-compatible)
rstp mode	Displays or sets RSTP administrative mode for specified interfaces
rstp cost	Displays or sets RSTP path cost for specified interfaces
rstp priority	Displays or sets RSTP priority for specified interfaces
rstp edge	Displays or sets RSTP edge port for specified ports
rstp autoedge	Displays or sets RSTP automatic edge detection for specified ports
rstp p2p	Displays or sets RSTP point-to-point link type for specified ports
rstp status	Displays RSTP operational status for the bridge and any specified ports or link aggregation groups
rstp statistics	Displays RSTP statistics on protocol messages for any specified ports or link aggregation groups
rstp mcheck	Performs RSTP protocol migration check for specified ports

rstp configuration

This command displays RSTP configuration settings for specified interfaces.

SYNTAX

rstp configuration [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, **all** for all ports, or 0 for all link aggregation groups)

EXAMPLE

In the following example, Key refers to the LACP administration key, and Role to the protocol initiation mode.

```
RSTP>configuration 1-5
System Priority : 32768
Max Age         : 20
Forward Delay   : 15
Tx Hold Count   : 6
Protocol Version: Normal (RSTP)

Port  Mode      Path Cost   Priority  AdminEdge AutoEdge  Point2point
----  --------  ----------  --------  ----------------  -----------
1     Enabled   Auto        128       Enabled   Enabled   Auto
2     Enabled   Auto        128       Enabled   Enabled   Auto
3     Enabled   Auto        128       Enabled   Enabled   Auto
4     Enabled   Auto        128       Enabled   Enabled   Auto
5     Enabled   Auto        128       Enabled   Enabled   Auto
RSTP>
```

rstp sysprio

This command Displays or sets RSTP system priority.

SYNTAX

rstp sysprio [*system-priority*]

system-priority - Bridge priority used in selecting the root device, root port, and designated port. (Options: 0-61440, in steps of 4096)

DEFAULT SETTING

32768

COMMAND USAGE

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.

EXAMPLE

```
RSTP>syspri 40960
RSTP>
```

rstp age

This command displays or sets RSTP maximum age.

SYNTAX

rstp age [*maximum-age*]

maximum-age - The maximum time a device can wait without receiving a configuration message before attempting to reconfigure. (Range: 6-40 seconds)

Minimum: The higher of 6 or [2 x (Hello Time + 1)]
Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

DEFAULT SETTING

20 seconds

COMMAND USAGE

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. (Note that references to "ports" in this section mean "interfaces," which includes both ports and trunks.)

EXAMPLE

```
RSTP>age 28
RSTP>
```

rstp delay

This command displays or sets RSTP forward delay.

SYNTAX

rstp delay [*forward-delay*]

forward-delay - The maximum time this device will wait before changing states (i.e., discarding to learning to forwarding). (Range: 4-30 seconds)

Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
Maximum: 30

DEFAULT SETTING

15

COMMAND USAGE

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.

EXAMPLE

```
RSTP>delay 20
RSTP>
```

rstp txhold

This command displays or sets RSTP Transmit Hold Count.

SYNTAX

rstp txhold [*transmit-hold*]

transmit-hold - The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. (Range: 1-10)

DEFAULT SETTING

6

EXAMPLE

```
RSTP>txhold 10
RSTP>
```

rstp version

This command displays or sets the type of spanning tree used on this switch (RSTP or STP-compatible).

SYNTAX

rstp version [**compatible** | **normal**]

compatible - Compatible with STP.

normal - RSTP

DEFAULT SETTING

Normal

COMMAND USAGE

- RSTP supports connections to either RSTP or STP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
- In normal 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.
- In compatible 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.

EXAMPLE

```
RSTP>version compatible
RSTP>
```

rstp mode

This command displays or sets RSTP administrative mode for specified interfaces.

SYNTAX

rstp mode [*port-list*] [**enable** | **disable**]

port-list - A specific port or a range of ports. (Range: 1-28, **all** for all ports, or 0 for all link aggregation groups)

enable - Enables RSTP.

disable - Disables RSTP.

DEFAULT SETTING

Enabled

EXAMPLE

```
RSTP>mode 19 disable
RSTP>
```

rstp cost

This command displays or sets RSTP path cost for specified interfaces.

SYNTAX

rstp cost [*port-list*] [*path-cost*]

port-list - A specific port or a range of ports. (Range: 1-28, **all** for all ports, or 0 for all link aggregation groups)

path-cost - The path cost for an interface. (Range: 1-200000000, or auto for auto-configuration)

DEFAULT SETTING

Auto-configuration

COMMAND USAGE

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.)

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

Table 24: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 25: Recommended STA Path Costs

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Table 26: Default STA Path Costs

Port Type	Link Type	IEEE 802.1w-2001
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

EXAMPLE

```
RSTP>cost 19 50
RSTP>
```

rstp priority

This command displays or sets RSTP priority for specified interfaces.

SYNTAX

rstp priority [*port-list*] [*priority*]

port-list - A specific port or a range of ports. (Range: 1-28, **all** for all ports, or 0 for all link aggregation groups)

priority - The priority for an interface. (Range: 0-240, in steps of 16)

DEFAULT SETTING

128

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 (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.

EXAMPLE

```
RSTP>priority 19 0
RSTP>
```

rstp edge

This command displays or sets an edge port to enable fast forwarding.

SYNTAX

rstp edge [*port-list*] [**enable** | **disable**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

enable - Enables interface as an edge port.

disable - Disables interface as an edge port.

DEFAULT SETTING

Enabled

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 re-configuration events, does not cause the spanning tree to initiate re-configuration when the interface changes state, and also

overcomes other STA-related time-out problems. However, remember that this feature should only be enabled for ports connected to an end-node device.

EXAMPLE

```
RSTP>edge 19 enable
RSTP>
```

rstp autoedge

This command displays or sets RSTP automatic edge port detection for specified ports.

SYNTAX

rstp autoedge [*port-list*] [**enable** | **disable**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

enable - Enables automatic edge port detection.

disable - Disables automatic edge port detection.

DEFAULT SETTING

Enabled

COMMAND USAGE

This command controls whether automatic edge detection is enabled on a bridge port. When enabled, the bridge can determine that a port is at the edge of the network if no BPDU's received on the port.

EXAMPLE

```
RSTP>autoedge 19 enable
RSTP>
```

rstp p2p

This command displays or sets RSTP point-to-point link type for specified ports.

SYNTAX

rstp p2p [*port-list*] [**enable** | **disable** | **auto**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

enable - Specifies a point-to-point connection to exactly one other bridge.

disable - Specifies a shared 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 medium.

DEFAULT SETTING

Automatic detection

COMMAND USAGE

- The link type attached to an interface can be set to automatically detect the link type, or manually configured as point-to-point or shared medium. Transition to the forwarding state is faster for point-to-point links than for shared media.
- 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.

EXAMPLE

```
RSTP>p2p 19 enable
RSTP>
```

rstp status

This command displays RSTP operational status for the bridge, specified ports, and any link aggregation groups.

SYNTAX

rstp status [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

EXAMPLE

This example displays RSTP status for the bridge, for port 1 and for LAG 1. For a description of the items displayed in this example, refer to "Displaying Bridge Status for STA" on page 152 and "Displaying Port Status for STA" on page 154.

```
RSTP>status 1
RSTP Bridge Status
Bridge ID    : 40960-00:01:C1:00:00:E1
Root ID      : 32768-00:01:EC:F8:D8:C6
Root Port    : 1
Root Cost    : 200000
TC Flag      : Steady
TC Count     : 161
TC Last      :   0d 01:10:47
Port       Port Role       State       Pri  PathCost  Edge  P2P  Uptime
---------  --------------  ----------  ---  --------  ----  ---  ------------
        1  DesignatedPort  Forwarding  128    200000  Yes   Yes    0d 03:03:10
    LLAG1  DesignatedPort  Forwarding  128    100000  No    Yes    0d 00:02:23
    LLAG2  DesignatedPort  Forwarding  128    100000  No    Yes    0d 00:00:21
RSTP>
```

rstp statistics

This command displays RSTP statistics on protocol messages for any specified ports and link aggregation groups.

SYNTAX

rstp statistics [*port-list*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

EXAMPLE

This example displays RSTP statistics for port 1 and LAG1. For a description of the items displayed in this example, refer to "Displaying Port Statistics for STA" on page 155.

```
RSTP>statistics 1
Port       Rx RSTP   Tx RSTP   Rx STP   Tx STP   Rx TCN   Tx TCN   Rx Ill.  Rx Unk.
---------  --------  --------  -------  -------  -------  -------  -------  -----
        1       943      8774     2587        3        0        1        0      0
    LLAG1         5      5041        1     2560        2        1        0      0
RSTP>
```

rstp mcheck

This command performs RSTP protocol migration check for specified ports.

SYNTAX

rstp mcheck [*port-list*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

COMMAND USAGE

- This command re-checks the appropriate BPDU format to send on the selected interface.
- 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 this 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

```
RSTP>mcheck
RSTP>
```

16 IEEE 802.1X COMMANDS

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). This section describes commands used to configure IEEE 802.1X Port Authentication.

Table 27: IEEE 802.1X Commands

Command	Function
dot1x configuration	Displays 802.1X settings for the switch and specified ports
dot1x mode	Displays or sets the 802.1X mode for the switch
dot1x state	Displays or sets the 802.1X authentication mode for specified ports
dot1x authenticate	Restarts the client authentication process for specified ports
dot1x reauthentication	Displays or sets periodic re-authentication for all ports
dot1x period	Displays or sets re-authentication period
dot1x timeout	Displays or sets the time between retransmitting EAP packets
dot1x clients	Displays or sets the maximum number of allowed clients for MAC-based ports
dot1x agetime	Displays or sets the time between checking for activity on successfully authenticated MAC addresses
dot1x holdtime	Displays or sets the hold time before MAC addresses that failed authentication expire
dot1x statistics	Displays 802.1X statistics

dot1x configuration

This command displays 802.1X settings for the switch and for specified ports.

SYNTAX

dot1x configuration [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

DEFAULT SETTING

All ports

COMMAND USAGE

The fields shown by this command are described below:

Table 28: 802.1X Configuration

Field	Description
Port	Port index
Admin State	Administrative state (Enabled or Disabled)
Port State	Operational state: • Disabled - 802.1X and MAC-based authentication are globally disabled. • Link Down - 802.1X or MAC-based authentication is enabled, but there is no link on the port. • Authorized - The port is authorized. This state exists when 802.1X authentication is enabled, the port has a link, the Admin State is "802.1X," and the supplicant is authenticated, or when the Admin State is "Authorized." • Unauthorized - The port is unauthorized. This state exists when 802.1X authentication is enabled, the port has a link, and the Admin State is "Auto," but the supplicant is not (or not yet) authenticated, or when the Admin State is "Unauthorized." • X Auth/Y Unauth - X clients are currently authorized and Y are unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to "MAC-Based."
Last Source	The source MAC address carried in the most recently received EAPOL frame for port-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame for port-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

EXAMPLE

```
Dot1x>configuration 1-10
Mode            : Enabled
Reauthentication: Disabled
Period          : 3600
Timeout         : 30
Age Period      : 300
Hold Time       : 10

Port  Admin State   Port State             Last Source        Last ID
----  ------------  ---------------------  -----------------  -------
1     Authorized    Authorized             -                  -
2     Authorized    Authorized             -                  -
3     Authorized    Link Down              -                  -
4     Authorized    Authorized             -                  -
5     Authorized    Authorized             -                  -
6     Authorized    Link Down              -                  -
7     Authorized    Link Down              -                  -
8     Authorized    Link Down              -                  -
9     Authorized    Link Down              -                  -
10    Authorized    Link Down              -                  -
Dot1x>
```

dot1x mode

This command displays or sets the 802.1X mode for the switch.

SYNTAX

dot1x mode [**enable** | **disable**]

enable - Enables 802.1X globally for the switch.

disable - Disables 802.1X globally for the switch.

DEFAULT SETTING

Disabled

COMMAND USAGE

This command configures 802.1X and MAC-based authentication globally on the switch. If globally disabled, all ports are allowed to forward frames.

EXAMPLE

```
Dot1x>mode enable
Dot1x>
```

dot1x state

This command displays or sets the 802.1X security state (i.e., authentication mode) for specified ports

SYNTAX

dot1x state [*port-list*] [**macbased** | **auto** | **authorized** | **unauthorized**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

macbased - Enables MAC-based authentication on the port. The switch does not transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic from an unsuccessfully authenticated client will be dropped. Clients that are not (or not yet) successfully authenticated will not be allowed to transmit frames of any kind.

auto - Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.

authorized - Forces the port to grant access to all clients, either dot1x-aware or otherwise.

unauthorized - Forces the port to deny access to all clients, either dot1x-aware or otherwise.

DEFAULT SETTING

Authorized

COMMAND USAGE

- The authentication mode can only be set to Authorized for ports participating in the Spanning Tree algorithm (see page 239).
- When 802.1X authentication is enabled on a port, the MAC address learning function for this interface is disabled, and the addresses dynamically learned on this port are removed from the common address table.
- Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table. Configured static MAC addresses are added to the secure address table when seen on a switch port (see the mac add command on page 272). Static addresses are treated as authenticated without sending a request to a RADIUS server.
- When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.

EXAMPLE

```
Dot1x>state 9 authorized
Dot1x>state 9

Port  Admin State   Port State            Last Source        Last ID
----  ------------  --------------------  -----------------  -------
9     Authorized    Link Down             -                  -
Dot1x>
```

dot1x authenticate

This command restarts the client authentication process for specified ports.

SYNTAX

dot1x authenticate [*port-list*] [**now**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

now - Forces re-initialization of the port/clients, and therefore immediately starts re-authentication. The port/clients are set to the unauthorized state while re-authentication is ongoing.

DEFAULT SETTING

None

COMMAND USAGE

- For port-based authentication, the re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected to the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.
- This command is only effective when 802.1X is globally enabled (using the dot1x mode command described on page 248) and the port's

authentication mode is set to "auto" or "macbased" (using the dot1x state command described on page 248).

EXAMPLE

```
Dot1x>authenticate 9
Dot1x>
```

dot1x reauthentication

This command displays or sets periodic re-authentication for all ports.

SYNTAX

dot1x reauthentication [**enable | disable**]

enable - Schedules reauthentication to whenever the quiet-period of the port runs out (port-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The process only effects successfully authenticated ports/clients and will not cause the port/client to be temporarily unauthorized.

disable - Disables 802.1X reauthentication.

DEFAULT SETTING

Disabled

COMMAND USAGE

- For port-based authentication, the re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected to the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.
- The connected client is re-authenticated after the interval specified by the dot1x period command (see page 251). The default is 3600 seconds.
- This command is only effective when 802.1X is globally enabled (using the dot1x mode command described on page 248) and the port's authentication mode is set to "auto" or "macbased" (using the dot1x state command described on page 248).

EXAMPLE

```
Dot1x>reauthentication enable
Dot1x>
```

dot1x period

This command displays or sets the re-authentication period.

SYNTAX

dot1x period [*reauth-period*]

reauth-period - The time after which a connected client must be re-authenticated. (Range: 1-3600 seconds)

DEFAULT SETTING

3600 seconds

EXAMPLE

```
Dot1x>period 300
Dot1x>
```

dot1x timeout

This command displays or sets the time the switch waits for a supplicant response during an authentication session before retransmitting an EAP packet.

SYNTAX

dot1x timeout [*eap-timeout*]

eap-timeout - The time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. (Range: 1-255 seconds)

DEFAULT SETTING

30 seconds

EXAMPLE

```
Dot1x>timeout 300
Dot1x>
```

dot1x clients

This command displays or sets the maximum number of allowed clients for MAC-based ports.

SYNTAX

dot1x clients [*port-list*] [**all** | *client-count*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

all - Allows all new clients.

client-count - The maximum number of hosts that can connect to a port when the 802.1x security state (i.e., authentication mode) is set to **macbased** by the dot1x state command. (Range: 1-112)

DEFAULT SETTING
Allows all new clients.

COMMAND USAGE
The switch has a fixed pool of state-machines, from which all ports draw whenever a new client is seen on the port. When a given port's maximum is reached (counting both authorized and unauthorized clients), further new clients are disallowed access. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available state-machines.

EXAMPLE

```
Dot1x>clients 9 10
Dot1x>
```

dot1x agetime

This command displays or sets the time between checking for activity on successfully authenticated MAC addresses.

SYNTAX

dot1x agetime [*age-time*]

age-time - The period used to calculate when to age out a client allowed access to the switch through MAC-based authentication as described below. (Range: 10-1000000 seconds)

DEFAULT SETTING
300 seconds

COMMAND USAGE
Suppose a client is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch that is running MAC-based authentication, and suppose the client gets successfully authenticated. Now assume that the client powers down his PC. What should make the switch forget about the authenticated client? Reauthentication will not solve this problem, since this doesn't require the client to be present, as discussed under Reauthentication Enabled above. The solution is aging out authenticated clients.

A timer is started when the client gets authenticated. After half the age period, the switch starts looking for frames sent by the client. If another half age period elapses and no frames are seen, the client is considered removed from the system, and it will have to authenticate again the next time a frame is seen from it. If, on the other hand, the client transmits a frame before the second half of the age period expires, the switch will consider the client alive, and leave it authenticated. Therefore, an age period of T will require the client to send frames more frequent than T/2 to stay authenticated.

EXAMPLE

```
Dot1x>agetime 900
Dot1x>
```

dot1x holdtime

This command displays or sets the hold time before MAC addresses that failed authentication expire.

SYNTAX

dot1x holdtime [*hold-time*]

hold-time - The time after an EAP Failure indication or RADIUS timeout that a client is not allowed access. This setting applies to ports running MAC-based authentication only. (Range: 10-1000000 seconds)

DEFAULT SETTING

10 seconds

COMMAND USAGE

If the RADIUS server denies a client access, or a RADIUS server request times out (according to the timeout period specified by the auth timeout command, page 206), the client is put on hold in the Unauthorized state. In this state, frames from the client will not cause the switch to attempt to re-authenticate the client.

EXAMPLE

```
Dot1x>holdtime 60
Dot1x>
```

dot1x statistics

This command displays IEEE 802.1X statistics and protocol information for specified ports.

SYNTAX

dot1x statistics [*port-list*] [**clear**] [**eapol** | **radius**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

clear - Clears 802.1X statistics

eapol - Shows IEEE 802.1X statistics for a specific switch port running port-based authentication.

radius - Shows statistics for the RADIUS authentication server (specified with the auth radius command described on page 207).

DEFAULT SETTING

Displays all statistics for all ports.

COMMAND USAGE

- For MAC-based ports, it shows only statistics for the backend RADIUS authentication server.
- For a description of the information displayed by command, see "Displaying Detailed Port Statistics" on page 142.

EXAMPLE

```
Dot1x>statistics 1

      Rx Access   Rx Other    Rx Auth.    Rx Auth.    Tx          MAC
Port  Challenges  Requests    Successes   Failures    Responses   Address
----  ----------  ----------  ----------  ----------  ----------  ----------
1     0           0           0           0           0           -
Dot1x>statistics 1

Port 1 EAPOL Statistics:

Rx Total:                           0   Tx Total:                           3
Rx Response/Id:                     0   Tx Request/Id:                      0
Rx Response:                        0   Tx Request:                         0
Rx Start:                           0
Rx Logoff:                          0
Rx Invalid Type:                    0
Rx Invalid Length:                  0

Port 1 Backend Server Statistics:

Rx Access Challenges:               0   Tx Responses:                       0
Rx Other Requests:                  0
Rx Auth. Successes:                 0
Rx Auth. Failures:                  0

Dot1x>
```

17 IGMP 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.

This section describes the commands used to configure IGMP snooping, query, throttling, and filtering.

Table 29: IGMP Commands

Command	Function
igmp configuration	Displays IGMP snooping settings for the switch, all VLANs, and specified ports
igmp mode	Displays or sets the IGMP snooping mode for the switch
igmp state	Displays or sets the IGMP snooping state for specified VLAN
igmp querier	Displays or sets the IGMP querier mode for specified VLAN
igmp fastleave	Displays or sets IGMP fast leave for specified ports
igmp leave proxy	Displays or sets IGMP leave proxy for the switch
igmp throttling	Displays or sets IGMP group throttling for specified ports
igmp filtering	Displays or sets IGMP group filtering for specified ports
igmp router	Displays or sets specified ports which are attached to a known IGMP router
igmp flooding	Displays or sets flooding of unregistered IGMP services
igmp groups	Displays active IGMP groups
igmp status	Displays IGMP querier status and protocol statistics

igmp configuration

This command displays IGMP snooping settings for the switch, all VLANs, and specified ports.

SYNTAX

igmp configuration [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

DEFAULT SETTING

All ports

COMMAND USAGE

The fields shown by this command are described below:

Table 30: IGMP Configuration

Field	Description
Global Settings	
IGMP Mode	Shows if IGMP snooping is enabled or disabled
IGMP Leave Proxy	Shows if leave messages are suppressed unless received from the last member port in the group
Flooding	Shows if unregistered multicast traffic is flooded into attached VLANs
VLAN Settings	
VID	VLAN identifier
State	Shows if IGMP snooping is enabled or disabled
Querier	Shows if the switch can serve as querier on this VLAN
Port Settings	
Port	Port identifier
Router	Shows if a port is set to function as a router port, which leads towards a Layer 3 multicast device or IGMP querier
Dynamic Router	Shows if the switch has detected a Layer 3 multicast device or IGMP querier on this port
Fast Leave	Shows if the switch immediately deletes a member port of a multicast service if a leave packet is received at that port
Group Throttling Number	Shows the number of multicast groups to which a port can belong
Filtering Groups	Shows the multicast groups that are denied on a port

EXAMPLE

```
IGMP>configuration 1-3
IGMP Mode: Disabled
IGMP Leave Proxy: Disabled
Flooding : Disabled

VID   State     Querier
----  --------  --------
1     Enabled   Disabled
2     Enabled   Disabled

Port  Router    Dynamic Router    Fast Leave  Group Throttling Number
----  --------  ----------------  ----------  ------------------------
1     Disabled    no              Disabled    Unlimited
2     Disabled    no              Disabled    Unlimited
3     Disabled    no              Disabled    Unlimited

Port  Filtering Groups
----  ------------------
1     No Filtering Group
2     No Filtering Group
3     No Filtering Group
IGMP>
```

igmp mode

This command displays or sets the IGMP snooping mode for the switch.

SYNTAX

igmp mode [**enable** | **disable**]

enable - Enables IGMP snooping globally for the switch. When IGMP snooping is enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.

disable - Disables IGMP snooping globally for the switch.

DEFAULT SETTING

Enabled

COMMAND USAGE

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.

EXAMPLE

```
IGMP>mode enable
IGMP>
```

igmp state

This command displays or sets the IGMP snooping state for the specified VLAN.

SYNTAX

igmp state [*vlan-id*] [**enable** | **disable**]

vlan-id - VLAN to which the management address is assigned. (Range: 1-4095)

enable - Enables IGMP snooping. When enabled, the switch will monitor network traffic on the indicated VLAN interface to determine which hosts want to receive multicast traffic.

disable - Disables IGMP snooping.

DEFAULT SETTING

Enabled

COMMAND USAGE

When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence. When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

EXAMPLE

```
IGMP>state enable
IGMP>
```

igmp querier

This command displays or sets the IGMP querier mode for the specified VLAN.

SYNTAX

igmp querier [*vlan-id*] [**enable** | **disable**]

vlan-id - VLAN to which the management address is assigned. (Range: 1-4095)

enable - Enables the switch to serve as querier on this VLAN. When enabled, the switch can serve as the querier if selected in the bidding process with other competing multicast switches/routers, and if selected will be responsible for asking hosts if they want to receive multicast traffic.

disable - Disables the switch from serving as querier on this VLAN.

DEFAULT SETTING

Disabled

COMMAND USAGE

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. This feature is not supported for IGMPv3 snooping.

EXAMPLE

```
IGMP>querier 1 enable
IGMP>
```

igmp fastleave

This command displays or sets IGMP fast leave for specified ports.

SYNTAX

igmp fastleave [*port-list*] [**enable** | **disable**]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

enable - Enables IGMP fast leave. If enabled, the switch immediately deletes a member port of a multicast service if a leave packet is received at that port.

disable - Disables IGMP fast leave.

DEFAULT SETTING

Disabled

COMMAND USAGE

- The switch can be configured to immediately delete a member port of a multicast service if a leave packet is received at that port and the Fast Leave function is enabled. This allows the switch to remove a port from the multicast forwarding table without first having to send an IGMP group-specific (GS) query to that interface.
- If Fast Leave is *not* used, a multicast router (or querier) will send a GS-query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified time-out period.
- If Fast Leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, Fast Leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- Fast Leave is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.
- Fast Leave does not apply to a port if the switch has learned that a multicast router is attached to it.
- Fast Leave can improve bandwidth usage for a network which frequently experiences many IGMP host add and leave requests.

EXAMPLE

```
IGMP>fastleave 6-10 enable
IGMP>
```

igmp leave proxy

This command displays or sets IGMP leave proxy for the switch.

SYNTAX

igmp leave proxy [**enable** | **disable**]

enable - Enables IGMP leave proxy. If enabled, the switch suppresses leave messages unless received from the last member port in the group.

disable - Disables IGMP leave proxy.

DEFAULT SETTING

Disabled

COMMAND USAGE

- IGMP leave proxy suppresses all unnecessary IGMP leave messages so that a non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.
- The leave-proxy feature does not function when a switch is set as the querier. When the switch is a non-querier, the receiving port is not the last dynamic member port in the group, the receiving port is not a router port, and no IGMPv1 member port exists in the group, the switch will generate and send a group-specific (GS) query to the member port which received the leave message, and then start the last member query timer for that port.
- When the conditions in the preceding item all apply, except that the receiving port is a router port, then the switch will not send a GS-query, but will immediately start the last member query timer for that port.

EXAMPLE

```
IGMP>leave proxy enable
IGMP>
```

igmp throttling

This command displays or sets IGMP group throttling for specified ports

SYNTAX

igmp throttling [*port-list*] [*group-limit*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

group-limit - The number of multicast groups to which a port can belong. (Range: 1-10, or 0 to indicate unlimited)

DEFAULT SETTING

unlimited

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, any new IGMP join reports will be dropped.

EXAMPLE

```
IGMP>throttling 9 5
IGMP>
```

igmp filtering

This command displays or sets IGMP group filtering for specified ports.

SYNTAX

igmp filtering [*port-list*] [**add** | **del**] [*group-address*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

add - Adds a new IGMP group filtering entry.

del - Deletes a IGMP group filtering entry.

group-address - IGMP multicast group address.

DEFAULT SETTING

None

COMMAND USAGE

Multicast groups specified by this command are denied access on the specified ports. When filter groups are defined, IGMP join reports received on a port are checked against the these groups. If a requested multicast group is denied, the IGMP join report is dropped.

EXAMPLE

```
IGMP>filtering 9 239.1.1.1
IGMP>
```

igmp router

This command displays or sets specified ports which are attached to a known IGMP router.

SYNTAX

igmp router [*port-list*] [**enable | disable**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

enable - Sets the specified ports to function as a router port, which leads towards a Layer 3 multicast device or IGMP querier.

disable - Disables router port functionality on the specified ports.

DEFAULT SETTING

Disabled

COMMAND USAGE

If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). 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.

EXAMPLE

```
IGMP>router 9 enable
IGMP>
```

igmp flooding

This command displays or sets flooding of unregistered IGMP services.

SYNTAX

igmp flooding [**enable | disable**]

enable - Floods unregistered multicast traffic into the attached VLAN.

disable - Disables IGMP flooding.

DEFAULT SETTING

Disabled

COMMAND USAGE

Once the table used to store multicast entries for IGMP snooping is filled, no new entries are learned. If no router port is configured in the attached VLAN, and unregistered multicast flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

EXAMPLE

```
IGMP>flooding enable
IGMP>
```

igmp groups

This command displays active IGMP groups.

SYNTAX

igmp groups [*vlan-id*]

vlan-id - VLAN identifier. (Range: 1-4095)

DEFAULT SETTING

Displays groups for all VLANs.

EXAMPLE

```
IGMP>groups
VID   Group            Ports
----  ---------------  -----
1     239.255.255.250  1,2
IGMP>
```

igmp status

This command displays IGMP querier status and protocol statistics.

SYNTAX

igmp status [*vlan-id*]

vlan-id - VLAN to which the management address is assigned. (Range: 1-4095)

DEFAULT SETTING

Displays status for all VLANs.

COMMAND USAGE

For a description of the information displayed by this command, see "Showing IGMP Snooping Information" on page 160.

EXAMPLE

```
IGMP>status
      Querier Rx         Tx         Rx         Rx         Rx         Rx
VID   Status  Queries    Queries    V1 Reports V2 Reports V3 Reports V2 Leave
----  ------  ---------- ---------- ---------- ---------- ---------- ----------
1     ACTIVE  0          64         0          149        0          0
2     ACTIVE  0          64         0          0          0          0
IGMP>
```

18 LLDP COMMANDS

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

This section describes the commands used to configure LLDP.

Table 31: LLDP Commands

Command	Function
lldp configuration	Displays LLDP configuration settings for the switch and for specified ports
lldp mode	Displays or sets LLDP message transmit and receive modes for specified ports
lldp optional_tlv	Displays or sets LLDP optional TLVs for specified ports
lldp interval	Displays or sets the transmit interval for LLDP advertisements
lldp hold	Displays or sets the TTL value sent in LLDP advertisements
lldp delay	Displays or sets the delay between the successive transmission of LLDP advertisements
lldp reinit	Displays or sets the delay before attempting to re-initialize information in the remote system's LLDP MIB
lldp info	Displays LLDP neighbor device information
lldp statistics	Displays LLDP statistics
lldp cdp_aware	Displays or sets if discovery information from received CDP frames is added to the LLDP neighbor table

lldp configuration

This command displays LLDP configuration settings for the switch and for specified ports.

SYNTAX

lldp configuration [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

DEFAULT SETTING

All ports

EXAMPLE

```
LLDP>configuration 1
Interval    : 30
Hold        : 3
Tx Delay    : 2
Reinit Delay: 2

Port  Mode      Port Descr  System Name  System Descr  System Capa  Mgmt Addr  CDP awareness
----  --------  ----------  -----------  ------------  -----------  ---------  ------------
1     Disabled  Enabled     Enabled      Enabled       Enabled      Enabled    Disabled
LLDP>
```

lldp mode

This command displays or sets LLDP message transmit and receive modes for LLDP Protocol Data Units for specified ports.

SYNTAX

igmp mode [*port-list*] [**enable** | **disable** | **rx** | **tx**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

enable - Enables LLDP reception and transmission.

disable - Disables LLDP.

rx - Enables LLDP reception only.

tx - Enables LLDP transmission only.

DEFAULT SETTING

Disabled

EXAMPLE

```
LLDP>mode enable
LLDP>
```

lldp optional_tlv

This command displays or sets LLDP optional TLVs for specified ports.

SYNTAX

lldp optional_tlv [*port-list*] [**port_descr** | **sys_name** | **sys_descr** | **sys_capa** | **mgmt_addr**] [**enable** | **disable**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

port_descr - 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.

sys_name - The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name. To configure the system name, see page 187.

sys_descr - 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.

sys_capa - 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.

mgmt_addr - The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

enable - Enables advertisement of specified optional TLVs.

disable - Disables advertisement of specified optional TLVs.

DEFAULT SETTING

All optional TLVs are enabled.

COMMAND USAGE

The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

EXAMPLE

```
LLDP>optional_tlv mgmt_addr disable
LLDP>
```

lldp interval

This command displays or sets the periodic transmit interval for LLDP advertisements.

SYNTAX

lldp interval [*interval*]

interval - The periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds)

This attribute must comply with the following rule:

(Transmission Interval * Transmission Hold Time) ≤ 65536, and Transmission Interval ≥ (4 * Transmission Delay)

DEFAULT SETTING

30 seconds

EXAMPLE

```
LLDP>interval 60
LLDP>
```

lldp hold

This command displays or sets the TTL value sent in LLDP advertisements.

SYNTAX

lldp hold [*hold*]

hold - The time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10)

TTL in seconds is based on the following rule:

(Transmission Interval * Transmission Hold Time) ≤ 65536. Therefore, the default TTL is 30*3 = 90 seconds.

DEFAULT SETTING

3

COMMAND USAGE

The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

EXAMPLE

```
LLDP>hold 10
LLDP>
```

lldp delay

This command displays or sets the delay between the successive transmission of LLDP advertisements.

SYNTAX

lldp delay [*delay*]

delay - The delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds)

This attribute must comply with the rule:

(4 * Transmission Delay) ≤ Transmission Interval

DEFAULT SETTING

2 seconds

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

```
LLDP>delay 10
LLDP>
```

lldp reinit

This command displays or sets the delay before attempting to re-initialize information in the remote system's LLDP MIB after LLDP ports are disabled or the link goes down.

SYNTAX

lldp reinit [*reinit*]

reinit - The delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds)

DEFAULT SETTING
2 seconds

COMMAND USAGE
When LLDP is re-initialized on a port, all information in the remote system's LLDP MIB associated with this port is deleted.

EXAMPLE

```
LLDP>reinit 10
LLDP>
```

lldp info

This command displays information about devices connected directly to the switch's ports which are advertising information through LLDP.

SYNTAX

lldp info [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

DEFAULT SETTING
All ports

COMMAND USAGE
For a description of the information displayed by this command, see "Displaying LLDP Neighbor Information" on page 162.

EXAMPLE

```
LLDP>info

Local port          : Port 4
Chassis ID          : 00-30-FC-12-34-56
Port ID             : 00-30-FC-12-34-58
Port Description    : Ethernet Port on unit 1, port 2
System Name         :
System Description  :
System Capabilities : Bridge(+)
Management Address  : 192.168.1.20 (IPv4)

LLDP>
```

lldp statistics

This command displays statistics on LLDP global counters and control frames.

SYNTAX

lldp statistics [*port-list*] [**clear**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

clear - Clears LLDP statistics.

DEFAULT SETTING

Disabled

COMMAND USAGE

For a description of the information displayed by this command, see "Displaying LLDP Port Statistics" on page 163.

EXAMPLE

```
LLDP>statistics 4

LLDP global counters
Neighbor entries was last changed at 1970-01-01 05:52:43 +0000 (5314 sec.
  ago).
Total Neighbors Entries Added    2.
Total Neighbors Entries Deleted  0.
Total Neighbors Entries Dropped  0.
Total Neighbors Entries Aged Out 0.

LLDP local counters
       Rx       Tx       Rx       Rx       Rx TLV   Rx TLV   Rx TLV
Port   Frames   Frames   Errors   Discards Errors   Unknown  Organz.  Aged
----   ------   ------   ------   -------- ------   -------  -------  -----
4      174      144      0        0        0        0        1392     0
LLDP>
```

lldp cdp_aware

This command displays or configures whether or not discovery information from received CDP frames is added to the LLDP neighbor table.

SYNTAX

lldp cdp_aware [*port-list*] [**enable** | **disable**]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

enable - Enables decoding of Cisco Discovery Protocol frames.

disable - Disables decoding of Cisco Discovery Protocol frames.

DEFAULT SETTING

Disabled

COMMAND USAGE

- If enabled, CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded, all others are discarded. CDP TLVs are mapped into LLDP neighbors table as shown below:
  - CDP TLV "Device ID" is mapped into the LLDP "Chassis ID" field.
  - CDP TLV "Address" is mapped into the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.
  - CDP TLV "Port ID" is mapped into the LLDP "Port ID" field.
  - CDP TLV "Version and Platform" is mapped into the LLDP "System Description" field.
  - Both the CDP and LLDP support "system capabilities," but the CDP capabilities cover capabilities that are not part of LLDP. These capabilities are shown as "others" in the LLDP neighbors table.
- If all ports have CDP awareness disabled, the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the switch.
- When CDP awareness for a port is disabled, the CDP information is not removed immediately, but will be removed when the hold time is exceeded.

EXAMPLE

```
LLDP>cdp_aware enable
LLDP>
```

19 MAC COMMANDS

This section describes commands used to configure the MAC address table, including learning mode, aging time, and setting static addresses.

Table 32: MAC Commands

Command	Function
mac configuration	Displays MAC address table configuration for specified ports
mac add	Adds a static MAC address to the specified port and VLAN
mac delete	Deletes a MAC address entry from the specified VLAN
mac lookup	Searches for the specified MAC address in the specified VLAN
mac agetime	Displays or sets the MAC address aging time
mac learning	Displays or sets the MAC address learning mode
mac dump	Displays sorted list of MAC address entries
mac statistics	Displays statistics on the type and number of MAC addresses associated with specified ports
mac flush	Clears all learned entries

mac configuration

This command displays the MAC address table configuration for specified ports.

SYNTAX

mac configuration [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

EXAMPLE

```
MAC>configuration 1
MAC Age Time: 300

Port  Learning
----  --------
1     Auto
MAC>
```

mac add

This command adds a static MAC address to the specified port and VLAN.

SYNTAX

mac add *mac-address port-list* [*vlan-id*]

mac-address - Physical address of a device mapped to a port.

port-list - A specific port or a range of ports. (Range: 1-28, **all**, or **none**)

vlan-id - VLAN identifier. (Range: 1-4095)

DEFAULT SETTING

No static addresses are configured.

COMMAND USAGE

- A static address can be assigned to a specific port on this switch. Static addresses are bound to the assigned port and will not be moved. When a static address is seen on another port, 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 mac delete command (see page 272).

EXAMPLE

```
MAC>add 00-12-cf-94-34-dd 1 1
MAC>
```

mac delete

This command deletes a MAC address entry from the specified VLAN.

SYNTAX

mac delete *mac-address* [*vlan-id*]

mac-address - Physical address of a device mapped to a port.

vlan-id - VLAN identifier. (Range: 1-4095)

COMMAND USAGE

If the VLAN identifier is not specified, all entries found in the address table are deleted.

EXAMPLE

```
MAC>del 00-12-cf-94-34-dd
MAC>
```

mac lookup

This command searches for the specified MAC address in the specified VLAN.

SYNTAX

mac lookup *mac-address* [*vlan-id*]

mac-address - Physical address of a device mapped to a port.

vlan-id - VLAN identifier. (Range: 1-4095)

EXAMPLE

```
MAC>lookup 00-12-cf-94-34-dd
Type    VID  MAC Address        Ports
------  ---  -----------------  -----
Static  1    00-12-cf-94-34-dd  1
MAC>
```

mac agetime

This command displays or sets the MAC address aging time.

SYNTAX

mac agetime [*age-time*]

age-time - The time after which a learned entry is discarded. (Range: 10-1000000 seconds, or 0 to disable aging)

DEFAULT SETTING

300 seconds

EXAMPLE

```
MAC>agetime 100
MAC>
```

mac learning

This command displays or sets the MAC address learning mode.

SYNTAX

mac learning [*port-list*] [**auto** | **disable** | **secure**]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

auto - Learning is done automatically as soon as a frame with an unknown source MAC address is received.

disable - No addresses are learned and stored in the MAC address table.

secure - Only static MAC address entries are used, all other frames are dropped.

DEFAULT SETTING
Auto

COMMAND USAGE
Make sure that the link used for managing the switch is added to the Static MAC Table before changing to secure learning mode. Otherwise the management link will be lost, and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

NOTE: If another software module is in control of the learning mode for a given port, it cannot be changed by this command. An example of such a module is the MAC-Based Authentication under 802.1X.

EXAMPLE

```
MAC>learning 9 secure
MAC>
```

mac dump

This command displays sorted list of MAC address entries.

SYNTAX

mac dump [*mac-max*] [*mac-addr*] [*vlan-id*]

mac-max - Maximum number of MAC addresses to display.

mac-addr - First MAC address to display.
(Format: xx-xx-xx-xx-xx-xx)

vlan-id - VLAN identifier. (Range: 1-4095)

DEFAULT SETTING
Maximum: Displays all addresses.
First address: MAC address zero
VLAN ID: 1

EXAMPLE

```
MAC>dump 5
Type    VID  MAC Address        Ports
------  ---  -----------------  -----
Static  1    00-01-c1-00-00-e1  None,CPU
Dynamic 1    00-12-cf-61-24-2f  7,8
Dynamic 1    00-12-cf-61-24-30  7,8
Dynamic 1    00-30-fc-12-34-56  4,5
Dynamic 1    00-30-fc-12-34-57  4,5
MAC>
```

mac statistics

This command displays statistics on the type and number of MAC addresses associated with specified ports.

SYNTAX

mac statistics [*port-list*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

DEFAULT SETTING

Displays statistics for all ports.

EXAMPLE

```
MAC>statistics 1
Port  Dynamic Addresses
----  -----------------
1     0

Total Dynamic Addresses: 5
Total Static Addresses : 4
MAC>
```

mac flush

This command clears all learned entries.

SYNTAX

mac flush

EXAMPLE

```
MAC>flush
MAC>dump
Type    VID  MAC Address        Ports
------  ---  -----------------  -----
Static  1    00-01-c1-00-00-e1  None,CPU
Static  1    33-33-ff-00-00-e1  None,CPU
Static  1    33-33-ff-a8-02-0a  None,CPU
Static  1    ff-ff-ff-ff-ff-ff  1-28,CPU
MAC>
```

20 VLAN COMMANDS

This section describes commands used to configure standard IEEE 802.1Q VLANs port members and port attributes.

Table 33: VLAN Commands

Command	Function
vlan configuration	Displays VLAN attributes for specified ports and list of ports assigned to each VLAN
vlan aware	Displays or sets whether or not a port processes the VLAN ID in ingress frames
vlan pvid	Displays or sets the VLAN ID assigned to untagged frames received on specified ports
vlan frametype	Displays or sets a port to accept all frame types, including tagged or untagged frames, or only tagged frames
vlan ingressfilter	Displays or sets ingress filtering for specified ports, which discards frames tagged for VLANs for which it is not a member
vlan qinq	Displays or sets whether or not a port accepts double tagged frames
vlan add	Adds specified ports to a VLAN
vlan delete	Deletes specified VLAN
vlan lookup	Displays port members for specified VLAN

vlan configuration

This command displays VLAN attributes for specified ports and lists the ports assigned to each VLAN.

SYNTAX

vlan configuration [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

EXAMPLE

```
VLAN>configuration 1

Port  Aware     PVID  Frame Type  Ingress Filter  QinQ
----  --------  ----  ----------  --------------  ----
1     Disabled  1     All         Disabled        Disabled

VID   Ports
----  -----
1     1-28
VLAN>
```

vlan aware

This command displays or sets whether or not a port processes the VLAN ID in ingress frames.

SYNTAX

vlan aware [**enable** | **disable**]

enable - Each frame is assigned to the VLAN indicated in the VLAN tag, and the tag is removed.

disable - All frames are assigned to the default VLAN (as specified by the vlan pvid command) and tags are not removed.

DEFAULT SETTING

Disabled

COMMAND USAGE

- If the port is VLAN aware, untagged frames received on the port are assigned to the default PVID, and tagged frames are processed using the frame's VLAN ID. If the port is not VLAN aware, all frames received on the port are assigned to the default PVID.

  Regardless of whether or not a port is VLAN aware, if the VLAN to which the frame has been assigned is different from the default PVID, a tag indicating the VLAN to which this frame was assigned will be inserted in the egress frame. Otherwise, the frame is transmitted without a VLAN tag.

- When the PVID is set to "none" by the vlan pvid command (see page 278) the ID for the VLAN to which this frame has been assigned is inserted in frames transmitted from the port. The assigned VLAN ID can be based on the ingress tag for tagged frames, or the default PVID for untagged ingress frames. Note that this mode is normally used for ports connected to VLAN aware switches.

- 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 should first strip off the VLAN tag before forwarding the frame.

EXAMPLE

```
VLAN>aware enable
VLAN>
```

vlan pvid

This command displays or sets the VLAN ID assigned to untagged frames received on specified ports.

SYNTAX

vlan pvid [*port-list*] [*vlan-id* | **none**]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

vlan-id - VLAN identifier. (Range: 1-4095)

none - The ID for the VLAN to which this frame has been assigned is inserted in frames transmitted from the port.

DEFAULT SETTING

All ports are assigned to native VLAN 1.

COMMAND USAGE

- The port must be a member of the same VLAN as the Port VLAN ID.
- When the PVID is set to "none," the ID for the VLAN to which this frame has been assigned is inserted in frames transmitted from the port. The assigned VLAN ID can be based on the ingress tag for tagged frames, or the default PVID for untagged ingress frames. Note that this mode is normally used for ports connected to VLAN-aware switches.

EXAMPLE

```
VLAN>pvid 9 2
VLAN>
```

vlan frametype

This command displays or sets a port to accept all frame types, including tagged or untagged frames, or only tagged frames.

SYNTAX

vlan frametype [*port-list*] [**all** | **tagged**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

all - Accepts all frame types, including tagged or untagged frames. Any received frames that are untagged are assigned to the default VLAN

tagged - Accepts only tagged frames. All untagged frames received on the interface are discarded

DEFAULT SETTING

Accepts all frame types.

EXAMPLE

```
VLAN>frametype 9 tagged
VLAN>
```

vlan ingressfilter

This command displays or sets ingress filtering for specified ports, which when enabled, discards frames tagged for VLANs for which it is not a member.

SYNTAX

vlan ingressfilter [*port-list*] [**enable** | **disable**]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

enable - If a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.

disable - If a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports.

DEFAULT SETTING

Disabled

COMMAND USAGE

- Ingress filtering only affects tagged frames.
- 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.

EXAMPLE

```
VLAN>ingressfilter 9 enable
VLAN>
```

vlan qinq

This command displays or sets whether or not a port accepts double tagged frames received on the specified ports.

SYNTAX

vlan qinq [*port-list*] [**enable** | **disable**]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

enable - Accepts double tagged frames.

disable - Discards double tagged frames.

DEFAULT SETTING

Disabled

EXAMPLE

```
VLAN>qinq 9 enable
VLAN>
```

vlan add

This command adds specified ports to a VLAN.

SYNTAX

vlan add [*vlan-id*] [*port-list*]

vlan-id - VLAN identifier. (Range: 1-4095)

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

DEFAULT SETTING

All ports are assigned to VLAN 1.

COMMAND USAGE

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 must connect them through a router.

EXAMPLE

```
VLAN>add 2 9
VLAN>
```

vlan delete

This command deletes the specified VLAN.

SYNTAX

vlan delete [*vlan-id*]

vlan-id - VLAN identifier. (Range: 1-4095)

EXAMPLE

```
VLAN>delete 2
VLAN>
```

vlan lookup

This command displays port members for specified VLAN.

SYNTAX

vlan lookup [*vlan-id*]

vlan-id - VLAN identifier. (Range: 1-4095)

EXAMPLE

```
VLAN>lookup 2

VID   Ports
----  -----
2     9
VLAN>
```

21 PVLAN COMMANDS

This section describes commands used to configure private VLANs (PVLAN) and isolated ports, providing port-based security and isolation between ports within the assigned VLAN.

Table 34: PVLAN Commands

Command	Function
pvlan configuration	Displays PVLAN member ports, and whether or not port isolation is enabled
pvlan add	Add specified ports to a PVLAN
pvlan delete	Deletes the specified PVLAN
pvlan lookup	Displays the specified PVLANs and port members
pvlan isolate	Displays or sets port isolation between ports within the same PVLAN

pvlan configuration

This command displays PVLAN member ports, and whether or not port isolation is enabled.

SYNTAX

pvlan configuration [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

EXAMPLE

```
PVLAN>configuration 1-10

Port  Isolation
----  ---------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled

PVLAN ID  Ports
--------  -----
1         1-28
PVLAN>
```

pvlan add

This command add specified ports to a PVLAN.

SYNTAX

pvlan add *pvlan-id* [*port-list*]

pvlan-id - PVLAN identifier. (Range: 1-4095)

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

DEFAULT SETTING

Adds all ports.

COMMAND USAGE

- Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on ports assigned to a private VLAN can only be forwarded to, and from, uplink ports (that is, ports configured as members of both a standard IEEE 802.1Q VLAN and the private VLAN).
- By default, all ports are configured as members of VLAN 1 and PVLAN 1. Because all of these ports are members of 802.1Q VLAN 1, isolation cannot be enforced between the members of PVLAN 1. To use PVLAN 1 properly, remove the ports to be isolated from VLAN 1 (using the vlan add described on page 280). Then connect the uplink ports to the local servers or other service providers to which the members of PVLAN 1 require access.

EXAMPLE

```
PVLAN>add 9
PVLAN>up
>vlan add 1 1-8,10-28
>
```

pvlan delete

This command deletes the specified PVLAN.

SYNTAX

pvlan delete *pvlan-id*

pvlan-id - PVLAN identifier. (Range: 1-4095)

DEFAULT SETTING

None

EXAMPLE

```
VLAN>delete 2
VLAN>
```

pvlan lookup

This command displays the specified PVLANs and port members.

SYNTAX

vlan lookup [*pvlan-id*]

pvlan-id - PVLAN identifier. (Range: 1-4095)

EXAMPLE

```
PVLAN>lookup 2

PVLAN ID  Ports
--------  -----
2         6-10
PVLAN>
```

pvlan isolate

This command displays or sets port isolation between ports within the same PVLAN.

SYNTAX

vlan isolate [*port-list*] [**enable** | **disable**]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

enable - Enables port isolation.

disable - Disables port isolation.

DEFAULT SETTING

Disabled

COMMAND USAGE

Ports within a PVLAN are isolated from other ports which are not in the same PVLAN. Port Isolation can be used to further prevent communications between ports within the same PVLAN. An isolated port cannot forward any unicast, multicast, or broadcast traffic to any other ports in the same PVLAN.

EXAMPLE

```
PVLAN>isolate 9 enable
PVLAN>
```

22 QoS Commands

This section describes commands used to configure quality of service parameters, including the default port queue, the default tag assigned to untagged frames, input rate limiting, output shaping, queue mode, queue weight, quality control lists, storm control, DSCP remarking, and DSCP queue mapping.

Table 35: QoS Commands

Command	Function
qos configuration	Displays QoS configuration settings, including storm control, default priority queue, default tag priority, quality control list, rate limiting, queuing mode and queue weights
qos default	Displays or sets default priority (traffic class) for specified ports
qos tagprio	Displays or sets default tag priority (used when adding a tag to untagged frames) for specified ports
qos qcl port	Displays or sets the QCL assigned to specified ports
qos qcl add	Adds or modifies a QoS control entry
qos qcl delete	Deletes a QoS control entry
qos qcl lookup	Displays the specified QoS control list or control entry
qos mode	Displays or sets the egress queuing mode for specified ports
qos weight	Displays or sets the egress queue weight for specified ports
qos rate limiter	Displays or sets ingress rate limiting for specified ports
qos shaper	Displays or sets egress rate limiting for specified ports
qos storm unicast	Displays or sets unknown unicast storm rate limits for the switch
qos storm multicast	Displays or sets multicast storm rate limits for the switch
qos storm broadcast	Displays or sets broadcast storm rate limits for the switch
qos dscp remarking	Displays or sets the status of DSCP remarking for specified ports
qos dscp queue mapping	Displays or sets the DSCP value used for DSCP remarking for specified ports

qos configuration

This command displays QoS configuration settings, including storm control, default priority queue, default tag priority, quality control list, rate limiting, queuing mode and queue weights.

SYNTAX

qos configuration [*port-list*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

EXAMPLE

```
QoS>configuration 1-10
Traffic Classes: 4

Storm Multicast: Disabled     1 pps
Storm Broadcast: Disabled     1 pps
Storm Unicast  : Disabled     1 pps

Port  Default  Tag Priority  QCL ID  Rate Limiter  Shaper     Mode      Weight
----  -------  ------------  ------  ------------  ---------  --------  -----
1     Low      0             1       Disabled      Disabled   Strict    1/2/4/8
2     Low      0             1       Disabled      Disabled   Strict    1/2/4/8
3     Low      0             1       Disabled      Disabled   Strict    1/2/4/8
4     Low      0             1       Disabled      Disabled   Strict    1/2/4/8
5     Low      0             1       Disabled      Disabled   Strict    1/2/4/8
6     Low      0             1       Disabled      Disabled   Strict    1/2/4/8
7     Low      0             1       Disabled      Disabled   Strict    1/2/4/8
8     Low      0             1       Disabled      Disabled   Strict    1/2/4/8
9     Low      0             1       Disabled      Disabled   Strict    1/2/4/8
10    Low      0             1       Disabled      Disabled   Strict    1/2/4/8

QoS>
```

qos default

This command displays or sets the default priority (i.e., traffic class) for specified ports.

SYNTAX

qos default [*port-list*] *class*

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

class - The priority assigned to ingress frames that do not match any of the entries in the QCL assigned by the qos qcl port command (see page 287). (Options: low/norma/medium/high or 1/2/3/4)

DEFAULT SETTING

Low

EXAMPLE

```
QoS>default 9 high
QoS>
```

qos tagprio

This command displays or sets the default tag priority (used when adding a tag to untagged frames) for specified ports.

SYNTAX

qos tagprio [*port-list*] [*tag-priority*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

tag-priority - The default priority used when adding a tag to untagged frames. (Range: 0-7)

DEFAULT SETTING

0

COMMAND USAGE

- The default tag priority applies to untagged frames 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.
- Inbound frames that do not have VLAN tags are tagged with the input port's default ingress tag priority, and then placed in the appropriate priority queue at 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

```
QoS>tagprio 9 7
QoS>
```

qos qcl port

This command displays or sets the QCL assigned to specified ports.

SYNTAX

qos qcl port [*port-list*] [*qcl-id*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

qcl-id - A Quality Control List which classifies ingress frames based on criteria including Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS, or VLAN priority tag (see the qos qcl add command on page 288). Traffic matching the first entry in the QCL is assigned to the traffic class (output queue) defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port. (Range: 1-28)

DEFAULT SETTING

None

EXAMPLE

```
QoS>QCL>port 9 1
QoS>QCL>
```

qos qcl add

This command adds or modifies a QoS control entry.

SYNTAX

qos qcl add [*qcl-id*] [*qce-id*] [*qce-id-next*]
{**etype** *ethernet-type* | **vid** *vlan-id* | **port** *udp-tcp-port* | **dscp** *dscp* | **tos** *tos-list* | **tag-prio** *tag-priority-list*} *class*

qcl-id - A Quality Control List containing one or more classification criteria used to determine the traffic class to which a frame is assigned. (Range: 1-28)

qce-id - A QCL entry which specifies one of the following criteria to be matched in the ingress frame. (Range: 1-24)

qce-id-next - Inserts the QCE before this row. If not specified, the QCE is inserted at the bottom of the list. (Range: 1-24)

ethernet-type - This option can only be used to filter Ethernet II formatted packets. (Range: 0x600-0xffff hex; Default: 0xffff)

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).

vlan-id - VLAN identifier. (Range: 1-4095)

udp-tcp-port - Source/destination port number or range. (Range: 0-65535)

dscp - IPv4/IPv6 DSCP priority level. (Range: 0-63)

tos-list - Type of Service level, which processes the precedence part of the IPv4/IPv6 ToS (3 bits) as an index to the eight QoS Class values. (Range: 0-7)

tag-priority-list - Uses the User Priority value (3 bits as defined by IEEE 802.1p) as an index to the eight QoS Class values.

The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Table 36: Mapping CoS Values to Egress Queues

Priority	0	1	2	3	4	5	6	7
Queue	Normal	Low	Low	Normal	Medium	Medium	High	High

class - Output queue buffer. (Range: low/normal/medium/high or 1/2/3/4)

DEFAULT SETTING

QCL: 1
QCE: 1

COMMAND USAGE

- The braces used in the syntax of this command indicate that one of the classification criteria must be specified. The *class* parameter must also be specified in each command. The other parameters are optional.
- Once a QCL is mapped to a port using the qos qcl port (see page 287), traffic matching the first entry in the QCL is assigned to the traffic class (Low, Medium, Normal or High) defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port (see the qos default command on page 286).

EXAMPLE

```
QoS>QCL>add 1 1 tos 1,2-4 1
QoS>QCL>
```

qos qcl delete

This command deletes a QoS control entry.

SYNTAX

qos qcl delete *qcl-id qce-id*

qcl-id - A Quality Control List containing one or more classification criteria used to determine the traffic class to which a frame is assigned. (Range: 1-28)

qce-id - A QCL entry which specifies one of the following criteria to be matched in the ingress frame. (Range: 1-24)

DEFAULT SETTING

None

EXAMPLE

```
QoS>QCL>delete 1 1
QoS>QCL>
```

qos qcl lookup

This command displays the specified QoS control list or control entry.

SYNTAX

qos qcl lookup [*qcl-id*] [*qce-id*]

qcl-id - A Quality Control List containing one or more classification criteria used to determine the traffic class to which a frame is assigned. (Range: 1-28)

qce-id - A QCL entry which specifies one of the following criteria to be matched in the ingress frame. (Range: 1-24)

DEFAULT SETTING

Displays all QCLs.

EXAMPLE

```
QoS/QCL>lookup
QCL ID 1:

QCE ID  Type     Class Mapping
------  -------  -------------
1       VLAN ID  1 -> Low
2       UDP/TCP  0 -> Low
QoS>QCL>
```

qos mode

This command displays or sets the egress queuing mode for specified ports.

SYNTAX

qos mode [*port-list*] [**strict** | **weighted**]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

strict - Services the queues based on a strict rule that requires all traffic in a higher priority queues to be processed before lower priority queues are serviced.

weighted - Services the queues based on Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue.

DEFAULT SETTING

Strict queuing

EXAMPLE

```
QoS>mode weighted
QoS>
```

qos weight

This command displays or sets the egress queue weight for specified ports.

SYNTAX

qos weight [*port-list*] [*class*] [*weight*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

class - Output queue buffer. (Range: low/normal/medium/high or 1/2/3/4)

weight - The weight assigned to the specified egress queue, and thereby to the corresponding traffic priorities. (Range: 1, 2, 4, 8)

DEFAULT SETTING

Low - 1
Normal - 2
Medium - 4
High - 8

COMMAND USAGE

When the Queuing Mode is set to weighted with the qos mode command (page 290), the switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. The traffic classes are mapped to one of the egress queues provided for each port. You can assign a weight to each of these queues, and thereby to the corresponding traffic priorities.

EXAMPLE

```
QoS>weight 3 8
QoS>
```

qos rate limiter

This command displays or sets ingress rate limiting for specified ports.

SYNTAX

qos rate limiter [*port-list*] [**enable** | **disable**] [*bit-rate*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

enable - Enables ingress rate limiting.

disable - Disables ingress rate limiting.

bit-rate - Maximum ingress rate in kilobits/second. (Range: 500-1000000 kbps)

DEFAULT SETTING

Disabled
500 kbps when enabled

COMMAND USAGE

Rate limiting controls the maximum rate for traffic transmitted or received on an interface. Rate limiting can be configured on interfaces at the edge of a network to form part of the customer service package by limiting traffic into or out of the switch. Packets that exceed the acceptable amount of traffic are dropped, while conforming traffic is forwarded without any changes.

EXAMPLE

```
QoS>rate limiter enable 600
QoS>
```

qos shaper

This command displays or sets egress rate limiting for specified ports.

SYNTAX

qos shaper [*port-list*] [**enable** | **disable**] [*bit-rate*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

enable - Enables egress rate limiting.

disable - Disables egress rate limiting.

bit-rate - Maximum egress rate in kilobits/second. (Range: 500-1000000 kbps)

DEFAULT SETTING

Disabled
500 kbps when enabled

COMMAND USAGE

Rate limiting controls the maximum rate for traffic transmitted or received on an interface. Rate limiting can be configured on interfaces at the edge of a network to form part of the customer service package by limiting traffic into or out of the switch. Packets that exceed the acceptable amount of traffic are dropped, while conforming traffic is forwarded without any changes.

EXAMPLE

```
QoS>shaper enable 600
QoS>
```

qos storm unicast

This command displays or sets unknown unicast storm rate limits for the switch.

SYNTAX

qos storm unicast [**enable** | **disable**] [*packet-rate*]

enable - Enables unknown unicast storm control.

disable - Disables unknown unicast storm control.

packet-rate - The threshold above which packets are dropped. (Options: 1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k pps)

DEFAULT SETTING

Disabled
2 pps when enabled

COMMAND USAGE

- The specified limit applies to each port.
- Any packets exceeding the specified threshold will then be dropped.
- Due to an ASIC limitation, the enforced rate limits are slightly less than the listed options. For example: 1 Kpps translates into an enforced threshold of 1002.1 pps.

EXAMPLE

```
QoS>Storm>unicast enable 2k
QoS>Storm>
```

qos storm multicast

This command displays or sets multicast storm rate limits for the switch.

SYNTAX

qos storm multicast [**enable** | **disable**] [*packet-rate*]

enable - Enables multicast storm control.

disable - Disables multicast storm control.

packet-rate - The threshold above which packets are dropped. (Options: 1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k pps)

DEFAULT SETTING

Disabled
2 pps when enabled

COMMAND USAGE

- The specified limit applies to each port.
- Any packets exceeding the specified threshold will then be dropped.

- Due to an ASIC limitation, the enforced rate limits are slightly less than the listed options. For example: 1 Kpps translates into an enforced threshold of 1002.1 pps.

EXAMPLE

```
QoS>Storm>multicast enable 2k
QoS>Storm>
```

qos storm broadcast

This command displays or sets broadcast storm rate limits for the switch.

SYNTAX

qos storm broadcast [**enable** | **disable**] [*packet-rate*]

enable - Enables broadcast storm control.

disable - Disables broadcast storm control.

packet-rate - The threshold above which packets are dropped. (Options: 1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k pps)

DEFAULT SETTING

Disabled
2 pps when enabled

COMMAND USAGE

- The specified limit applies to each port.
- Any packets exceeding the specified threshold will then be dropped.
- Due to an ASIC limitation, the enforced rate limits are slightly less than the listed options. For example: 1 Kpps translates into an enforced threshold of 1002.1 pps.

EXAMPLE

```
QoS>Storm>broadcast enable 2k
QoS>Storm>
```

qos dscp remarking

This command displays or sets the status of DSCP remarking for specified ports.

SYNTAX

qos dscp remarking [*port-list*] [**enable** | **disable**]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

enable - Enables DSCP remarking.

disable - Disables DSCP remarking.

DEFAULT SETTING
Disabled

EXAMPLE

```
QoS>DSCP>remarking 9 enable
QoS>DSCP>
```

qos dscp queue mapping

This command displays or sets the DSCP value used for DSCP remarking for specified ports.

SYNTAX

qos dscp queue mapping [*port-list*] [*class*] [*dscp*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

class - Output queue buffer. (Range: low/normal/medium/high or 1/2/3/4)

dscp - IPv4/IPv6 DSCP priority level.
(Options: 0/8/16/24/32/40/46/48/56)

DEFAULT SETTING
Low: 8
Normal: 16
Medium: 24
High: 32

EXAMPLE

```
QoS>DSCP>queue mapping 9 low 16
QoS>DSCP>
```

23 ACL COMMANDS

This section describes commands used to configure access control lists, including policies, responses, and rate limiters.

Table 37: ACL Commands

Command	Function
acl configuration	Displays ACL configuration settings, including policy, response, rate limiters, port copy, logging, and shutdown
acl action	Displays or sets default action for specified ports, including permit/deny, rare limiters, port copy, logging, and shutdown
acl policy	Displays or sets the policy assigned to specified ports
acl rate	Displays or sets the rate limiter and maximum packet rate
acl add	Adds or modifies an access control entry
acl delete	Deletes an access control entry
acl lookup	Displays the specified access control entry
acl clear	Clears all ACL counters

acl configuration

This command displays ACL configuration settings, including policy, response, rare limiters, port copy, logging, and shutdown.

SYNTAX

acl configuration [*port-list*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

EXAMPLE

```
ACL>configuration 1-5

Port  Policy  Action  Rate Limiter  Port Copy  Logging   Shutdown  Counter
----  ------  ------  ------------  ---------  --------  --------  -------
1     1       Permit  Disabled      Disabled   Disabled  Disabled  1463
2     1       Permit  Disabled      Disabled   Disabled  Disabled  26429
3     1       Permit  Disabled      Disabled   Disabled  Disabled  0
4     1       Permit  Disabled      Disabled   Disabled  Disabled  818
5     1       Permit  Disabled      Disabled   Disabled  Disabled  818

Rate Limiter  Rate
------------  ----
1             1
2             1
3             1
4             1
5             1
6             1
```

```
7               1
8               1
9               1
10              1
11              1
12              1
13              1
14              1
15              1

ACL>
```

acl action

This command displays or sets the default action for specified ports, including permit/deny, rate limiters, port copy, logging, and shutdown.

SYNTAX

acl action [*port-list*] [**permit** | **deny**] [*rate-limiter*] [*port-copy*] [*logging*] [*shutdown*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

permit - Permits a frame if it matches a rule defined in the assigned policy (see the acl policy command on page 298).

deny - Denies a frame if it matches a rule defined in the assigned policy (see the acl policy command).

rate-limiter - Specifies a rate limiter (see the acl rate command on page 298) to apply to the port. (Range: 1-15, or **disable**)

port-copy - Defines a port to which matching frames are copied. (Range: 1-28, or **disable**)

logging - Enables logging of matching frames to the system log. (Options: **log** or **log_disable**)

Use the system log command (page 189) to view any information stored in the system log for this entry. Related entries will be displayed under the "info" or "all" logging levels.

shutdown - Shuts down a port when a matching frame is seen. (Options: **shut** or **shut_disable**)

DEFAULT SETTING

Forwarding: Permit
Rate Limiter: Disabled
Port Copy: Disabled
Logging: Disabled
Shutdown: Disabled

EXAMPLE

```
ACL>action 9 permit 1 15 log shut
ACL>
```

acl policy

This command displays or sets the policy assigned to specified ports.

SYNTAX

acl policy [*port-list*] [*policy*]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

policy - An ACL policy configured with the acl add command, containing one or more ACEs. (Range: 1-8)

DEFAULT SETTING

Policy 1, which is undefined.

EXAMPLE

```
ACL>policy 9 7
ACL>
```

acl rate

This command displays or sets the rate limiter and maximum packet rate.

SYNTAX

acl rate [*rate-limiter-list*] [*packet-rate*]

rate-limiter-list - Rate limiter identifier. (Range: 1-15)

packet-rate - The threshold above which packets are dropped. (Options: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, 1024K pps)

Due to an ASIC limitation, the enforced rate limits are slightly less than the listed options. For example: 1 Kpps translates into an enforced threshold of 1002.1 pps.

DEFAULT SETTING

All rate limiters

EXAMPLE

```
ACL>rate 2 512k
ACL>
```

acl add

This command adds or modifies an access control entry.

SYNTAX

acl add [*ace-id*] [*ace-id-next*]
[**switch** | (**port** *port*) | (**policy** *policy*)]
[*vlan-id*] [*tag-priority*] [*dmac-type*]
[(**etype** [*ethernet-type*] [*smac*] [*dmac*]) |
(**arp** [*sip*] [*dip*] [*smac*] [*arp-opcode*] [*arp-flags*]) |
(**ip** [*sip*] [*dip*] [*protocol*] [*ip-flags*]) |
(**icmp** [*sip*] [*dip*] [*icmp-type*] [*icmp-code*] [*ip-flags*]) |
(**udp** [*sip*] [*dip*] [*sport*] [*dport*] [*ip-flags*]) |
(**tcp** [*sip*] [*dip*] [*sport*] [*dport*] [*ip-flags*] [*tcp-flags*])]
[**permit** | **deny**] [*rate-limiter*] [*port-copy*] [*logging*] [*shutdown*]

ace-id - An ACL entry which specifies one of the following criteria to be matched in the ingress frame. (Range: 1-128; Default: Next available ID)

ace-id-next - Inserts the ACE before this row. If not specified, the ACE is inserted at the bottom of the list. (Range: 1-128)

switch - ACE applies to all ports on the switch.

port *port* - ACE applies to specified port or a range of ports. (Range: 1-28)

policy *policy* - An ACL policy identifier to which this ACE is assigned. (Range: 1-8)

vlan-id - The VLAN to filter for this rule. (Range: 1-4095, or **any**)

tag-priority - Specifies the User Priority value found in the VLAN tag (3 bits as defined by IEEE 802.1p) to match for this rule. (Range: 0-7, or **any**)

dmac-type - The type of destination MAC address. (Options: **any**, **unicast**, **multicast**, **broadcast**; Default: **any**)

etype - One of the following Ethernet or MAC parameters:

ethernet-type - This option can only be used to filter Ethernet II formatted packets. (Range: 0x600-0xffff hex, or **any**; Default: **any**)

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).

smac - Source MAC address (xx-xx-xx-xx-xx-xx) or **any**.

dmac - Destination MAC address (xx-xx-xx-xx-xx-xx) or **any**.

arp - One of the following MAC or ARP parameters:

sip - Source IP address (a.b.c.d/n) or **any**.

dip - Destination IP address (a.b.c.d/n) or **any**.

smac - Source MAC address (xx-xx-xx-xx-xx-xx) or **any**.

arp-opcode - Specifies the type of ARP packet. (Options: **any** - no ARP/RARP opcode flag is specified, **arp** - frame must have

ARP/RARP opcode set to ARP, **rarp** - frame must have ARP/RARP opcode set to RARP, **other** - frame has unknown ARP/RARP opcode flag; Default: **any**)

arp-flags - One of the following ARP flags:

request - Frame must have ARP Request or RARP Request opcode flag set.

smac - ARP frame where sender hardware address (SHA) field is equal to the SMAC address.

tmac - RARP frames where target hardware address (THA) is equal to the SMAC address.

len - ARP/RARP frames where the hardware address length (HLN) is equal to Ethernet (0x06) and the protocol address length (PLN) is equal to IPv4 (0x04).

ip - ARP/RARP frames where the hardware address space (HRD) is equal to Ethernet (1).

ether [**0** | **1** | **any**] - Frames can be matched according to their ARP/RARP protocol address space (PRO) settings (Options: **0** - ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry, **1** - ARP/RARP frames where the PRO is equal to IP (0x800), **any** - any value is allowed; Default: **any**)

ip - One of the following IP parameters:

sip - Source IP address (a.b.c.d/n) or **any**.

dip - Destination IP address (a.b.c.d/n) or **any**.

protocol - IP protocol number (0-255) or **any**.

ip-flags - One of the following IP flags:

ttl - Time-to-Live flag with any value.

options - Options flag with any value.

fragment [**0** | **1** | **any**] - Specifies the fragment offset settings for this rule. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. (Options: **0** - IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not match this entry, **1** - IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must match this entry, **any** - any value is allowed; Default: **any**)

icmp - One of the following ICMP parameters:

sip - Source IP address (a.b.c.d/n) or **any**.

dip - Destination IP address (a.b.c.d/n) or **any**.

icmp-type - ICMP type number (0-255) or **any**.

icmp-code - ICMP code number (0-255) or **any**.

ip-flags - One of the IP flags listed under the **ip** parameter.

udp - One of the following UDP parameters:

sip - Source IP address (a.b.c.d/n) or **any**.

dip - Destination IP address (a.b.c.d/n) or **any**.

sport - Source UDP port/range (0-65535) or **any**.

dport - Destination UDP port/range (0-65535) or **any**.

ip-flags - One of the IP flags listed under the **ip** parameter.

tcp - One of the following TCP parameters:

sip - Source IP address (a.b.c.d/n) or **any**.

dip - Destination IP address (a.b.c.d/n) or **any**.

sport - Source TCP port/range (0-65535) or **any**.

dport - Destination TCP port/range (0-65535) or **any**.

ip-flags - One of the IP flags listed under the **ip** parameter.

tcp-flags - One of the following TCP flags:

fin - TCP frames with any value in the FIN field.

syn - TCP frames with any value in the SYN field.

rst - TCP frames with any value in the RST field.

psh - TCP frames with any value in the PSH field.

ack - TCP frames with any value in the ACK field.

urg [**0** | **1** | **any**] - Specifies the TCP "Urgent Pointer field significant" (URG) value for this rule. (Options: **0** - TCP frames where the URG field is set must not match this entry, **1** - TCP frames where the URG field is set must match this entry, **any** - any value is allowed; Default: **any**)

permit - Permits a frame which matches this ACE. (This is the default.)

deny - Drops a frame which matches this ACE.

rate-limiter - Specifies a rate limiter (see the acl rate command, page 298) to apply to the specified ports. (Range: 1-15 or **disable**; Default: Disabled)

port-copy - Defines a port to which matching frames are copied. (Range: 1-28, or **disable**; Default: Disabled)

logging - Enables logging of matching frames to the system log. (Options: **log** or **log_disable**; Default: Disabled)

shutdown - Shuts down an ingress port when a matching frame is seen. (Options: **shut** or **shut_disable**; Default: Disabled)

DEFAULT SETTING

See defaults in Syntax section.

COMMAND USAGE

Rules within an ACL are checked in the configured order, from top to bottom. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted.

EXAMPLE

```
ACL>add port 9 etype any
ACE ID 31 added last
ACL>
```

acl delete

This command deletes an access control entry.

SYNTAX

acl delete *ace-id*

ace-id - An ACL entry. (Range: 1-128)

DEFAULT SETTING

None

EXAMPLE

```
ACL>delete 9
ACL>
```

acl lookup

This command displays the specified access control entry.

SYNTAX

acl lookup [*ace-id*]

ace-id - An ACL entry. (Range: 1-128)

DEFAULT SETTING

Displays all ACEs.

EXAMPLE

```
ACL>lookup 1
ACE ID      : 1                     Rate Limiter: Disabled
Ingress Port: Port 9                Port Copy   : Disabled
Type        : User                  Logging     : Disabled
Frame Type  : Any                   Shutdown    : Disabled
Action      : Permit                Counter     : 0

MAC Parameters                      VLAN Parameters
--------------                      ---------------
DMAC Type   : Any                   VLAN ID     : Any
```

```
                                        Tag Priority: Any
ACL>
```

acl clear This command clears all ACL counters displayed in the ACL lookup table (see the acl lookup command, page 302).

SYNTAX

acl clear

EXAMPLE

```
ACL>clear
ACL>
```

24 MIRROR COMMANDS

This section describes commands used to mirror data to another port for analysis without affecting the data passing through or the performance of the monitored port.

Table 38: Mirror Commands

Command	Function
mirror configuration	Displays the port mirroring configuration
mirror port	Displays or sets the destination port to which data is mirrored
mirror mode	Displays or sets the mirror mode for specified source ports

mirror configuration

This command displays the port mirroring configuration.

SYNTAX

mirror configuration [*port-list*]

port-list - A specific port or a range of ports. (Range: 1-28, or **all**)

EXAMPLE

```
Mirror>configuration 1-5
Mirror Port: 9

Port  Mode
----  --------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
Mirror>
```

mirror port

This command displays or sets the destination port to which data is mirrored.

SYNTAX

mirror port [*port* | **disable**]

port - The destination port that will mirror the traffic from the source port. All mirror sessions must share the same destination port. (Range: 1-28)

disable - Disables mirroring to the destination port.

DEFAULT SETTING

Displays the destination mirror port.

EXAMPLE

```
Mirror>port 9
Mirror>
```

mirror mode

This command displays or sets the mirror mode for specified source ports.

SYNTAX

mirror mode [*port-list*] [**enable** | **disable** | **rx** | **tx**]

port-list - A specific port or range of ports. (Range: 1-28, or **all**)

enable - Mirror both received and transmitted packets.

disable - Disables mirroring from the specified ports.

rx - Mirror received packets.

tx - Mirror transmitted packets.

DEFAULT SETTING

Disabled

EXAMPLE

```
Mirror>mode 10 enable
Mirror>
```

25 CONFIG COMMANDS

This section describes commands used to saves or restore configuration settings.

Table 39: Configuration Commands

Command	Function
config save	Saves configuration settings to a TFTP server
config load	Loads configuration settings from a TFTP server

config save

This command saves the switch's current configuration settings to a file on a TFTP server.

SYNTAX

config save *tftp-server file-name*

tftp-server - TFTP server's IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.

file-name - The name of the file to store on the TFTP server.

COMMAND USAGE

- 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.
- The configuration file is in XML format. The configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire configuration including syntax descriptions is included in the file. The file may be modified using an editor and loaded to a switch.

EXAMPLE

```
Config>save 192.168.1.19 GEL-2870-config
Saved 29683 bytes to server
Config>
```

config load

This command loads configuration settings from a TFTP server to the switch.

SYNTAX

config load *tftp-server file-name* [**check**]

tftp-server - TFTP server's IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.

file-name - The name of a previously saved configuration file. 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 is 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

check - Just check the configuration file for errors, do not apply

DEFAULT SETTING

Check and apply the file.

COMMAND USAGE

You can also restore the factory default settings using the system restore default command (page 187).

EXAMPLE

```
Config>load 192.168.1.19 GEL-2870-config
Config>
```

26 SNMP COMMANDS

This section describes commands used to control access to this switch from management stations using the Simple Network Management Protocol (SNMP), including configuring community strings, trap managers, and basic settings for SNMPv3.

SNMP Version 3 also provides strong security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To configure management access for SNMPv3 clients, you need to first create a user, assign the user to a group, create a view that defines the portions of MIB that the client can read or write, and then create an access entry with the group and view.

Table 40: SNMP Commands

Command	Function
snmp configuration	Displays the SNMP configuration settings
snmp mode	Displays or sets the SNMP administrative mode
snmp version	Displays or sets the SNMP protocol version
snmp read community	Displays or sets the community string for SNMP read access
snmp write community	Displays or sets the community string for SNMP read/write access
snmp trap mode	Displays or sets the SNMP trap mode
snmp trap version	Displays or sets the SNMP trap protocol version
snmp trap community	Displays or sets the community string for SNMP traps
snmp trap destination	Displays or sets the SNMP trap destination's IPv4 address
snmp trap ipv6 destination	Displays or sets the SNMP trap destination's IPv6 address
snmp trap authentication failure	Displays or sets the SNMP authentication failure trap mode
snmp trap link-up	Displays or sets the port link-up and link-down trap mode
snmp trap inform mode	Displays or sets the SNMP trap inform mode
snmp trap inform timeout	Displays or sets the SNMP trap inform time-out
snmp trap inform retry times	Displays or sets the SNMP trap inform retry times
snmp trap probe security engine id	Displays or sets the SNMP trap security engine ID probe mode
snmp trap security engine id	Displays or sets the SNMP trap security engine ID
snmp trap security name	Displays or sets the SNMP trap security name
snmp engine id	Displays or sets the SNMPv3 local engine ID

Table 40: SNMP Commands (Continued)

Command	Function
snmp community add	Adds or modifies an SNMPv3 community entry
snmp community delete	Deletes an SNMPv3 community entry
snmp community lookup	Displays SNMPv3 community entries
snmp user add	Adds an SNMPv3 user entry
snmp user delete	Deletes an SNMPv3 user entry
snmp user changekey	Changes an SNMPv3 user password
snmp user lookup	Displays SNMPv3 user entries
snmp group add	Adds an SNMPv3 group entry
snmp group delete	Deletes an SNMPv3 group entry
snmp group lookup	Displays SNMPv3 group entries
snmp view add	Adds or modifies an SNMPv3 view entry
snmp view delete	Deletes an SNMPv3 view entry
snmp view lookup	Displays SNMPv3 view entries
snmp access add	Adds or modifies an SNMPv3 access entry
snmp access delete	Deletes an SNMPv3 access entry
snmp access lookup	Displays SNMPv3 access entries

snmp configuration

This command displays the SNMP configuration settings.

SYNTAX

snmp configuration

COMMAND USAGE

This command provides information on all SNMP configuration settings, including communities, users, groups, views, and access tables.

EXAMPLE

```
SNMP>configuration
SNMP Mode                     : Disabled
SNMP Version                  : 2c
Read Community                : public
Write Community               : private
Trap Mode                     : Disabled
Trap Version                  : 1
Trap Community                : public
Trap Destination              :
Trap IPv6 Destination         : ::
Trap Authentication Failure   : Enabled
Trap Link-up and Link-down    : Enabled
Trap Inform Mode              : Disabled
Trap Inform Timeout (seconds) : 1
Trap Inform Retry Times       : 5
Trap Probe Security Engine ID : Enabled
```

```
Trap Security Engine ID       :
Trap Security Name            : None

SNMPv3 Engine ID : 800007e5017f000001

SNMPv3 Communities Table:
Idx Community                          Source IP        Source Mask
--- ------------------------------- --------------- ---------------
1   public                          0.0.0.0          0.0.0.0
2   private                         0.0.0.0          0.0.0.0
3    tps                             192.168.1.0      255.255.255.0

Number of entries: 3

SNMPv3 Users Table:
Idx Engine ID User Name                          Level          Auth Priv
--- --------- ------------------------------- -------------- ---- ----
1   Local     default_user                      NoAuth, NoPriv None None

Number of entries: 1

SNMPv3 Groups Table;
Idx Model Security Name                    Group Name
--- ----- -------------------------------- --------------------------------
1   v1    public                           default_ro_group
2   v1    private                          default_rw_group
3   v2c   public                           default_ro_group
4   v2c   private                          default_rw_group
5   usm   default_user                     default_rw_group

Number of entries: 5

SNMPv3 Views Table:
Idx View Name                      View Type OID Subtree
--- ------------------------------ --------- --------------------------
1   default_view                   included  .1

Number of entries: 1

SNMPv3 Accesses Table:
Idx Group Name                     Model Level
--- ------------------------------ ----- --------------
1   default_ro_group               any   NoAuth, NoPriv
2   default_rw_group               any   NoAuth, NoPriv

Number of entries: 2
SNMP>
```

snmp mode

This command displays or sets the SNMP administrative mode.

SYNTAX

snmp mode [**enable** | **disable**]

enable - Enables SNMP service.

disable - Disables SNMP service.

DEFAULT SETTING

Disabled

COMMAND USAGE
To manage the switch through SNMP, you must first enable the protocol and configure the basic access parameters.

EXAMPLE

```
SNMP>mode enable
SNMP>
```

snmp version

This command displays or sets the SNMP protocol version.

SYNTAX

snmp version [**1** | **2c** | **3**]

1 - SNMP version 1.

2c - SNMP version 2c.

3 - SNMP version 3.

DEFAULT SETTING
Displays current SNMP version.

EXAMPLE

```
SNMP>version 3
SNMP>
```

snmp read community

This command displays or sets the community string for SNMP read access.

SYNTAX

snmp read community [*community*]

community - The community string used for read-only access to the SNMP agent. (Range: 0-255 characters, ASCII characters 33-126 only)

DEFAULT SETTING
public

COMMAND USAGE
This parameter only applies to SNMPv1 and SNMPv2c. SNMPv3 uses the User-based Security Model (USM) for authentication and privacy. This community string is associated with SNMPv1 or SNMPv2 clients in the SNMPv3 communities table (see the snmp community lookup command on page 320).

EXAMPLE

```
SNMP>read community tps
SNMP>
```

snmp write community

This command displays or sets the community string for SNMP read/write access.

SYNTAX

snmp write community [*community*]

community - The community used for read/write access to the SNMP agent. (Range: 0-255 characters, ASCII characters 33-126 only)

DEFAULT SETTING

private

COMMAND USAGE

This parameter only applies to SNMPv1 and SNMPv2c. SNMPv3 uses the User-based Security Model (USM) for authentication and privacy. This community string is associated with SNMPv1 or SNMPv2 clients in the SNMPv3 communities table (see the snmp community lookup command on page 320).

EXAMPLE

```
SNMP>write community r&d
SNMP>
```

snmp trap mode

This command displays or sets the SNMP trap mode.

SYNTAX

snmp trap mode [**enable** | **disable**]

enable - Enables SNMP traps.

disable - Disables SNMP traps.

DEFAULT SETTING

Disabled

COMMAND USAGE

You should enable SNMP traps so that key events are reported by this switch to your management station. Traps indicating status changes can be issued by the switch to the specified trap manager by sending authentication failure messages and other trap messages.

EXAMPLE

```
SNMP/Trap>mode enable
SNMP/Trap>
```

snmp trap version

This command displays or sets the SNMP trap protocol version.

SYNTAX

snmp trap version [**1** | **2c** | **3**]

1 - SNMP version 1.

2c - SNMP version 2c.

3 - SNMP version 3.

DEFAULT SETTING

SNMP v1

COMMAND USAGE

This command specifies whether to send notifications as SNMP v1, v2c, or v3 traps.

EXAMPLE

```
SNMP/Trap>version 3
SNMP/Trap>
```

snmp trap community

This command displays or sets the community string for SNMP traps.

SYNTAX

snmp trap community [*community*]

community - The community access string to use when sending SNMP trap packets. (Range: 0-255 characters, ASCII characters 33-126 only)

DEFAULT SETTING

public

EXAMPLE

```
SNMP/Trap>community r&d
SNMP/Trap>
```

snmp trap destination

This command displays or sets the SNMP trap destination's IPv4 address.

SYNTAX

snmp trap destination [*ip-address*]

ip-address - IPv4 address or alias of the management station to receive notification messages. An IPv4 address consists of 4 numbers, 0 to 255, separated by periods.

DEFAULT SETTING

Displays trap destination.

EXAMPLE

```
SNMP/Trap>destination 192.168l.2.19
SNMP/Trap>
```

snmp trap ipv6 destination

This command displays or sets the SNMP trap destination's IPv6 address.

SYNTAX

snmp trap ipv6 destination [*ipv6-address*]

ipv6-address - IPv6 address of the management station to receive notification messages. An IPv6 address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.

DEFAULT SETTING

Displays trap destination.

EXAMPLE

```
SNMP/Trap>ipv6 destination 2001:DB8:2222:7272::72
SNMP/Trap>
```

snmp trap authentication failure

This command displays or sets the SNMP authentication failure trap mode.

SYNTAX

snmp trap authentication failure [**enable** | **disable**]

enable - Enables sending SNMP authentication failure traps.

disable - Disables sending SNMP authentication failure traps.

DEFAULT SETTING

Enabled

COMMAND USAGE
When this function is enabled, the switch will issue a notification message to specified IP trap managers whenever authentication of an SNMP request fails.

EXAMPLE

```
SNMP/Trap>authentication failure enable
SNMP/Trap>
```

snmp trap link-up

This command displays or sets the port link-up and link-down trap mode.

SYNTAX

snmp trap link-up [**enable** | **disable**]

enable - Enables sending link-up and link-down traps.

disable - Disables sending link-up and link-down traps.

DEFAULT SETTING
Enabled

COMMAND USAGE
When this function is enabled, the switch will issue a notification message whenever a port link is established or broken.

EXAMPLE

```
SNMP/Trap>link-up enable
SNMP/Trap>
```

snmp trap inform mode

This command displays or sets the SNMP trap inform mode.

SYNTAX

snmp trap inform mode [**enable** | **disable**]

enable - Enables sending notifications as inform messages.

disable - Disables sending notifications as inform messages.

DEFAULT SETTING
Traps are used

COMMAND USAGE
- This option is only available for version 2c and 3 hosts.
- 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.

EXAMPLE

```
SNMP/Trap/Inform>mode enable
SNMP/Trap/Inform>
```

snmp trap inform timeout

This command displays or sets the SNMP trap inform timeout.

SYNTAX

snmp trap inform timeout [*timeout*]

timeout - The number of seconds to wait for an acknowledgment before re-sending an inform message. (Range: 0-2147 seconds)

DEFAULT SETTING

1 second

EXAMPLE

```
SNMP/Trap/Inform>timeout 5
SNMP/Trap/Inform>
```

snmp trap inform retry times

This command displays or sets the retry times for re-sending an SNMP trap inform when the recipient does not acknowledge receipt.

SYNTAX

snmp trap inform retry times [*retries*]

retries - The maximum number of times to re-send an inform message if the recipient does not acknowledge receipt. (Range: 0-255)

DEFAULT SETTING

5

EXAMPLE

```
SNMP/Trap/Inform>retry times 1
SNMP/Trap/Inform>
```

snmp trap probe security engine id

This command displays or sets the SNMP trap security engine ID probe mode.

SYNTAX

snmp trap probe security engine id [**enable** | **disable**]

enable - Enable SNMP trap security engine ID probe mode, whereby the switch uses the engine ID of the SNMP trap probe in trap and inform messages.

disable - Disables SNMP trap security engine ID probe mode.

DEFAULT SETTING

Enabled

EXAMPLE

```
SNMP/Trap>probe security engine id enable
SNMP/Trap>
```

snmp trap security engine id

This command displays or sets the SNMP trap security engine ID.

SYNTAX

snmp trap security engine id [*engine-id*]

engine-id - Specifies the SNMP trap security engine ID. (Range: 10-64 hex digits, excluding a string of all 0's or all F's)

DEFAULT SETTING

None

COMMAND USAGE

- SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When trap probe security engine ID is enabled (see page 317), the ID will be probed automatically. Otherwise, the ID specified by this command is used.
- The Trap Probe Security Engine ID must be disabled (see page 317) before an engine ID can be manually entered with this command.

EXAMPLE

```
SNMP/Trap>probe security engine id disable
SNMP/Trap>security engine id 800007e5017f000002
SNMP/Trap>
```

snmp trap security name

This command displays or sets the SNMP trap security name.

SYNTAX

snmp trap security name [*security-name*]

security-name - Specifies the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when SNMPv3 traps or informs are enabled.

DEFAULT SETTING

None

COMMAND USAGE

Before entering a trap security name with this command, first enter an SNMPv3 user with the snmp user add command (page 320).

EXAMPLE

```
SNMP>user add 800007e5017f000002 steve
SNMP>trap security name steve
SNMP>
```

snmp engine id

This command displays or sets the SNMPv3 local engine ID.

SYNTAX

snmp engine id [*engine-id*]

engine-id - The SNMPv3 engine ID. (Range: 10-64 hex digits, excluding a string of all 0's or all F's)

DEFAULT SETTING

800007e5017f000001

COMMAND USAGE

- 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 local SNMP users will be cleared. You will need to reconfigure all existing users.

EXAMPLE

```
SNMP>engine id 800007e5017f000005
Changing Engine ID will clear all original local users
SNMP>
```

snmp community add

This command adds or modifies an SNMPv3 community entry.

SYNTAX

snmp community add *community* [*ip-address*] [*address-mask*]

community - Specifies the community strings which allow access to the SNMP agent. (Range: 1-32 characters, ASCII characters 33-126 only)

For SNMPv3, these strings are treated as a security name (see the snmp trap security name command, page 318), and are mapped as an SNMPv1 or SNMPv2 community string in the SNMPv3 groups table (see snmp group add command, page 323).

ip-address - Specifies the source address of an SNMP client.

address-mask - Specifies the address mask for the SNMP client.

DEFAULT SETTING

public, private

COMMAND USAGE

- All community strings used to authorize access by SNMP v1 and v2c clients should be listed in the SNMPv3 communities table. For security reasons, you should consider removing the default strings.
- Add any new community strings required for SNMPv1 or v2 clients that need to access the switch, along with the source address and address mask for each client.
- Up to 64 community names can be configured.

EXAMPLE

```
SNMP/Community>add r&d 192.168.1.19 255.255.255.0
SNMP/Community>
```

snmp community delete

This command deletes an SNMPv3 community entry.

SYNTAX

snmp community delete *index*

index - Index to SNMP community table. (Range: 1-64)

DEFAULT SETTING
None

EXAMPLE

```
SNMP/Community>lookup
Idx Community                        Source IP        Source Mask
--- -------------------------------- ---------------- ---------------
1   public                           0.0.0.0          0.0.0.0
2   private                          0.0.0.0          0.0.0.0
3   r&d                              192.168.1.19     255.255.255.0
4   tps                              192.168.1.18     255.255.255.0

Number of entries: 4
SNMP/Community>delete 4
SNMP/Community>
```

snmp community lookup

This command displays SNMPv3 community entries.

SYNTAX

snmp community lookup [*index*]

index - Index to SNMP community table. (Range: 1-64)

DEFAULT SETTING
Displays all entries.

EXAMPLE

```
SNMP/Community>lookup
Idx Community                        Source IP        Source Mask
--- -------------------------------- ---------------- ---------------
1   public                           0.0.0.0          0.0.0.0
2   private                          0.0.0.0          0.0.0.0
3   r&d                              192.168.1.19     255.255.255.0

Number of entries: 3
SNMP/Community>
```

snmp user add

This command adds an SNMPv3 user entry.

SYNTAX

snmp user add *engine-id user-name* [**md5** | **sha**] [*auth-password*] [**des**] [*priv-password*]

engine-id - The engine identifier for the SNMP agent on the remote device where the user resides. (Range: 10-64 hex digits, excluding a string of all 0's or all F's)

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 the snmp trap security engine id command on page 317.)

user-name - The name of user connecting to the SNMP agent. (Range: 1-32 characters, ASCII characters 33-126 only)

md5 | **sha** - The method used for user authentication.

auth-password - A plain text string identifying the authentication pass phrase. (Range: 1-32 characters for MD5, 8-40 characters for SHA)

des - The encryption algorithm use for data privacy; only 56-bit DES is currently available.

priv-password - A string identifying the privacy pass phrase. (Range: 8-40 characters, ASCII characters 33-126 only)

DEFAULT SETTING

Authentication method: MD5

COMMAND USAGE

- Each SNMPv3 user is defined by a unique name and remote engine ID. Users must be configured with a specific security level, and the types of authentication and privacy protocols to use.
- Any user created with this command is associated with the group assigned to the USM Security Model with the snmp group add command (page 323), and the views assigned to that group with the snmp view add command (page 325).
- Up to 64 user names can be configured.

EXAMPLE

```
SNMP/User>add 800007e5017f000009 steve sha elephant des hippopotams
SNMP/User>
```

snmp user delete

This command deletes an SNMPv3 user entry.

SYNTAX

snmp user delete *index*

index - Index to SNMPv3 user table. (Range: 1-64)

DEFAULT SETTING

None

EXAMPLE

```
SNMP/User>lookup
Idx Engine ID User Name                          Level          Auth Priv
--- --------- ------------------------------- -------------- ---- ----
1   Remote    william                         Auth, Priv     SHA  DES
2   Remote    steve                           Auth, Priv     SHA  DES

Number of entries: 2
SNMP/User>delete 2
SNMP/User>
```

snmp user changekey

This command changes an SNMPv3 user password.

SYNTAX

snmp user changekey *engine-id user-name auth-password* [*priv-password*]

engine-id - The engine identifier for the SNMP agent on the remote device where the user resides. (Range: 10-64 hex digits, excluding a string of all 0's or all F's)

user-name - The name of user connecting to the SNMP agent. (Range: 1-32 characters, ASCII characters 33-126 only)

auth-password - A plain text string identifying the authentication pass phrase. (Range: 1-32 characters for MD5, 8-40 characters for SHA)

priv-password - A string identifying the privacy pass phrase. (Range: 8-40 characters, ASCII characters 33-126 only)

DEFAULT SETTING

None

EXAMPLE

```
SNMP/User>changekey 800007e5017f000007 william dogtails cattails
SNMP/User>
```

snmp user lookup

This command displays SNMPv3 user entries.

SYNTAX

snmp user lookup [*index*]

index - Index to SNMPv3 user table. (Range: 1-64)

DEFAULT SETTING

Displays all entries.

EXAMPLE

```
SNMP/User>lookup
Idx Engine ID User Name                          Level          Auth Priv
--- --------- ------------------------------- -------------- ---- ----
1   Remote    william                         Auth, Priv     SHA  DES

Number of entries: 1
SNMP/User>
```

snmp group add

This command adds an SNMPv3 group entry.

SYNTAX

snmp group add *security-model security-name group-name*

security-model - The user security model. (Options: v1, v2c, or the User-based Security Model – usm)

security-name - The name of user connecting to the SNMP agent. (Range: 1-32 characters, ASCII characters 33-126 only)

The options available for this parameter depend on the selected Security Model. For SNMP v1 and v2c, the names configured with the snmp community add command (page 319) can be used. For USM (or SNMPv3), the names configured with the local engine ID with the snmp user add command (page 320) can be used. To modify an entry for USM, the current entry must first be deleted.

group-name - The name of the SNMP group. (Range: 1-32 characters, ASCII characters 33-126 only)

DEFAULT SETTING

None

COMMAND USAGE

- An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read and write views as defined by the snmp access add command (page 326). You can use the pre-defined default groups, or create a new group and the views authorized for that group.
- Note that the views assigned to a group must be specified with the snmp view add command (page 325).

EXAMPLE

```
SNMP>user add 800007e5017f000005 steve sha elephant des hippopotamus
SNMP>group add usm steve tps
SNMP>
```

snmp group delete

This command deletes an SNMPv3 group entry.

SYNTAX

snmp group delete *index*

index - Index to SNMPv3 group table. (Range: 1-64)

DEFAULT SETTING

None

EXAMPLE

```
SNMP/Group>lookup
Idx Model Security Name                    Group Name
--- ----- -------------------------------- --------------------------------
1   v1    public                           default_ro_group
2   v1    private                          default_rw_group
3   v2c   public                           default_ro_group
4   v2c   private                          default_rw_group
5   usm   default_user                     default_rw_group
6   usm   steve                            tps

Number of entries: 6
SNMP/Group>delete 6
SNMP/Group>
```

snmp group lookup

This command displays SNMPv3 group entries.

SYNTAX

snmp group lookup [*index*]

index - Index to SNMPv3 group table. (Range: 1-64)

DEFAULT SETTING

Displays all entries.

EXAMPLE

```
SNMP/Group>lookup
Idx Model Security Name                    Group Name
--- ----- -------------------------------- --------------------------------
1   v1    public                           default_ro_group
2   v1    private                          default_rw_group
3   v2c   public                           default_ro_group
4   v2c   private                          default_rw_group
5   usm   default_user                     default_rw_group
6   usm   steve                            tps

Number of entries: 6
SNMP/Group>
```

snmp view add

This command adds or modifies an SNMPv3 view entry.

SYNTAX

snmp view add *view-name* [**included** | **excluded**] *oid-subtree*

view-name - The name of the SNMP view. (Range: 1-32 characters, ASCII characters 33-126 only)

included | **excluded** - Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view. Generally, if the view type of an entry is "excluded," another entry of view type "included" should exist and its OID subtree should overlap the "excluded" view entry.

oid-subtree - Object identifiers of branches within the MIB tree. Note that the first character must be a period (.). Wild cards can be used to mask a specific portion of the OID string using an asterisk. (Length: 1-128)

DEFAULT SETTING

None

COMMAND USAGE

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

EXAMPLE

```
SNMP/View>add ifEntry.a included .1.3.5.1.2.1.2.2.1.1.*
SNMP/View>
```

snmp view delete

This command deletes an SNMPv3 view entry.

SYNTAX

snmp view delete *index*

index - Index to SNMPv3 view table. (Range: 1-64)

DEFAULT SETTING

None

EXAMPLE

```
SNMP/View>lookup
Idx View Name                        View Type OID Subtree
--- -------------------------------- --------- --------------------------
1   default_view                     included  .1
2   ifEntry.a                        included  .1.3.5.1.2.1.2.2.1.1.*

Number of entries: 2
```

```
SNMP/View>delete 2
SNMP/View>
```

snmp view lookup

This command displays SNMPv3 view entries.

SYNTAX

snmp view lookup [*index*]

index - Index to SNMPv3 view table. (Range: 1-64)

DEFAULT SETTING

Displays all entries.

EXAMPLE

```
SNMP/View>lookup
Idx View Name                        View Type OID Subtree
--- -------------------------------- --------- --------------------------
1   default_view                     included  .1
2   ifEntry.a                        included  .1.3.5.1.2.1.2.2.1.1.*

Number of entries: 2
SNMP/View>
```

snmp access add

This command adds or modifies an SNMPv3 access entry.

SYNTAX

snmp access add *group-name security-model security-level* [*read-view-name*] [*write-view-name*]

group-name - The name of the SNMP group. (Range: 1-32 characters, ASCII characters 33-126 only)

security-model - The user security model. (Options: any, v1, v2c, or the User-based Security Model – usm)

security-level - The security level assigned to the group.

noAuthNoPriv - There is no authentication or encryption used in SNMP communications.

AuthNoPriv - SNMP communications use authentication, but the data is not encrypted.

AuthPriv - SNMP communications use both authentication and encryption.

read-view-name - The configured view for read access. (Range: 1-32 characters, ASCII characters 33-126 only)

write-view-name - The configured view for write access. (Range: 1-32 characters, ASCII characters 33-126 only)

DEFAULT SETTING
Security model: any
Security level: noAuthNoPriv

COMMAND USAGE
Use this command to assign portions of the MIB tree to which each SNMPv3 group is granted access. You can assign more than one view to a group to specify access to different portions of the MIB tree.

EXAMPLE

```
SNMP/Access>add r&d usm authpriv default_view ifEntry.a
SNMP/Access>
```

snmp access delete

This command deletes an SNMPv3 access entry.

SYNTAX

snmp access delete *index*

index - Index to SNMPv3 access table. (Range: 1-64)

DEFAULT SETTING
None

EXAMPLE

```
SNMP/Access>lookup
Idx Group Name                       Model Level
--- -------------------------------- ----- --------------
1   default_ro_group                 any   NoAuth, NoPriv
2   default_rw_group                 any   NoAuth, NoPriv
3   r&d                              usm   Auth, Priv

Number of entries: 3
SNMP/Access>delete 3
SNMP/Access>
```

snmp access lookup

This command displays SNMPv3 access entries.

SYNTAX

snmp access lookup [*index*]

index - Index to SNMPv3 access table. (Range: 1-64)

DEFAULT SETTING
Displays all entries.

EXAMPLE

```
SNMP/Access>lookup
Idx Group Name                       Model Level
--- -------------------------------- ----- --------------
1   default_ro_group                 any   NoAuth, NoPriv
2   default_rw_group                 any   NoAuth, NoPriv
3   r&d                              usm   Auth, Priv

Number of entries: 3
SNMP/Access>
```

27 HTTPS COMMANDS

This section describes commands used to enables or disable HTTPS, or automatically redirect management access from HTTP connections to HTTPS.

Table 41: HTTPS Commands

Command	Function
https configuration	Displays HTTPS configuration settings
https mode	Displays or sets HTTPS operational mode
https redirect	Displays or sets HTTPS redirect mode from HTTP connections

https configuration

This command displays HTTPS configuration settings.

SYNTAX

https configuration

EXAMPLE

```
HTTPS>configuration
HTTPS Mode          : Disabled
HTTPS Redirect Mode : Disabled
HTTPS>
```

https mode

This command displays or sets HTTPS operational mode.

SYNTAX

https mode [**enable** | **disable**]

enable - Enables HTTPS service on the switch.

disable - Disables HTTPS service on the switch.

DEFAULT SETTING

Disabled

COMMAND USAGE

- 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.

- 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, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above.
- The following web browsers and operating systems currently support HTTPS:

Table 42: 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, Windows Vista
Netscape 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows Vista, Solaris 2.6
Mozilla Firefox 2.0.0.0 or later	Windows 2000, Windows XP, Windows Vista, Linux

EXAMPLE

```
HTTPS>mode enable
HTTPS>
```

https redirect

This command displays or sets HTTPS redirect mode from HTTP connections.

SYNTAX

https redirect [**enable** | **disable**]

enable - Enables HTTPS redirect. When enabled, management access to the HTTP web interface for the switch are automatically redirected to HTTPS.

disable - Disables HTTPS redirect.

DEFAULT SETTING

Disabled

EXAMPLE

```
HTTPS>redirect enable
HTTPS>
```

28 SSH COMMANDS

This section describes commands used to enable or disable management access via secure shell (SSH).

Table 43: SSH Commands

Command	Function
ssh configuration	Displays SSH configuration settings
ssh mode	Displays or sets SSH operational mode

ssh configuration

This command displays SSH configuration settings.

SYNTAX

ssh configuration

EXAMPLE

```
SSH>configuration
SSH Mode : Disabled
SSH>
```

ssh mode

This command displays or sets SSH operational mode.

SYNTAX

ssh mode [**enable** | **disable**]

enable - Enables SSH service on the switch.

disable - Disables HTTPS service on the switch.

DEFAULT SETTING

Disabled

COMMAND USAGE

- SSH provides 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.

- You need to install an SSH client on the management station to access the switch for management via the SSH protocol. The switch supports both SSH Version 1.5 and 2.0 clients.

- SSH service on this switch only supports password authentication. The password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified the auth radius command (page 207) or auth tacacs+ command (page 210).

  To use SSH with 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.

- The SSH service on the switch supports up to four client sessions.

EXAMPLE

```
SSH>mode enable
SSH>
```

29 UPnP Commands

This section describes commands used to configure Universal Plug and Play (UPnP) protocol settings.

Table 44: UPnP Commands

Command	Function
upnp configuration	Displays UPnP configuration settings
upnp mode	Displays or sets UPnP operational mode
upnp ttl	Displays or sets the TTL value for UPnP messages
upnp advertising duration	Displays or sets the advertising duration of UPnP messages

upnp configuration

This command displays UPnP configuration settings.

Syntax

upnp configuration

Example

```
UPnP>configuration
UPnP Mode                 : Disabled
UPnP TTL                  : 4
UPnP Advertising Duration : 100
UPnP>
```

upnp mode

This command displays or sets UPnP operational mode.

Syntax

upnp mode [**enable** | **disable**]

enable - Enables UPnP on the switch.

disable - Disables UPnP on the switch.

Default Setting

Disabled

Command Usage

The first step in UPnP networking is discovery. When a device is added to the network, the UPnP discovery protocol allows that device to broadcast 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 UPnP enabled devices on the network.

Once a control point has discovered a device its next step is to learn more about the device and its capabilities by retrieving 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, it can send actions to the 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).

When a device is known to the control point, periodic event notification messages are sent. 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.

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.

EXAMPLE

```
UPnP>mode enable
UPnP>
```

upnp ttl

This command displays or sets the TTL value for UPnP messages.

SYNTAX

upnp ttl [*ttl*]

ttl - The time-to-live (TTL) value for UPnP messages transmitted by the switch. This is the number of router hops a UPnP packet can travel before it is discarded. (Range: 4-255)

DEFAULT SETTING

4

COMMAND USAGE

- This command specifies the number of router hops a UPnP packet can travel before it is discarded.
- UPnP devices and control points must be within the local network, that is, within the TTL value for multicast messages.

EXAMPLE

```
UPnP>ttl 255
UPnP>
```

upnp advertising duration

This command displays or sets the advertising duration of UPnP messages.

SYNTAX

upnp advertising duration [*duration*]

duration - The duration, carried in Simple Service Discover Protocol (SSDP) packets, which informs a control point or control points how often it or they should receive a SSDP advertisement message from this switch. Due to the unreliable nature of UDP, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. (Range: 100-86400 seconds)

DEFAULT SETTING

100 seconds

EXAMPLE

```
UPnP>advertising duration
UPnP>
```

30 DHCP COMMANDS

This section describes commands used to configure DHCP Relay and Option 82 Information.

Table 45: DHCP Commands

Command	Function
dhcp relay configuration	Displays DHCP relay configuration settings
dhcp relay mode	Displays or sets DHCP relay operational mode
dhcp relay server	Displays or sets the IP address of the DHCP relay server
dhcp relay information mode	Displays or sets the DHCP Relay Option 82 mode
dhcp relay information policy	Displays or sets the DHCP relay policy for DHCP client packets that include Option 82 information
dhcp relay statistics	Displays or clears DHCP relay statistics

dhcp relay configuration

This command displays DHCP relay configuration settings.

SYNTAX

dhcp relay configuration

EXAMPLE

```
DHCP/Relay>configuration
DHCP Relay Mode               : Disabled
DHCP Relay Server             : NULL
DHCP Relay Information Mode   : Disabled
DHCP Relay Information Policy : replace
DHCP/Relay>
```

dhcp relay mode

This command displays or sets DHCP relay operational mode.

SYNTAX

dhcp relay mode [**enable** | **disable**]

enable - Enables the DHCP relay function.

disable - Disables the DHCP relay function.

DEFAULT SETTING

Disabled

COMMAND USAGE

- The switch supports DHCP relay service for attached host devices. If a subnet does not include a DHCP server, you can relay DHCP client requests to a DHCP server on another subnet.
- When DHCP relay is enabled and the switch sees a DHCP request broadcast, it inserts its own IP address into the request (so that the DHCP server knows the subnet of the client), then forwards the packet to the DHCP server. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the switch. The switch then broadcasts the DHCP response to the client.
- A DHCP relay server must first be configured (see the dhcp relay server command on page 338) before DHCP relay mode can be enabled with this command.

EXAMPLE

```
DHCP/Relay>mode enable
DHCP/Relay>
```

dhcp relay server

This command displays or sets the IP address of the DHCP relay server.

SYNTAX

dhcp relay server [*ip-address*]

ip-address - IP address of DHCP server to be used by the switch's DHCP relay agent.

DEFAULT SETTING

None

EXAMPLE

```
DHCP/Relay>server 192.168.1.25
DHCP/Relay>
```

dhcp relay information mode

This command displays or sets the DHCP Relay Option 82 mode.

SYNTAX

dhcp relay information mode [**enable** | **disable**]

enable - Enables DHCP Relay Option 82 support. Note that DHCP relay mode must also be enabled with the dhcp relay mode command (see page 337) for DHCP relay information mode to take effect.

disable - Disables DHCP Relay Option 82 support.

DEFAULT SETTING
Disabled

COMMAND USAGE
- DHCP also provides a 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.
- Using DHCP Relay Option 82, clients can be identified by the VLAN and 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.

EXAMPLE

```
DHCP/Relay/Information>mode enable
DHCP/Relay/Information>
```

dhcp relay information policy

This command displays or sets the DHCP relay policy for DHCP client packets that include Option 82 information.

SYNTAX

dhcp relay information policy [**replace** | **keep** | **drop**]

replace - Overwrites the DHCP client packet information with the switch's relay information.

keep - Retains the client's DHCP information.

drop - Drops the packet when it receives a DHCP message that already contains relay information.

DEFAULT SETTING
Replace Option 82 information

EXAMPLE

```
DHCP/Relay/Information>policy keep
DHCP/Relay/Information>
```

dhcp relay statistics

This command displays or clears DHCP relay statistics.

SYNTAX

dhcp relay statistics [**clear**]

clear - Clears DHCP relay statistics.

DEFAULT SETTING
Displays DHCP statistics

COMMAND USAGE
For a description of the information displayed by this command, see "Displaying DHCP Relay Statistics" on page 164.

EXAMPLE

```
DHCP/Relay>statistics

Server Statistics:
------------------
Transmit to Server         :          0   Transmit Error               :          0
Receive from Server        :          0   Receive Missing Agent Option :          0
Receive Missing Circuit ID :          0   Receive Missing Remote ID    :          0
Receive Bad Circuit ID     :          0   Receive Bad Remote ID        :          0

Client Statistics:
--------------------
Transmit to Client   :          0   Transmit Error       :          0
Receive from Client  :          0   Receive Agent Option :          0
Replace Agent Option :          0   Keep Agent Option    :          0
Drop Agent Option    :          0

DHCP/Relay>
```

31 FIRMWARE COMMANDS

This section describes commands used to upgrade firmware via a TFTP server.

Table 46: Firmware Commands

Command	Function
firmware load	Loads new firmware from an IPv4 TFTP server
firmware ipv6 load	Loads new firmware from an IPv6 TFTP server

firmware load

This command loads new firmware from a TFTP server using an IPv4 address.

SYNTAX

firmware load *tftp-server file-name*

tftp-server - TFTP server's IPv4 address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.

file-name - The name of the file to load from the TFTP server. The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.). (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

COMMAND USAGE

- You can upgrade the switch's system firmware by specifying a file provided by Transition Networks. You can download firmware files for your switch from the Support section of the Transition Networks web site at www.transition.com.
- After the software image is uploaded, a message announces that the firmware update has been initiated. After about a minute, the firmware is updated and the switch is rebooted.

CAUTION: While the firmware is being updated, the switch cannot be accessed through any management protocol. The front LED flashes Green/Off at a frequency of 10 Hz while the firmware update is in progress. Do not reset or power off the device at this time or the switch may fail to function afterwards.

EXAMPLE

```
Firmware>load 192.168.1.19 GEL-2870-0_7_smbstax_estax_34.dat
Downloaded "GEL-2870-0_7_smbstax_estax_34.dat", 1812567 bytes
```

```
Master initiated software updating starting
Waiting for firmware update to complete
Transferred image to switch 1
All switches confirmed reception, programming
Starting flash update - do not power off device!
Erasing image...
Programming image...
... Erase from 0x807e0000-0x807effff: .
... Program from 0x01ff0000-0x02000000 to 0x807e0000: .
... Program from 0x01ff000a-0x01ff000c to 0x807e000a: .
Flash update succeeded.
+
RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_12 - built 10:20:10, Jul  6 2009
Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCOREII system (ARM9) @178MHz
RAM: 0x00000000-0x02000000 [0x0002c348-0x01fe1000 available]
FLASH: 0x80000000-0x807fffff, 128 x 0x10000 blocks
== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> led_set -g
RedBoot> diag -d -m -h
Memory BIST: Running... Done
DDR SDRAM: Testing [0x0002c348-0x01fe1000]... Done
H/W specific tests: Running... Done
RedBoot> led_set -g
RedBoot> fis load -a managed
Image loaded from 0x00100000-0x00445a9c
RedBoot> go

Username:
```

firmware ipv6 load

This command loads new firmware from an IPv6 TFTP server.

SYNTAX

firmware ipv6 load *ipv6-tftp-server file-name*

ipv6-tftp-server - TFTP server's IPv6 address. All IPv6 addresses must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

file-name - The name of the file to load from the TFTP server. The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.). (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

COMMAND USAGE

See the Command Usage section under the firmware load command on page 341.

EXAMPLE

```
Firmware>ipv6 load 2001:DB8:2222:7272::72 GEL-2870-0_7_smbstax_estax_34.dat
Downloaded "GEL-2870-0_7_smbstax_estax_34.dat", 1812567 bytes
:
RedBoot> go

Username:
```

SECTION IV

APPENDICES

This section provides additional information and includes these items:

- "Software Specifications" on page 345
- "Troubleshooting" on page 349

A SOFTWARE SPECIFICATIONS

SOFTWARE FEATURES

AUTHENTICATION	Local, RADIUS, TACACS+, Port (802.1X), AAA, HTTPS, SSH, Port Security, IP Filter, DHCP Snooping
ACCESS CONTROL LISTS	128 rules per system
PORT CONFIGURATION	1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex 100BASE-BX - 100 Mbps at full duplex (SFP) 1000BASE-BX/SX/LX/LH - 1000 Mbps at full duplex (SFP)
FLOW CONTROL	Full Duplex: IEEE 802.3-2005 Half Duplex: Back pressure
STORM CONTROL	Broadcast, multicast, or unicast traffic throttled above a critical threshold
PORT MIRRORING	Multiple source ports, one destination port
RATE LIMITS	Input/ouput limit per port (using ACL)
PORT TRUNKING	Static trunks (Cisco EtherChannel compliant) Dynamic trunks (Link Aggregation Control Protocol)
SPANNING TREE ALGORITHM	Spanning Tree Protocol (STP, IEEE 802.1D-2004) Rapid Spanning Tree Protocol (RSTP, STP, IEEE 802.1D-2004)
VLAN SUPPORT	Up to 256 groups; port-based, protocol-based, or tagged (802.1Q) private VLANs

CLASS OF SERVICE
Supports four levels of priority
Strict or Weighted Round Robin queueing
Queue mode and CoS configured by Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS bit, VLAN tag priority, or port
Layer 3/4 priority mapping: IP DSCP remarking

QUALITY OF SERVICE
DiffServ supports DSCP remarking, ingress traffic policing, and egress traffic shaping

MULTICAST FILTERING
IGMP Snooping

ADDITIONAL FEATURES
DHCP Client
DNS Proxy
LLDP (Link Layer Discover Protocol)
RMON (Remote Monitoring, groups 1,2,3,9)
SMTP Email Alerts
SNMP (Simple Network Management Protocol)
SNTP (Simple Network Time Protocol)
UPnP

MANAGEMENT FEATURES

IN-BAND MANAGEMENT
Telnet, web-based HTTP or HTTPS, SNMP manager, or Secure Shell

OUT-OF-BAND MANAGEMENT
RS-232 DB-9 console port
Software Loading: HTTP or TFTP in-band, or XModem out-of-band

SNMP
Management access via MIB database
Trap management to specified hosts

RMON
Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

STANDARDS

IEEE 802.1AB Link Layer Discovery Protocol
IEEE 802.1D-2004 Spanning Tree Algorithm and traffic priorities
  Spanning Tree Protocol
  Rapid Spanning Tree Protocol
IEEE 802.1p Priority tags
IEEE 802.1Q VLAN
IEEE 802.1X Port Authentication
IEEE 802.3-2005
  Ethernet, Fast Ethernet, Gigabit Ethernet
  Link Aggregation Control Protocol (LACP)
IEEE 802.3ac VLAN tagging
ARP (RFC 826)
DHCP Client (RFC 2131)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
IGMPv3 (RFC 3376) - partial support
RADIUS+ (RFC 2618)
RMON (RFC 2819 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)

MANAGEMENT INFORMATION BASES

Bridge MIB (RFC 1493)
Differentiated Services MIB (RFC 3289)
DNS Resolver MIB (RFC 1612)
Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP MIB (RFC 2011)

IP Multicasting related MIBs
IPV6-MIB (RFC 2065)
IPV6-ICMP-MIB (RFC 2066)
IPV6-TCP-MIB (RFC 2052)
IPV6-UDP-MIB (RFC2054)
MAU MIB (RFC 3636)
MIB II (RFC 1213)
Port Access Entity MIB (IEEE 802.1X)
Port Access Entity Equipment MIB
Private MIB
Quality of Service MIB
RADIUS Accounting Server MIB (RFC 2621)
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 Community MIB (RFC 3584)
SNMP Framework MIB (RFC 3411)
SNMP-MPD MIB (RFC 3412)
SNMP Target MIB, SNMP Notification MIB (RFC 3413)
SNMP User-Based SM MIB (RFC 3414)
SNMP View Based ACM MIB (RFC 3415)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2012)
Trap (RFC 1215)
UDP MIB (RFC 2013)

B TROUBLESHOOTING

PROBLEMS ACCESSING THE MANAGEMENT INTERFACE

Table 47: 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 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 your local distributor.

USING SYSTEM LOGS

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Contact your distributor's service engineer.

For example:

```
>system log
>system log all
>snmp mode enable
>snmp trap mode enable
>snmp trap destination 192.168.1.23
⋮
```

GLOSSARY

ACL Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

BOOTP Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CoS Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DIFFSERV Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

DHCP Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP OPTION 82 A relay option for sending information about the requesting client (or an intermediate relay agent) in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information can be used by DHCP servers to assign fixed IP addresses, or set other services or policies for clients.

DNS Domain Name Service. A system used for translating host names for network nodes into IP addresses.

DSCP Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

EUI Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.

EAPOL Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

GARP Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

GMRP Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

GVRP GARP VLAN Registration Protocol. Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

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 802.1W An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)

IEEE 802.1X Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3AC Defines frame extensions for VLAN tagging.

IEEE 802.3X Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

IGMP Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

IGMP QUERY On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP SNOOPING Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IN-BAND MANAGEMENT Management of the network from a station attached directly to the network.

IP MULTICAST FILTERING A process whereby this switch can pass multicast traffic along to participating hosts.

IP PRECEDENCE The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

LACP Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

LAYER 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

LINK AGGREGATION *See Port Trunk.*

MD5 MD5 Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MULTICAST SWITCHING A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

MVR Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as such as television channels or video-on-demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard or private VLAN groups.

NTP Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

OUT-OF-BAND MANAGEMENT Management of the network from a station not attached to the network.

PORT AUTHENTICATION *See IEEE 802.1X*.

PORT MIRRORING A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

PORT TRUNK Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

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.

QOS Quality of Service. QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS Remote Authentication Dial-in User Service. RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RMON Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

RSTP Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

SMTP Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

SNMP Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

SNTP Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

SSH Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

STA Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

TACACS+ Terminal Access Controller Access Control System Plus. TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

TCP/IP Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

TELNET Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

TFTP Trivial File Transfer Protocol. A TCP/IP protocol commonly used for software downloads.

UDP User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XMODEM A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

INDEX

NUMERICS

802.1X, port authentication 76, 246

A

acceptable frame type 97, 278
Access Control List *See* ACL
ACL 110, 296
  binding to a port 111, 298
address table 92, 271
  aging time 93, 273

B

BPDU 72
  selecting protocol based on message format 244
broadcast storm, threshold 109, 294

C

CLI, showing commands 180
command line interface *See* CLI
community string 39, 123, 126, 311, 312, 314
configuration files
  restoring 173, 307
  saving 173, 306
configuration files, restoring defaults 174, 307
configuration settings, restoring 174, 307
configuration settings, saving 173, 306
configuration settings, saving or restoring 42, 173, 306
console port, required connections 33
CoS, queue mode 101, 290

D

default IPv4 gateway, configuration 52, 197
default IPv6 gateway, configuration 54, 201
default priority, ingress port 101, 286
default settings, system 30
DHCP 52, 196
  client 52, 196
  dynamic configuration 37
DHCP relay
  information option 135, 338
  information option policy 135, 339
DNS, server 52, 199
Domain Name Service *See* DNS
downloading software 341
  using HTTP 172, 341
  using TFTP 341
downoading software 172
dynamic addresses, displaying 93, 166, 274

E

edge port, STA 74, 75, 241, 243
event logging 137, 189

F

firmware
  displaying version 136
  upgrading 172, 341
  upgrading with HTTP 172, 341
  upgrading with TFTP 341

G

gateway, IPv4 default 52, 197
gateway, IPv6 default 54, 201

H

HTTP/HTTPS
  filtering IP addresses 56, 191
HTTPS 81, 329
  configuring 81, 329
HTTPS, secure server 81, 329

I

IEEE 802.1D 72, 238
IEEE 802.1X 76, 246
IGMP 84, 255
  fast leave, status 86, 259
  filter, parameters 88, 261
  filtering 88, 261
  groups, displaying 160, 263
  query 85, 258
  snooping 84, 255
  snooping & query, parameters 85
  snooping, configuring 85, 86, 255
  snooping, fast leave 86, 259
  throttling 87, 260
ingress filtering 96, 279
IP address, setting 51, 197

IPv4 address
DHCP 52, 196
dynamic configuration 37, 196
manual configuration 36, 197
setting 35, 51, 197
IPv6 address
dynamic configuration (global unicast) 38, 54, 200
dynamic configuration (link-local) 38
EUI format 54, 201
EUI-64 setting 54, 201
global unicast 54, 201
link-local 54
manual configuration (global unicast) 36, 54
manual configuration (link-local) 36, 54
setting 35, 53, 201

K

key
private 333
public 83, 333

L

LACP
configuration 67, 229
local parameters 68, 150, 233
partner parameters 150, 233
protocol message statistics 151, 233
protocol parameters 67, 229
leave proxy 85, 260
Link Aggregation Control Protocol *See* LACP
Link Layer Discovery Protocol *See* LLDP
link type, STA 75, 243
LLDP 89, 264
device statistics, displaying 163, 269
remote information, displaying 162, 268
TLV 89, 264
TLV, management address 91, 266
TLV, port description 91, 265
TLV, system capabilities 91, 266, 268
TLV, system description 91, 265
TLV, system name 91, 265
log-in, web interface 45
logon authentication 60, 205
encryption keys 62, 209, 210
RADIUS client 61, 207
RADIUS server 61, 207
settings 61, 205
TACACS+ client 60, 210
TACACS+ server 60, 210

M

main menu 46
management access, filtering IP addresses 56, 190
Management Information Bases (MIBs) 347
maximum frame size 59
mirror port
configuring 120, 304
multicast filtering 84, 255
multicast groups 160, 263
displaying 160, 263
multicast services
displaying 160, 263
leave proxy 85, 260
multicast storm, threshold 109, 293
multicast, filtering 88, 261
multicast, static router port 86, 262
multicast, throttling 87, 260

P

password 35
administrator setting 56, 60, 188
path cost 71, 74, 239
STA 71, 74, 239
port authentication 76, 246
port priority
configuring 101, 286
default ingress 101, 286
STA 74, 241
port security, configuring 76, 246
port, maximum frame size 59
port, statistics 140, 221
ports
autonegotiation 58, 217
broadcast storm threshold 109, 294
capabilities 58, 217
duplex mode 58, 217
flow control 58, 218
mirroring traffic 120, 304
multicast storm threshold 109, 293
speed 58, 217
unknown unicast storm threshold 109, 293
ports, configuring 58, 215
priority, default port ingress 101, 286
private key 333
private VLANs, configuring 98, 282
problems, troubleshooting 349
protocol migration 244
public key 83, 333
PVID, port native VLAN 278, 280, 281
PVLAN, configuring 98, 282

Q

QoS 100, 285
binding QCL to interface 101, 287
configuring 101, 285
queue mode 101, 290
traffic class weights 101, 291
Quality of Service *See* QoS
queue weights 101, 291

R

RADIUS
  logon authentication 61, 207
  settings 61, 207
rate limits, setting 107, 291
restarting the system 171, 186
RSTP 71, 235
  global settings, displaying 72, 236
  interface settings 73, 239–243
  interface settings, displaying 236
  settings, configuring 72, 235

S

secure shell 83, 332, 333
  configuration 83, 332
Simple Network Management Protocol *See* SNMP
SNMP 56, 57, 121, 308
  community string 123, 126, 311, 312, 314
  enabling traps 123, 312, 314, 315
  filtering IP addresses 56, 191
  trap manager 123, 314
SNMPv3
  engine identifier, local 123, 318, 320
  engine identifier, remote 128, 320
  groups 129, 130, 323
  user configuration 127, 128, 320
  views 130, 325
SNTP
  setting the system clock 52, 55, 200
  specifying servers 55, 200
software
  displaying version 136
  downloading 172, 341
Spanning Tree Protocol *See* STA
specifications, software 345
SSH 83, 333
  configuring 83, 332
  server, configuring 83, 332
STA 71, 236
  edge port 74, 75, 241, 243
  global settings, displaying 72, 236
  interface settings 73, 239–243
  link type 75, 243
  path cost 71, 74, 239
  port priority 74, 241
  protocol migration 244
  transmission hold count 72, 238
  transmission limit 72, 238
standards, IEEE 347
static addresses, setting 93, 272
statistics, port 140, 221
STP 72, 238
STP *Also see* STA
switch settings
  restoring 173, 174, 306, 307
  saving 173, 306
system clock
  setting the time zone 50, 189
  setting with SNTP 52, 55, 200
system information
  configuring 50
  displaying 136, 186
system logs 137, 189
  displaying 137, 189
system software
  downloading 172, 341
  downloading from server 172, 341

T

TACACS+
  logon authentication 60, 210
  settings 61, 210
Telnet/SSH, filtering IP addresses 56, 191
throttling, IGMP 87, 260
time zone, setting 50, 189
traffic class weights 101, 291
trap manager 40, 123, 314
troubleshooting 349
trunk
  configuration 65, 67, 229
  LACP 67, 229
  static 65, 224, 229
Type Length Value
  See LLDP TLV
  See also LLDP-MED TLV

U

unknown unicast storm, threshold 109, 293
upgrading software 172, 341
UPnP
  advertisements 133, 336
  configuration 132, 334
  enabling advertisements 133, 334

V

VLAN
  acceptable frame type 97, 278
  egress mode 97
  ingress filtering 96, 279
  interface configuration 96, 97, 277–280
VLANs 276
  adding static members 95, 280
  creating 95, 280
  description 94
  displaying basic information 281
  displaying port members 96, 281
  private 98, 282
  PVID 278, 280, 281
  QinQ 97, 279

W

web interface
- access requirements 44
- configuration buttons 45
- home page 45
- menu list 46
- panel display 46