

S3900 Series Switches Web Management User Manual

Models: S3900-48T4S/S3900-24F4S/S3900-24T4S

Contents

System Information.....	1
System Info.....	1
System Description.....	1
User Accounts.....	2
Switch Management.....	3
Jumbo Frame.....	3
Interface.....	3
Port.....	3
sFlow.....	6
Transceiver.....	8
Cable Test.....	10
Green Ethernet.....	11
Traffic Segment.....	12
Statistics.....	13
Statistics Info.....	13
History Management.....	16
Show History Statistics.....	17
Vlan.....	18
Static Vlan.....	18
GVRP.....	20
Protocol Vlan.....	21
IP Subnet Vlan.....	23
MAC-Based Vlan.....	24
Vlan Translation.....	25
VLAN Trunking.....	26
QinQ.....	27
Voice Vlan.....	32
L2PT.....	34
MAC Address.....	36
Dynamic MAC Learning.....	36
Static Mac Setting.....	38
Port Mirror.....	40
Local Port Mirror.....	40
RSPAN.....	41
Static Link Aggregation.....	43
Static Trunk.....	43
Static Trunk Member.....	44
Static Trunk Management.....	44
Load Balance.....	45
LACP.....	46
Configure Aggregator.....	46
Configure Aggregation Port.....	47
Show Aggregation Port Information.....	49
Dynamic Trunk.....	50
Show Dynamic Trunk Member.....	50
STP.....	51
STP-RSTP.....	53
MSTP.....	61
Loopback Detection.....	63
IGMP Snooping.....	64
General.....	65
Current Multicast.....	68
Static Multicast Router.....	69
Static Member.....	69
VLAN Information.....	70

Configure Interface.....	74
Forwarding Entry.....	74
Query Statistics.....	75
VLAN Statistics.....	76
Port Statistics.....	77
Trunk Stastics.....	78
IGMP Filtering and Throttling.....	79
Filter General.....	79
Filter Profile.....	80
Filter Range.....	81
Configure Filter Interface.....	81
MLD Snooping.....	82
General.....	83
Immediate Leave Status.....	84
Current Multicast Router.....	84
Static Multicast Router.....	85
Current Member.....	86
Static Member.....	86
Group Information.....	87
Statistics.....	88
MVR For IPv4.....	90
Configure Global.....	91
Configure Domain.....	92
Show Configure Profile.....	93
Add Configure Profile.....	94
Show Associate Profile.....	95
Add Associate Profile.....	96
Configure Interface.....	96
Show Static Group Member.....	98
Add Static Group Member.....	99
Show Member.....	99
Show Query Statistics.....	100
Show VLAN Statistics.....	101
Show Port Statistics.....	102
Show Trunk Statistics.....	103
MVR For IPv6.....	104
Configure Global.....	104
Configure Domain.....	106
Show Configure Profile.....	107
Add Configure Profile.....	108
Show Associate Profile.....	109
Add Associate Profile.....	109
Configure Interface.....	110
Show Static Group Member.....	111
Add Static Group Member.....	112
Show Member.....	113
Show Query Statistics.....	113
Show VLAN Statistics.....	115
Show Port Statistics.....	116
Show Trunk Statistics.....	117
LLDP.....	118
Configure Global.....	119
Interface General.....	120
CA-Type.....	122
Show Local Information.....	123
Show Remote Information.....	125
Show Statistics.....	129
ERPS.....	130

Configure Global.....	131
Domain.....	131
Domain Details.....	132
Domain Operation.....	136
Show Statistics.....	136
Loopback Detection.....	137
Configure Global.....	137
Configure Interface.....	138
UDLD.....	138
Configure Global.....	139
Configure Interface.....	140
Show Information.....	141
Congestion Control.....	142
Rate Limit.....	142
Storm Control.....	143
Auto Traffic Control.....	144
Stacking.....	148
Configure Master Button.....	148
Configure Stacking Button.....	149
Renumber.....	149
PPPoE.....	149
Configure Global.....	149
Configure Interface.....	150
Show Statistics.....	151
Route Management.....	152
IPv4 Interface Configuration.....	152
IPv6 Interface Configuration.....	153
Configure Global.....	153
Configure Interface.....	153
IPv6 Address.....	156
Show IPv6 Neighbor Cache.....	158
Show Statistics.....	159
Show MTU.....	164
ARP.....	164
Configure General.....	165
Static Arp.....	167
Show Information.....	167
Routing Table.....	168
ACL.....	171
ACL Management.....	171
ACL Rule Management.....	172
Configuring A Standard Ipv4 Acl.....	172
Configuring An Extended Ipv4 Acl.....	173
Configuring A Standard Ipv6 Acl.....	174
Configuring An Extended Ipv6 Acl.....	175
Configuring A Mac Acl.....	176
Configuring An Arp Acl.....	177
Show TCAM.....	178
Configure Interface.....	179
Show Hardware Counter.....	179
CoS.....	180
Default Priority.....	180
Queue.....	181
Trust Mode.....	182
DSCP to DSCP.....	183
CoS to DSCP.....	185
DSCP to CoS.....	186
IP Precedence to DSCP.....	188
IP Port to DSCP.....	189

PHB to Queue.....	190
QoS.....	192
Class.....	192
Class Rule.....	193
Policy.....	194
Policy Rule.....	199
Configure Interface.....	200
Security.....	200
AAA.....	200
System Authentication.....	201
Configure AAA Server.....	202
AAA Group.....	202
Configure Accounting Periodic.....	203
Accounting Method.....	203
Configure Accounting Service.....	203
Show Accounting Information.....	204
Authorization Method.....	204
Configure Authorization service.....	205
Show Authorization Information.....	205
Web Authentication.....	205
Configure Global.....	206
Configure Interface.....	206
802.1X.....	207
Configure Global.....	208
Configure Interface.....	208
Show Statistics.....	208
Network Access.....	209
Configure Global.....	209
Configure Interface.....	210
HTTPS.....	210
Configure Global.....	210
Copy Certificate.....	211
SSH.....	212
Configure Global.....	212
Show Host Key.....	213
Show User Key.....	213
Port Security.....	214
DAI.....	216
Configure General.....	216
Configure VLAN.....	217
Configure Interface.....	218
Show Statistics.....	219
Show Log.....	220
IP Filter.....	220
IP Filter Management.....	220
DoS Protection.....	221
IPv4 DHCP Snooping.....	223
Configure Global.....	223
Configure VLAN.....	224
Configure Interface.....	225
Show Information.....	225
IPv6 DHCP Snooping.....	226
Configure Global.....	226
VLAN Management.....	228
Configure Interface.....	228
Show Information.....	229
IPv4 Source Guard.....	229
General.....	230
ACL Table.....	231

MAC Table.....	231
Dynamic Binding.....	232
IPv6 Source Guard.....	233
Port Configuration.....	233
Static Binding.....	235
Dynamic Binding.....	236
Application Filter.....	236
CPU Guard.....	237
Device Management.....	238
SNMP.....	238
Configure Global.....	239
Community.....	240
Set Engine ID.....	240
Remote Engine.....	241
View.....	242
View Subtree.....	243
Group.....	243
SNMPv3 Local User.....	244
Change SNMPv3 Local User.....	245
SNMPv3 Remote User.....	245
Trap.....	246
Show Statistics.....	248
RMON.....	250
Global Management.....	250
Interface Management.....	252
Show Interface Details.....	254
Cluster.....	254
Configure Global.....	254
Cluster Member.....	255
Show Candidate.....	256
DNS.....	256
Configure Global.....	256
Domain Names.....	257
Name Servers.....	257
Static Host.....	258
Cache.....	259
DHCP.....	259
Client.....	259
Relay.....	260
Relay Option82.....	261
Dynamic Provision.....	263
OAM.....	264
Interface.....	264
Counters.....	266
Event Log.....	266
Remote Interface.....	267
Show Loopback Result.....	268
Loopback Test.....	268
CFM.....	270
Configure Global.....	272
Configure Interface.....	274
MD Management.....	275
MD Details.....	277
MA Management.....	278
MA Details.....	279
MEP Management.....	280
Remote MEP Management.....	281
Transmit Link Trace.....	282
Transmit Loopback.....	283

Transmit Delay Measure.....	284
Show Local MEP.....	285
Show Local MEP Details.....	286
Show Local MIP.....	287
Show Remote MEP.....	287
Show Remote MEP Details.....	288
Show Link Trace Cache.....	289
Show Fault Notification Generator.....	290
Show Continuity Check Error.....	290
Time Setting.....	291
Configure time.....	291
SNTP Server.....	292
NTP Server.....	292
NTP authentication Key.....	293
Configure Time Zone.....	294
Configure Summer Time.....	294
Event Log.....	295
Show System Logs.....	295
Configure Global.....	296
Remote.....	297
SMTP.....	298
File Management.....	298
Copying Files Via Ftp/Tftp Or Http.....	299
Saving The Running Configuration To A Local File.....	300
Setting The Startup File.....	300
Auto Upgrade.....	301
Ping.....	303
Trace Route.....	304
System Reboot.....	305

System Information

System Info

Use the System Information > System Info page to identify the system by displaying information

Information:

- ◆ **System Model** – The device type.
- ◆ **System Up Time** – Length of time the device has been up.
- ◆ **System Name** – Name assigned to the switch system.
- ◆ **Serial Number** – The serial number of the device.
- ◆ **Hardware Version**– The version of the device hardware.
- ◆ **Loader Version** – The version of the boot loader.
- ◆ **Firmware Version**– The version of the firmware running in the device.



System Description

System Information > System Description display the information of the firmware and device.



The screenshot displays the 'System Description' page for a switch model S3900-24T4S. The interface includes a navigation menu on the left and a main content area with the following sections:

- System Description Table:**

System Description	S3900-24T4S
System Object ID	1.3.6.1.4.1.51134.10.1.45.101
System Up Time	0 days, 1 hours, 2 minutes, and 9.3 seconds
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
- Buttons:** 'Apply' and 'Revert' buttons are located at the bottom right of the form.

User Accounts

System Information > User Accounts page to control management access to the switch based on manually configured user names and passwords.

COMMAND USAGE

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

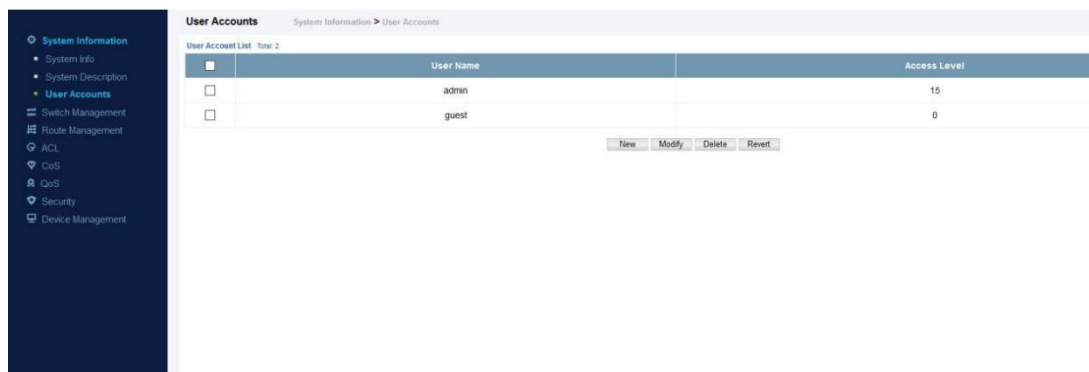
PARAMETERS

These parameters are displayed:

- ◆ **User Name** – The name of the user. (Maximum length: 32 characters; maximum number of users: 16)
- ◆ **Access Level** – Specifies the user level. (Options: 0 - Normal, 15 - Privileged) Normal privilege level provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Privileged level provides full access to all commands.
- ◆ **Password Type** – Specifies the following options:
 - **No Password** – No password is required for this user to log in.
 - **Plain Password** – Plain text unencrypted password.
 - **Encrypted Password** – Encrypted password.

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP or FTP server. There is no need for you to manually configure encrypted passwords.

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



<input type="checkbox"/>	User Name	Access Level
<input type="checkbox"/>	admin	15
<input type="checkbox"/>	guest	0

New Modify Delete Reset

Switch Management

Jumbo Frame

Use the Switch Management > Jumbo Frame page to configure support for layer 2 jumbo frames. The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 10240 bytes for Gigabit Ethernet. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

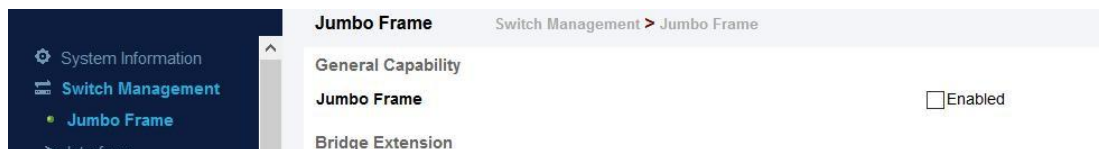
USAGE GUIDELINES

To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

PARAMETERS

The following parameters are displayed:

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

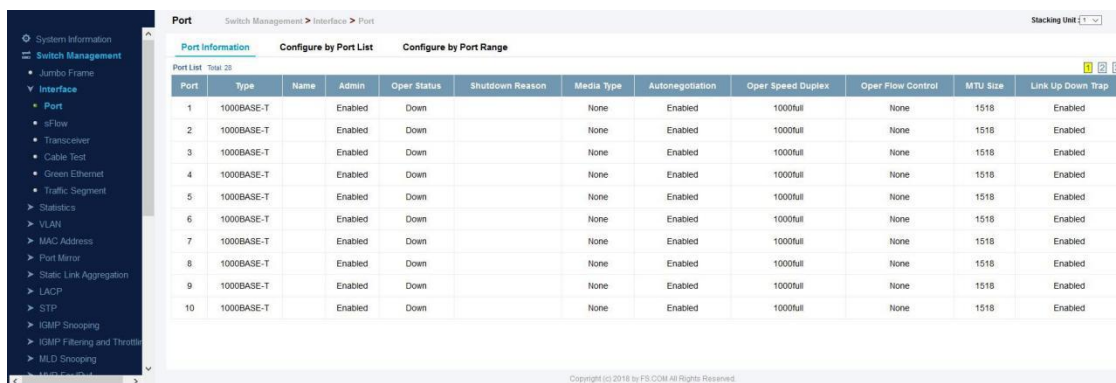


Interface

Port

Port Information

Use the Switch Management > Interface > Port > Port Information page to display the information of ports.



Port	Type	Name	Admin	Oper Status	Shutdown Reason	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control	MTU Size	Link Up Down Trap
1	1000BASE-T		Enabled	Down		None	Enabled	1000full	None	1518	Enabled
2	1000BASE-T		Enabled	Down		None	Enabled	1000full	None	1518	Enabled
3	1000BASE-T		Enabled	Down		None	Enabled	1000full	None	1518	Enabled
4	1000BASE-T		Enabled	Down		None	Enabled	1000full	None	1518	Enabled
5	1000BASE-T		Enabled	Down		None	Enabled	1000full	None	1518	Enabled
6	1000BASE-T		Enabled	Down		None	Enabled	1000full	None	1518	Enabled
7	1000BASE-T		Enabled	Down		None	Enabled	1000full	None	1518	Enabled
8	1000BASE-T		Enabled	Down		None	Enabled	1000full	None	1518	Enabled
9	1000BASE-T		Enabled	Down		None	Enabled	1000full	None	1518	Enabled
10	1000BASE-T		Enabled	Down		None	Enabled	1000full	None	1518	Enabled

Configuring by Port List

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

COMMAND USAGE

- ◆ Auto-negotiation must be disabled before you can configure or force a Gigabit RJ-45 interface to use the Speed/Duplex mode or Flow Control options.
- ◆ When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities. To set the speed, duplex mode, or flow control under auto-negotiation, the required operation modes must be specified in the capabilities list for an interface.
- ◆ The 1000BASE-T standard does not support forced mode. Autonegotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.
- ◆ The Speed/Duplex mode is fixed at 10Gfull on the 10GBASE SFP+ ports. When auto-negotiation is enabled, the only attributes which can be advertised include flow control and symmetric pause frames.

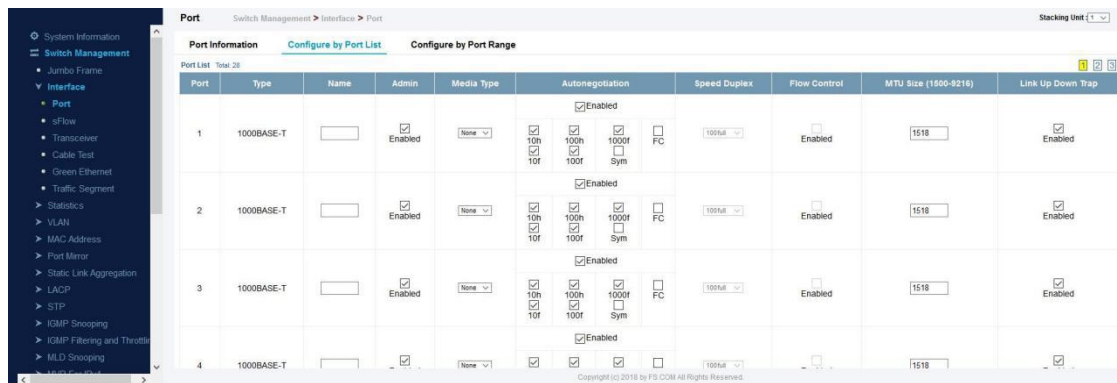
PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Type** – Indicates the port type. (1000BASE-T, 10GBASE SFP+)
- ◆ **Name** – Allows you to label an interface. (Range: 1-64 characters)
- ◆ **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons.
- ◆ **Media Type** – Not applicable for this switch.
- ◆ **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow

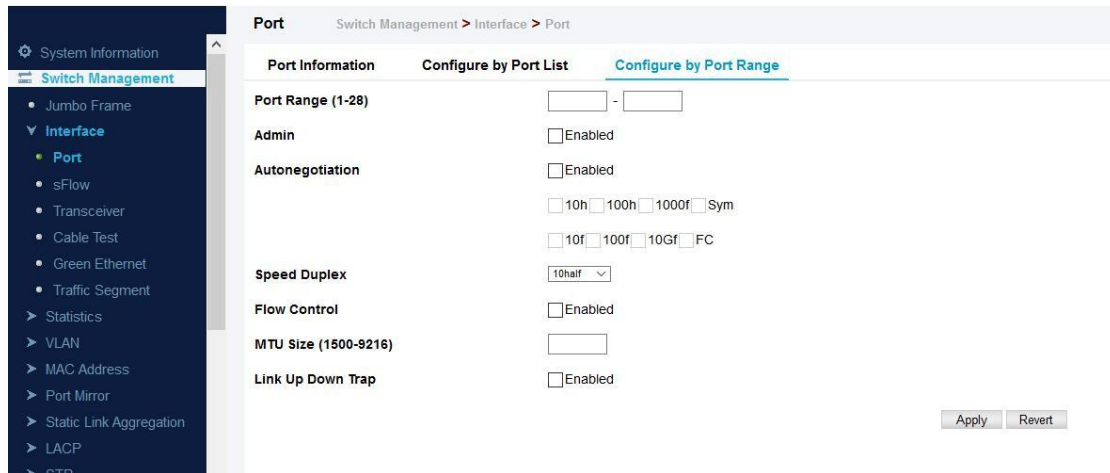
control. The following capabilities are supported.

- **10h** - Supports 10 Mbps half-duplex operation
 - **10f** - Supports 10 Mbps full-duplex operation
 - **100h** - Supports 100 Mbps half-duplex operation
 - **100f** - Supports 100 Mbps full-duplex operation
 - **1000f** (Gigabit ports only) - Supports 1000 Mbps full-duplex Operation
 - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames.
 - **FC** - Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2005 (formally IEEE 802.3x) for full duplex operation. Default: Autonegotiation enabled on Gigabit and 10 Gigabit ports;
- Advertised capabilities for
- 1000BASE-T – 10half, 10full, 100half, 100full, 1000full
 - 1000BASE-SX/LX/ZX (SFP+) – 1000full
 - 10GBASE-SR/LR/ER (SFP+) – 10Gfull
- ◆ **Speed/Duplex** – Allows you to manually set the port speed and duplex mode. (i.e., with auto-negotiation disabled)
 - ◆ **Flow Control** – Allows automatic or manual selection of flow control.



Configuring by Port Range

Use the Switch Management > Interface > Port > Configure by Port Range page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control. For more information on command usage and a description of the parameters.



sFlow

The flow sampling (sFlow) feature embedded on this switch, together with a remote sFlow Collector, can provide network administrators with an accurate, detailed and real-time overview of the types and levels of traffic present on their network. The sFlow Agent samples 1 out of n packets from all data traversing the switch, re-encapsulates the samples as sFlow datagrams and transmits them to the sFlow Collector. This sampling occurs at the internal hardware level where all traffic is seen, whereas traditional probes will only have a partial view of traffic as it is sampled at the monitored interface. Moreover, the processor and memory load imposed by the sFlow agent is minimal since local analysis does not take place. The wire-speed transmission characteristic of the switch is thus preserved even at high traffic levels.

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

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

Switch Management > Interface > sFlow page is used to create an sFlow receiver on the switch.

Parameters

These parameters are displayed:

- ◆ Receiver Owner Name 2 – The name of the receiver. (Range: 1-256 characters; Default: None)
- ◆ Receiver Timeout – The time that the sFlow process will continuously send samples to the

Collector before resetting all sFlow port parameters. (Range: 0-10000000 seconds, where 0 indicates no time out)

The sFlow parameters affected by this command include the sampling interval, the receiver's name, address and UDP port, the time out, maximum header size, and maximum datagram size.

- ◆ Receiver Destination 2 – IP address of the sFlow Collector.
- ipv4-address - IPv4 address of the sFlow collector. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods.
- ipv6-address - IPv6 address of the sFlow collector. A full IPv6 address including the network prefix and host address bits. An IPv6 address consists of 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ Receiver Socket Port 2 – The UDP port on which the sFlow Collector is listening for sFlow streams. (Range: 1-65534)
- ◆ Maximum Datagram Size – Maximum size of the sFlow datagram payload. (Range: 200-1500 bytes)
- ◆ Datagram Version – Sends either v4 or v5 sFlow datagrams to the receiver.

Receiver Owner Name

Receiver Timeout (30 - 10000000) sec

Receiver Destination

Receiver Socket Port (1 - 65535)

Maximum Datagram Size (200 - 1500) bytes

Datagram Version v4 v5

sFlow
Switch Management > Interface > sFlow
Stacking Unit: 1

sFlow Receiver Management
sFlow Management

Receiver List Total: 1

	Owner Name	Timeout	Destination	Socket Port	Maximum Datagram Size	Datagram Version
☐	test	998	1.1.1.12	22500	512	5

Switch Management > Interface > sFlow Management page is used to enable an sFlow polling data source that polls periodically based on a specified time interval, or an sFlow data source instance that takes samples periodically based on the number of packets processed.

sFlow Switch Management > Interface > sFlow Stacking Unit: 1

sFlow Receiver Management **sFlow Management**

Receiver Owner Name: test

Type: Sampling Polling

Sampling List Total: 1

	Data Source (Unit/Port)	Instance ID	Rate	Maximum Header Size (bytes)
<input type="checkbox"/>	1/3	1	256	200

Press 'new' button to set the parameters:

- ◆ Receiver Owner Name – The name of the receiver. (Range: 1-256 characters; Default: None)
- ◆ Type – Specifies the polling type as an sFlow polling data source for a specified interface that polls periodically based on a specified time interval, or an sFlow data source instance for a specific interface that takes samples periodically based on the number of packets processed.
- ◆ Data Source – The source from which the samples will be taken and sent to a collector.
- ◆ Instance ID – An instance ID used to identify the sampling source. (Range: 1)
- ◆ Sampling Rate – The number of packets out of which one sample will be taken. (Range: 256-16777215 packets; Default: Disabled)
- ◆ Maximum Header Size – Maximum size of the sFlow datagram header. (Range: 64-256 bytes)

Receiver Owner Name test

Type Sampling Polling

Data Source Unit: 1 Port: 1

Instance ID (1-1)

Sampling Rate (256-16777215)

Maximum Header Size (64-256) bytes

Transceiver

Switch Management > Interface > Transceiver page is used to configure thresholds for alarm

and warning messages for optical transceivers which support Digital Diagnostic Monitoring (DDM). This page also displays identifying information for supported transceiver types, and operational parameters for transceivers which support DDM.

Parameters

These parameters are displayed:

- ◆ **Port** – Port number. (ECS4620-28F/28F-DC: 1-28, Other models: SFP/SFP+ ports 25-28 / 49-52)
- ◆ **General** – Information on connector type and vendor-related parameters.
- ◆ **DDM Information** – Information on temperature, supply voltage, laser bias current, laser power, and received optical power. The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) provides information on transceiver parameters.
- ◆ **Trap** – Sends a trap when any of the transceiver's operation values falls outside of specified thresholds. (Default: Disabled)
- ◆ **Auto Mode** – Uses default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent. (Default: Enabled)
- ◆ **DDM Thresholds** – Information on alarm and warning thresholds. The switch can be configured to send a trap when the measured parameter falls outside of the specified thresholds.

The following alarm and warning parameters are supported:

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

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

The threshold value for Rx and Tx power is calculated as the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW). Threshold values for alarm and warning messages can be configured as described below.

- A high-threshold alarm or warning message is sent if the current value is greater than or equal to the threshold, and the last sample value was less than the threshold. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the high threshold and reaches the low threshold.
- A low-threshold alarm or warning message is sent if the current value is less than or equal to the threshold, and the last sample value was greater than the threshold. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the low threshold and reaches the high threshold.
- Threshold events are triggered as described above to avoid a hysteresis effect which would continuously trigger event messages if the power level were to fluctuate just above

and below either the high threshold or the low threshold.

■ Trap messages configured by this command are sent to any management station configured as an SNMP trap manager using the Administration > SNMP (Configure Trap) page.

Transceiver Switch Management > Interface > Transceiver Stacking Unit: 1

Port: 25

No SFP Insert.

DDM Thresholds

Trap

Auto Mode

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

Click this button to restore default DDM thresholds values.

Cable Test

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

COMMAND USAGE

◆ Cable diagnostics are performed using Digital Signal Processing (DSP) test methods. DSP analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse.

◆ Cable diagnostics can only be performed on twisted-pair media.

◆ This cable test is only accurate for cables 7 - 140 meters long.

◆ The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length to a fault.

◆ Potential conditions which may be listed by the diagnostics include:

■ OK: Correctly terminated pair

■ Open: Open pair, no link partner

■ Short: Shorted pair

■ Not Supported: This message is displayed for any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps, or for any 10G Ethernet ports.

■ Impedance mismatch: Terminating impedance is not in the reference range.

◆ Ports are linked down while running cable diagnostics.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Switch port identifier.
- ◆ **Type** – Displays media type. (GE – Gigabit Ethernet, Other – SFP+)
- ◆ **Link Status** – Shows if the port link is up or down.
- ◆ **Test Result** – The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found. To ensure more accurate measurement of the length to a fault, first disable power-saving mode on the link partner before running cable diagnostics. For link-down ports, the reported distance to a fault is accurate to within +/- 2 meters. For link-up ports, the accuracy is +/- 10 meters.
- ◆ **Last Updated** – Shows the last time this port was tested.

Cable Test							Stacking Unit :
Switch Management > Interface > Cable Test							1
Cable Test Port List Total: 28							1 2 3
Port	Test Result (Cable/Fault Distance in Meters)				Accuracy(Meters)	Last Updated	Action
	Pair A	Pair B	Pair C	Pair D			
1	OK (0)	OK (0)	OK (0)	OK (0)	0		Test
2	OK (0)	OK (0)	OK (0)	OK (0)	0		Test

Green Ethernet

Switch Management > Interface > Green Ethernet page is used to enable power savings mode on the selected port.

COMMAND USAGE

◆ IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can reduce power used for cable lengths of 60 meters or less, with more significant reduction for cables of 20 meters or less, and continue to ensure signal integrity.

◆ The power-saving methods provided by this switch include:

■ Power saving when there is no link partner:

Under normal operation, the switch continuously auto-negotiates to find a link partner, keeping the MAC interface powered up even if no link connection exists. When using power-savings mode, the switch checks for energy on the circuit to determine if there is a link partner. If none is detected, the switch automatically turns off the transmitter, and most of the receive circuitry (enters Sleep Mode). In this mode, the low-power energy-detection circuit continuously checks for energy on the cable. If none is detected, the MAC interface is also powered down to save additional energy. If energy is detected, the switch immediately turns on both the transmitter and receiver functions, and powers up the MAC interface.

■ Power saving when there is a link partner:

Traditional Ethernet connections typically operate with enough power to support at least 100 meters of cable even though average network cable length is shorter. When cable length is shorter, power consumption can be reduced since signal attenuation is proportional to cable length. When power-savings mode is enabled, the switch analyzes

cable length to determine whether or not it can reduce the signal amplitude used on a particular link.

PARAMETERS

These parameters are displayed:

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

Green Ethernet
Switch Management > Interface > Green Ethernet
Stacking Unit: 1

Port Green Ethernet List Total: 28
1 2 3

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

Traffic Segment

Switch Management > Interface > Traffic Segment page is used to enable traffic segmentation.

PARAMETERS

These parameters are displayed:

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

Traffic Segment
Switch Management > Interface > Traffic Segment

[Configure Global Status](#)
[Show Session](#)

Status Enabled

Uplink-to-Uplink Mode Blocking

Statistics

Statistics Info

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

PARAMETERS

These parameters are displayed:

Parameter	Description
<i>Interface Statistics</i>	
Received Octets	The total number of octets received on the interface, including framing characters.
Transmitted Octets	The total number of octets transmitted out of the interface, including framing characters.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmitted Errors	The number of outbound packets that could not be transmitted because of errors.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Transmitted Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Transmitted Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Transmitted	The total number of packets that higher-level protocols requested be

Multicast Packets	transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Transmitted Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
<i>Etherlike Statistics</i>	
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Alignment Errors	The number of alignment errors (missynchronized data packets).
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
<i>RMON Statistics</i>	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.

Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Octets	Total number of octets of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Packets	The total number of packets (bad, broadcast and multicast) received.
Broadcast Packets	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Packets	The total number of good packets received that were directed to this multicast address.
Undersize Packets	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Packets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
64 Bytes Packets	The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Input Octets in kbits per second	Number of octets entering this interface in kbits/second.
Input Packets per second	Number of packets entering this interface per second.
Input Utilization	The input utilization rate for this interface.
Output Octets in kbits per second	Number of octets leaving this interface in kbits/second.
Output Packets per second	Number of packets leaving this interface per second.
Output Utilization	The output utilization rate for this interface.

Statistics Info
Switch Management > Statistics > Statistics Info
Stacking Unit : 1

Port
Trunk

Mode Interface Etherlike RMON Utilization

Port 1

Auto-refresh

Interface Statistics

Received Octets	0	Transmitted Octets	0
Received Errors	0	Transmitted Errors	0
Received Unicast Packets	0	Transmitted Unicast Packets	0
Received Discarded Packets	0	Transmitted Discarded Packets	0
Received Multicast Packets	0	Transmitted Multicast Packets	0
Received Broadcast Packets	0	Transmitted Broadcast Packets	0
Received Unknown Packets	0		

Clear
Refresh

History Management

Switch Management > Statistics > History Management page is used to display statistical history for the specified interfaces.

Command Usage

- ◆ For a description of the statistics displayed on these pages, see “Showing Port or Trunk Statistics”

- ◆ To configure statistical history sampling, use the “Displaying Statistical History”

Parameters

These parameters are displayed:

Add

- ◆ Port – Port number. (Range: 1-28/52)
- ◆ History Name – Name of sample interval. (Range: 1-32 characters)
- ◆ Interval - The interval for sampling statistics. (Range: 1-86400 minutes)
- ◆ Requested Buckets - The number of samples to take. (Range: 1-96)

Show

- ◆ Port – Port number. (Range: 1-26/28/52)
- ◆ History Name – Name of sample interval. (Default settings: 15min, 1day)
- ◆ Interval - The interval for sampling statistics.
- ◆ Requested Buckets - The number of samples to take.

Show Details

- ◆ Mode
- Status – Shows the sample parameters.
- Current Entry – Shows current statistics for the specified port and named sample.
- Input Previous Entries – Shows statistical history for ingress traffic.
- Output Previous Entries – Shows statistical history for egress traffic.
- ◆ Port – Port number. (Range: 1-26/28/52)
- ◆ Name – Name of sample interval.

Port 1 ▾

History Name

Interval (1-86400) seconds

Requested Buckets (1-96)

History Management Switch Management > Statistics > History Management Stacking Unit: 1 ▾

Port 1 ▾

History Name List Total: 2

<input type="checkbox"/>	History Name	Interval (seconds)	Requested Buckets
<input type="checkbox"/>	15min	900	96
<input type="checkbox"/>	1day	86400	7

Show History Statistics

Show History Statistics Switch Management > Statistics > Show History Statistics Stacking Unit: 1 ▾

Port 1 ▾

Mode Status Current Entry Input Previous Entries Output Previous Entries

Name 15min ▾

History Status

Name 15min

Interval 900 second(s)

Requested Buckets 96

Granted Buckets 27

Status Active

Show History Statistics Switch Management > Statistics > Show History Statistics Stacki

Port **Trunk**

Mode Status Current Entry Input Previous Entries Output Previous Entries

Port 1

Name 15min

Current Entry

Start Time 00d 06:45:00

% 0.00 % 0.00

Received Octets	0	Transmitted Octets	0
Received Errors	0	Transmitted Errors	0
Received Unicast Packets	0	Transmitted Unicast Packets	0
Received Discarded Packets	0	Transmitted Discarded Packets	0
Received Multicast Packets	0	Transmitted Multicast Packets	0
Received Broadcast Packets	0	Transmitted Broadcast Packets	0
Received Unknown Packets	0		

Show History Statistics Switch Management > Statistics > Show History Statistics Stacking Unit :

Port **Trunk**

Mode Status Current Entry Input Previous Entries Output Previous Entries

Port 1

Name 15min

Input Previous Entry List Total: 27 1 2 3

Start Time	%	Octets	Unicast	Multicast	Broadcast	Discarded	Errors	Unknown Proto
00d 00:00:00	0.00	0	0	0	0	0	0	0
00d 00:15:00	0.00	0	0	0	0	0	0	0
00d 00:30:00	0.00	0	0	0	0	0	0	0
00d 00:45:00	0.00	0	0	0	0	0	0	0
00d 01:00:00	0.00	0	0	0	0	0	0	0
00d 01:15:00	0.00	0	0	0	0	0	0	0
00d 01:30:00	0.00	0	0	0	0	0	0	0
00d 01:45:00	0.00	0	0	0	0	0	0	0
00d 02:00:00	0.00	0	0	0	0	0	0	0

Vlan

Static Vlan

Switch Management > VLAN > Static Vlan > Vlan Management page is used to add ,modify or delete static VLAN groups, set administrative status, or specify Remote VLAN type.

To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

◆ **VLAN ID** – ID of VLAN or range of VLANs (1-4093). Up to 4093 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

◆ **VLAN Name** – Name of the VLAN (1 to 32 characters).

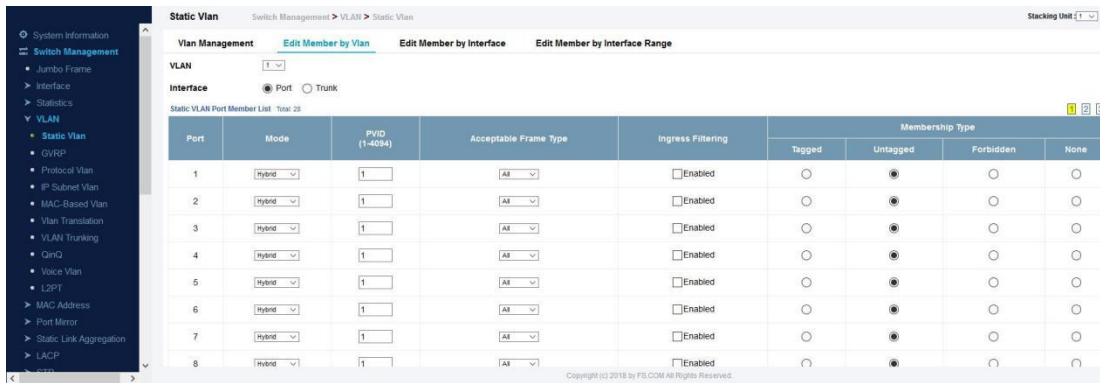
◆ **Status** – Enables or disables the specified VLAN.

◆ **Remote VLAN** – Reserves this VLAN for RSPAN.

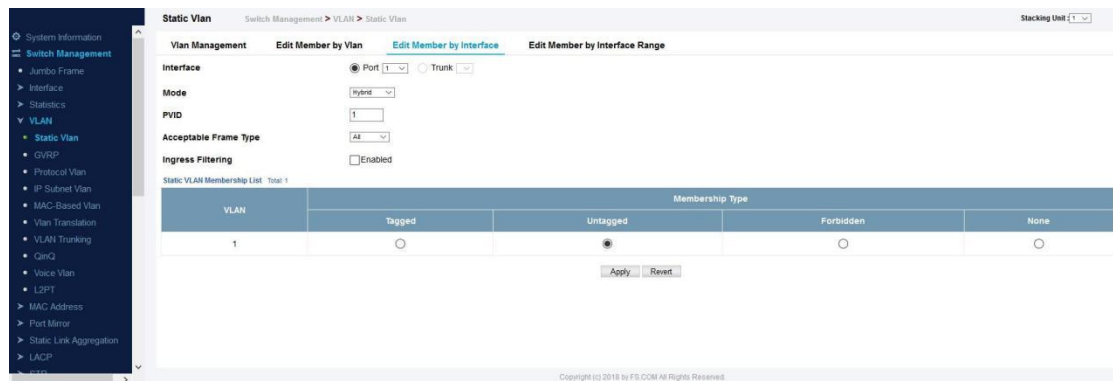
◆ **L3 Interface** – Sets the interface to support Layer 3 configuration, and reserves memory space required to maintain additional information about this interface type. This parameter must be enabled before you can assign an IP address to a VLAN



Switch Management > VLAN > Static VLAN > Edit member by vlan page is used to add/delete multiple port members to/from a special vln.

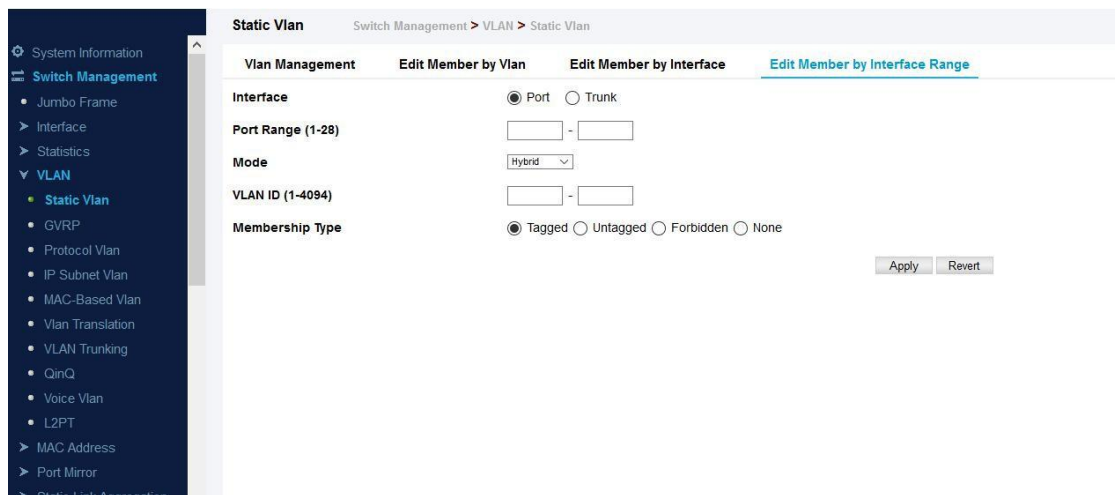


Switch Management > VLAN > Static VLAN > Edit member by interface page is used to add/delete a interface member to/from multiple vln



Switch Management > VLAN > Static VLAN > Edit member by interface range page is used to

add/delete multiple interface member to/from multiple vlan



The screenshot shows the 'Static VLAN' configuration page. The breadcrumb trail is 'Switch Management > VLAN > Static VLAN'. The page has four tabs: 'Vlan Management', 'Edit Member by Vlan', 'Edit Member by Interface', and 'Edit Member by Interface Range'. The 'Edit Member by Interface Range' tab is active. The configuration fields are as follows:

- Interface:** Radio buttons for 'Port' (selected) and 'Trunk'.
- Port Range (1-28):** Two input boxes separated by a hyphen.
- Mode:** A dropdown menu showing 'Hybrid'.
- VLAN ID (1-4094):** Two input boxes separated by a hyphen.
- Membership Type:** Radio buttons for 'Tagged' (selected), 'Untagged', 'Forbidden', and 'None'.

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

GVRP

Switch Management > VLAN > GVRP page is used to enable GVRP globally on the switch, or to enable GVRP and adjust the protocol timers per interface.

PARAMETERS

These parameters are displayed:

Configure General

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

Configure Interface

◆ **Interface** – Displays a list of ports or trunks.

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

◆ **Trunk** – Trunk Identifier. (Range: 1-12)

◆ **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect (using the Configure General page). When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled) GVRP cannot be enabled for ports set to Access mode

◆ **GVRP Timers** – Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer

■ **Join** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)

■ **Leave** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)

■ **LeaveAll** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)

Show Dynamic VLAN – Show VLAN

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

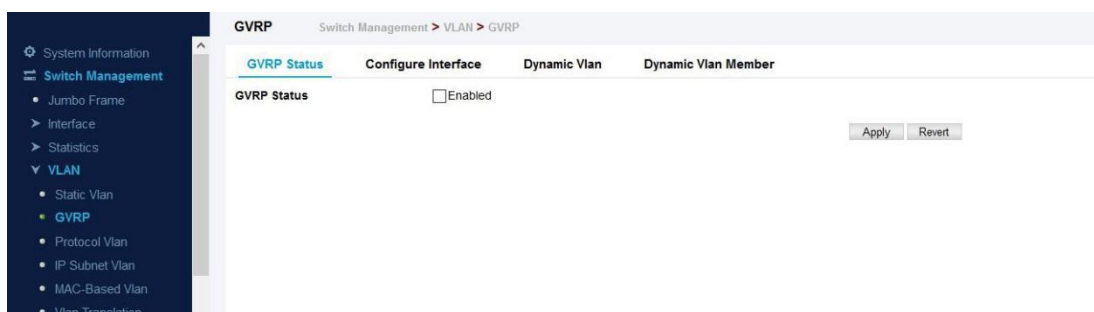
VLAN Name – Name of a VLAN this switch has joined through GVRP.

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

Show Dynamic VLAN – Show VLAN Member

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

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



Protocol Vlan

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

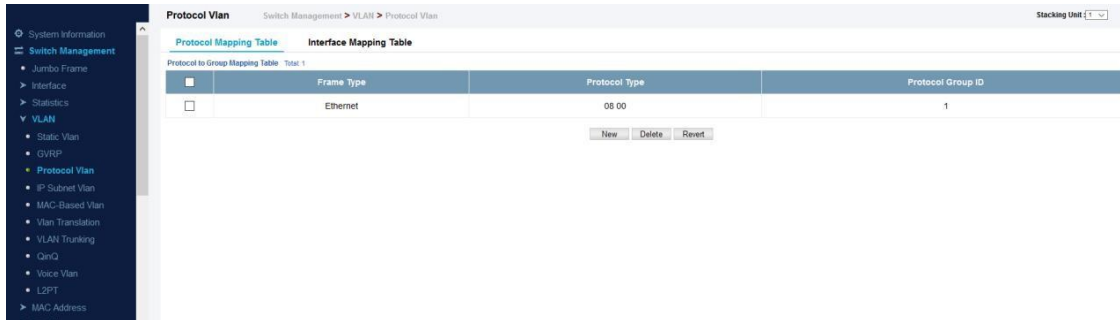
COMMAND USAGE

◆ To configure protocol-based VLANs, follow these steps:

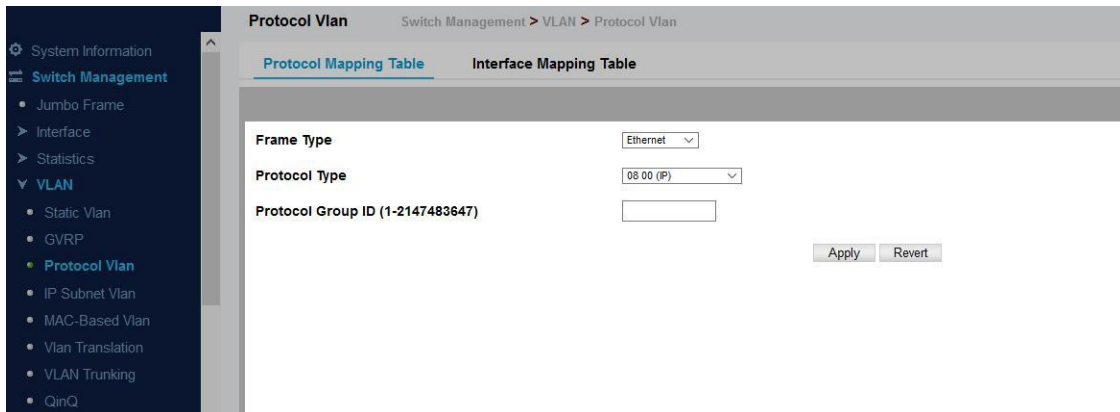
1. First configure VLAN groups for the protocols you want to use. Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Configure Protocol (Add) page.
3. Then map the protocol for each interface to the appropriate VLAN using the Configure Interface (Add) page.

◆ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

Switch Management > VLAN > Protocol Vlan page is used to create and delete a protocol vlan entry.

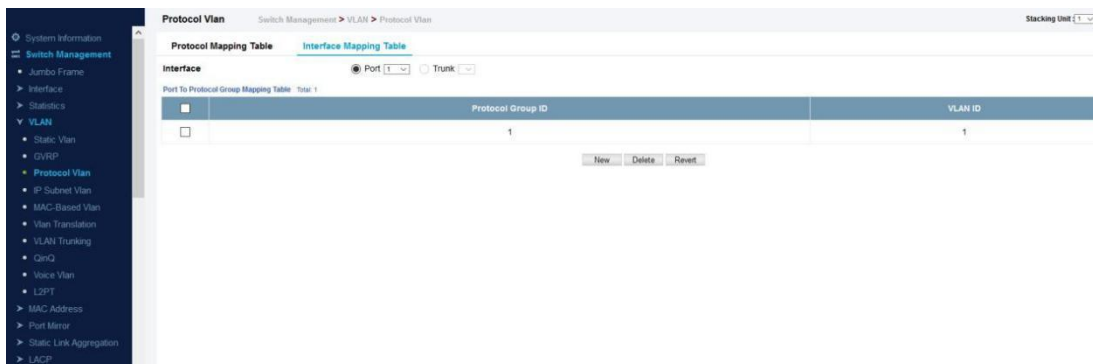


Press New button to create a protocol vlan entry:



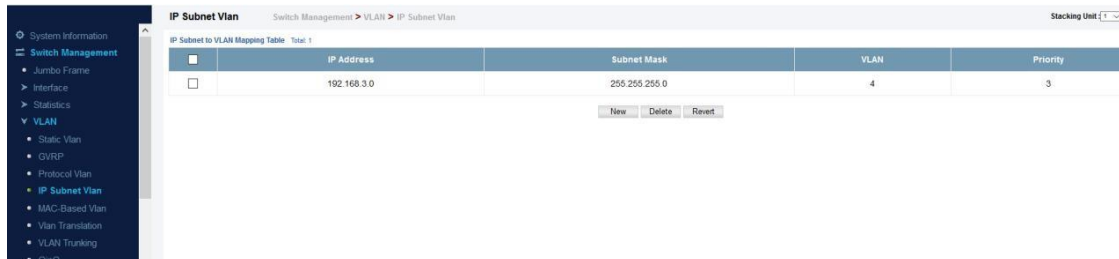
- ◆ **Frame Type** – Choose either Ethernet, RFC 1042, or LLC Other as the frame type used by this protocol.
- ◆ **Protocol Type** – Specifies the protocol type to match. The available options are IP, ARP, RARP and IPv6. If LLC Other is chosen for the Frame Type, the only available Protocol Type is IPX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

Switch Management > VLAN > Interface Mapping Table page is used to add/delete a interface member to protocol vlan group.



IP Subnet Vlan

Switch Management > VLAN > IP Subnet Vlan page is used to configure IP subnet-based VLANs. When using port-based classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

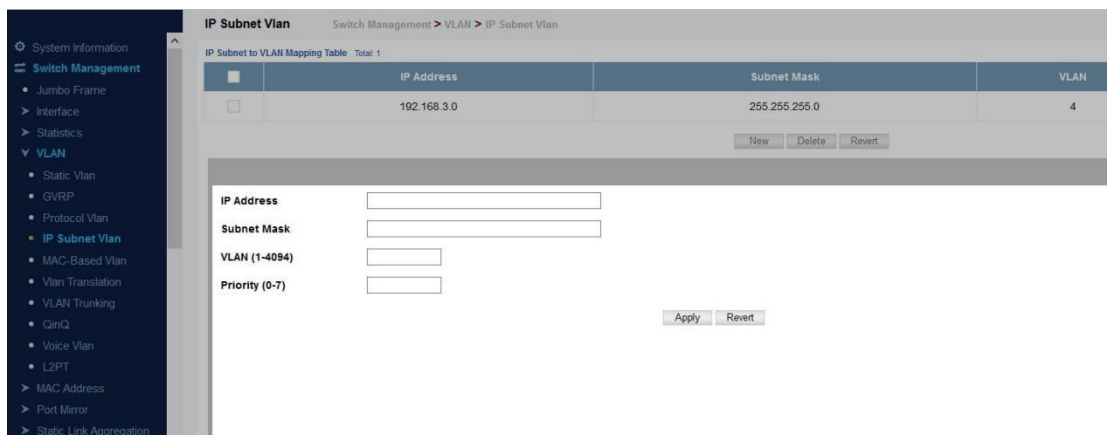


When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

COMMAND USAGE

- ◆ Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a mask. The specified VLAN need not be an existing VLAN.
- ◆ When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.
- ◆ The IP subnet cannot be a broadcast or multicast IP address.
- ◆ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

Press New button to create a IP subnet vlan entry.



- ◆ **IP Address** – The IP address for a subnet. Valid IP addresses consist of four decimal

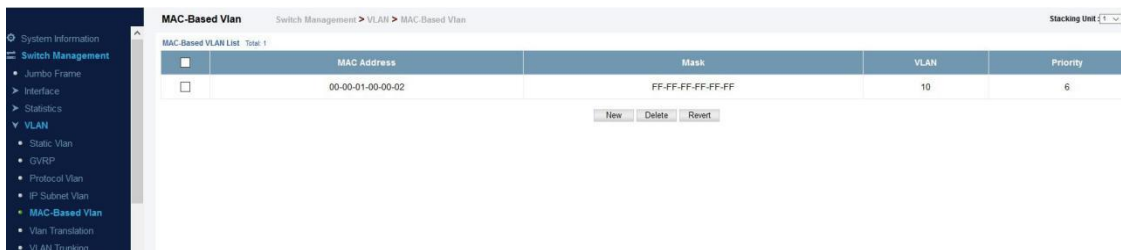
numbers, 0 to 255, separated by periods.

- ◆ **Subnet Mask** – This mask identifies the host address bits of the IP subnet.
- ◆ **VLAN** – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4093)
- ◆ **Priority** – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority; Default: 0)

To delete a IP subnet vlan entry, select the entry and press delete button.

MAC-Based Vlan

Switch Management > VLAN > Mac-Based Vlan page is used to configure VLAN based on MAC addresses.

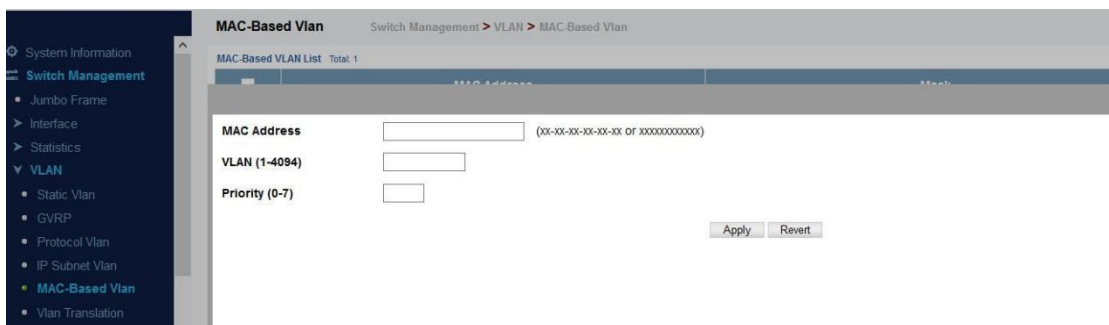


The MAC-based VLAN feature assigns VLAN IDs to ingress untagged frames according to source MAC addresses. When MAC-based VLAN classification is enabled, untagged frames received by a port are assigned to the VLAN which is mapped to the frame's source MAC address. When no MAC address is matched, untagged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

COMMAND USAGE

- ◆ The MAC-to-VLAN mapping applies to all ports on the switch.
- ◆ Source MAC addresses can be mapped to only one VLAN ID.
- ◆ Configured MAC addresses cannot be broadcast or multicast addresses.
- ◆ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

To create a Mac based vlan, press New button:



- ◆ **MAC Address** – A source MAC address which is to be mapped to a specific VLAN. The MAC address must be specified in the format xx-xxxx-xx-xx-xx.
- ◆ **VLAN** – VLAN to which ingress traffic matching the specified source MAC address is

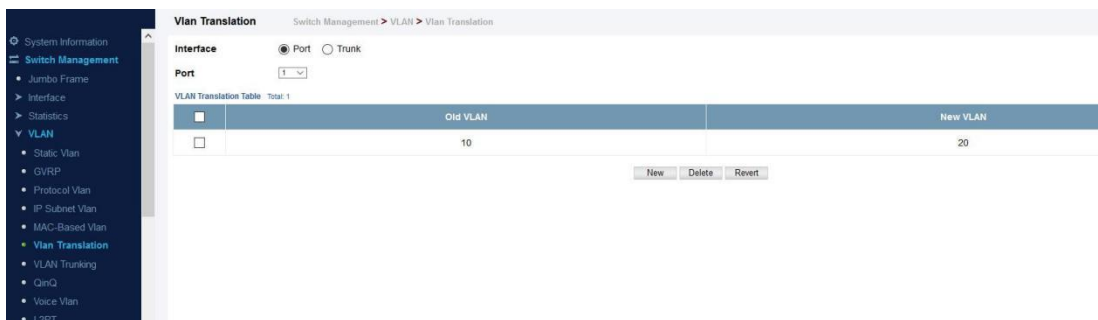
forwarded. (Range: 1-4093)

◆ **Priority** – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority; Default: 0)

To delete a Mac based vlan entry, select the entry and press delete button.

Vlan Translation

Switch Management > VLAN > Vlan Translation page is used to to map VLAN IDs between the customer and service provider for networks that do not support IEEE 802.1Q tunneling.



COMMAND USAGE

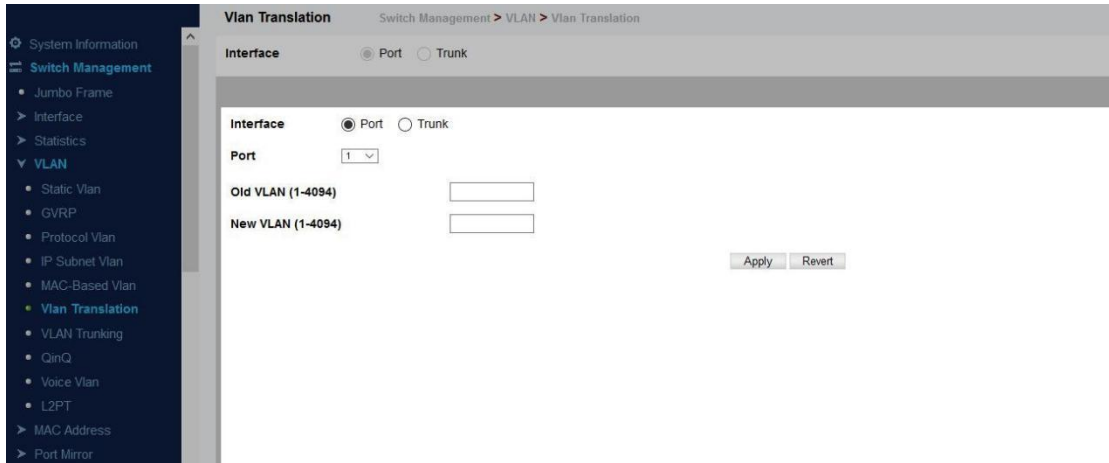
◆ QinQ tunneling uses double tagging to preserve the customer's VLAN tags on traffic crossing the service provider's network. However, if any switch in the path crossing the service provider's network does not support this feature, then the switches directly connected to that device can be configured to swap the customer's VLAN ID with the service provider's VLAN ID for upstream traffic, or the service provider's VLAN ID with the customer's VLAN ID for downstream traffic. For example, assume that the upstream switch does not support QinQ tunneling. Select Port 1, and set the Old VLAN to 10 and the New VLAN to 100 to map VLAN 10 to VLAN 100 for upstream traffic entering port 1, and VLAN 100 to VLAN 10 for downstream traffic leaving port 1 as shown below.



◆ The maximum number of VLAN translation entries is 8 per port, and up to 96 for the system. However, note that configuring a large number of entries may degrade the performance of other processes that also use the TCAM, such as IP Source Guard filter rules, Quality of Service (QoS) processes, QinQ, MAC-based VLANs, VLAN translation, or traps.

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

Press New button to create a vlan translation.



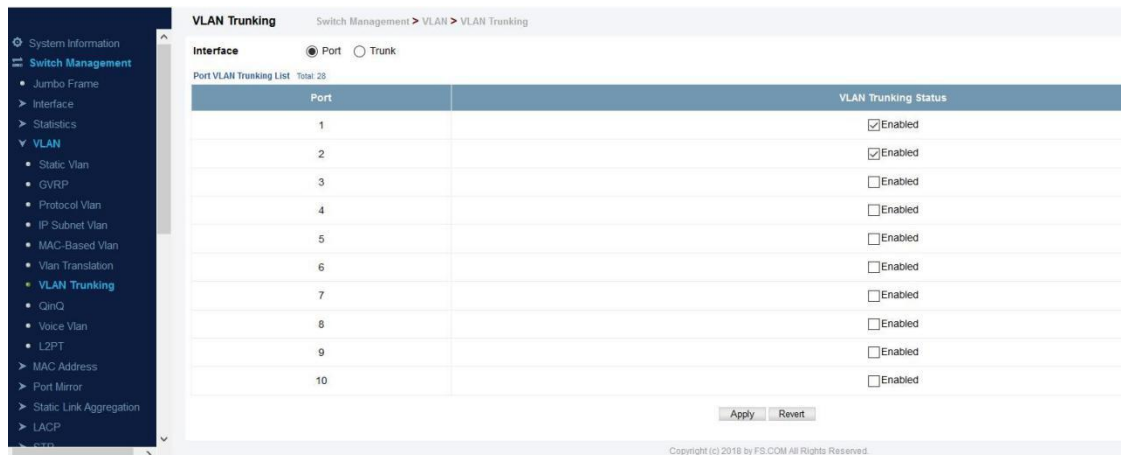
These parameters are displayed:

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

To delete a entry, select the entry and press delete button.

VLAN Trunking

Switch Management > VLAN > Vlan Trunking page is used to allow unknown VLAN groups to pass through the specified interface.



Command Usage

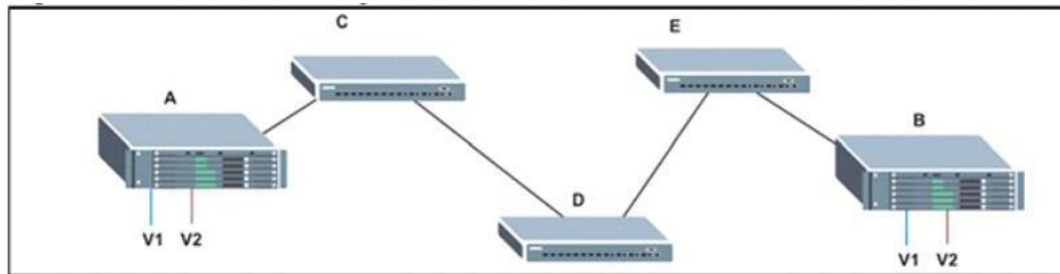
- ◆ Use this feature to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

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

Figure 67: Configuring VLAN Trunking

Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN

group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.



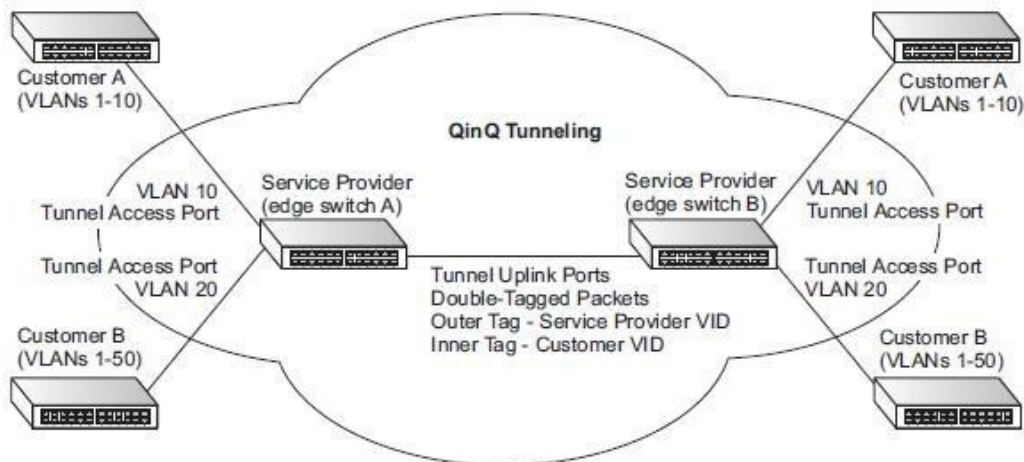
- ◆ VLAN trunking is mutually exclusive with the “access” switchport mode. If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.
- ◆ To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either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

QinQ

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

A service provider’s customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096. QinQ tunneling uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider’s network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer’s original tagged packets, and adding SPVLAN tags to each frame (also called double tagging). A port configured to support QinQ tunneling must be set to tunnel port mode. The Service Provider VLAN (SPVLAN) ID for the specific customer must be assigned to the QinQ tunnel access port on the edge switch where the customer traffic enters the service provider’s network. Each customer requires a separate SPVLAN, but this VLAN supports all of the customer’s internal

VLANs. The QinQ tunnel uplink port that passes traffic from the edge switch into the service provider's metro network must also be added to this SPVLAN. The uplink port can be added to multiple SPVLANs to carry inbound traffic for different customers onto the service provider's network. When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider's network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same SPVLAN tag is again added to the packet. When a packet enters the trunk port on the service provider's egress switch, the outer tag is again stripped for packet processing. However, the SPVLAN tag is not added when it is sent out the tunnel access port on the edge switch into the customer's network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer's network.



Layer 2 Flow for Packets Coming into a Tunnel Access Port

A QinQ tunnel port may receive either tagged or untagged packets. No matter how many tags the incoming packet has, it is treated as tagged packet. The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ tunnel port are processed in the following manner:

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

Layer 2 Flow for Packets Coming into a Tunnel Uplink Port

An uplink port receives one of the following packets:

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

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

1. If incoming packets are untagged, the PVID VLAN native tag is added.
2. If the ether-type of an incoming packet (single or double tagged) is not equal to the TPID of the uplink port, the VLAN tag is determined to be a Customer VLAN (CVLAN) tag. The uplink port's PVID VLAN native tag is added to the packet. This outer tag is used for learning and switching packets within the service provider's network. The TPID must be configured on a per port basis, and the verification cannot be disabled.
3. If the ether-type of an incoming packet (single or double tagged) is equal to the TPID of the uplink port, no new VLAN tag is added. If the uplink port is not the member of the outer VLAN of the incoming packets, the packet will be dropped when ingress filtering is enabled. If ingress filtering is not enabled, the packet will still be forwarded. If the VLAN is not listed in the VLAN table, the packet will be dropped.
4. After successful source and destination lookups, the packet is double tagged. The switch uses the TPID of 0x8100 to indicate that an incoming packet is double-tagged. If the outer tag of an incoming double-tagged packet is equal to the port TPID and the inner tag is 0x8100, it is treated as a double-tagged packet. If a single-tagged packet has 0x8100 as its TPID, and port TPID is not 0x8100, a new VLAN tag is added and it is also treated as double-tagged packet.
5. If the destination address lookup fails, the packet is sent to all member ports of the outer tag's VLAN.
6. After packet classification, the packet is written to memory for processing as a single-tagged or double-tagged packet.
7. The switch sends the packet to the proper egress port.
8. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packet will have two tags.

Configuration Limitations for QinQ

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

are not supported on tunnel ports.

■ Spanning tree bridge protocol data unit (BPDU) filtering is automatically disabled on a tunnel port.

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

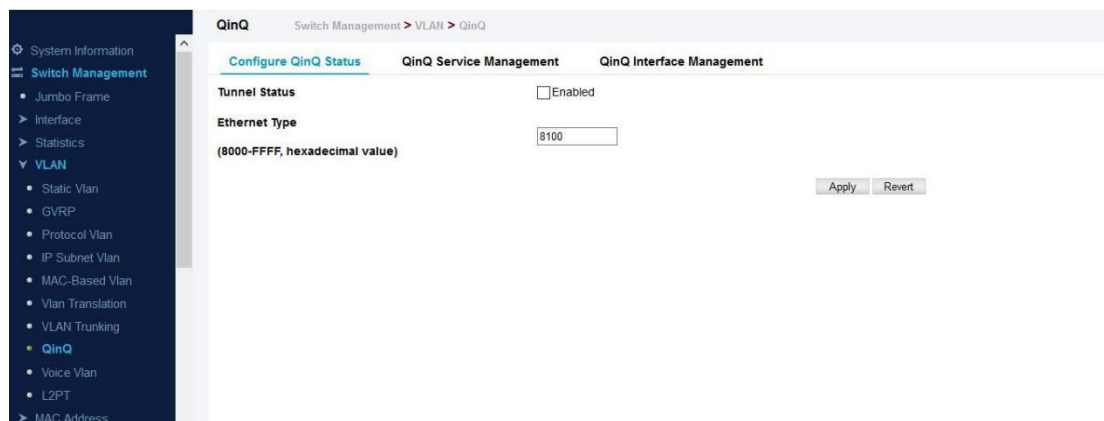
PARAMETERS

These parameters are displayed:

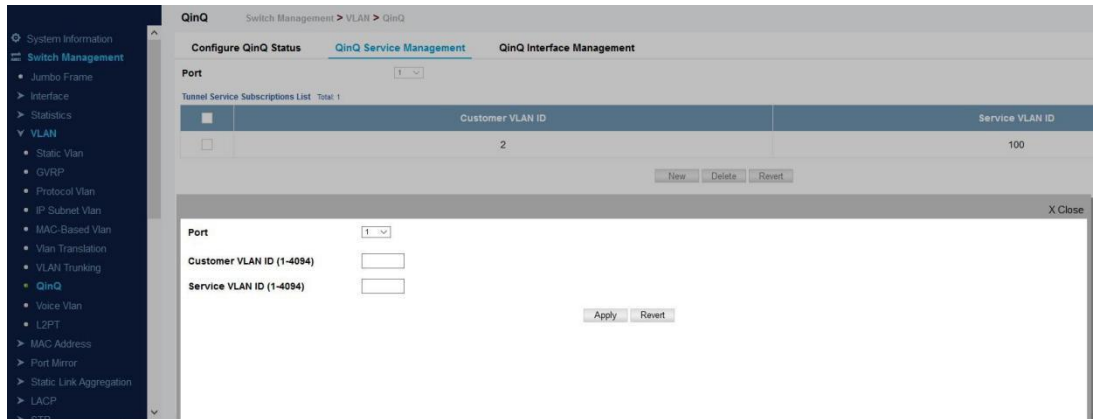
◆ **Tunnel Status** – Sets the switch to QinQ mode. (Default: Disabled)

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

Use this field to set a custom 802.1Q ethertype value for the 802.1Q Tunnel TPID. This feature allows the switch to interoperate with thirdparty switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port. The specified ethertype only applies to ports configured in Uplink mode. If the port is in normal mode, the TPID is always 8100. If the port is in Access mode, received packets are processed as untagged packets.



Switch Management > VLAN > QinQ > QinQ Service Management page is used to configure the QinQ entry.



Press New button to create new Qinq entry.

To delete a entry, select the entry and press delete button.

Switch Management > VLAN > Qinq > Qinq interface Management page is used to set the tunnel mode for any participating interface.

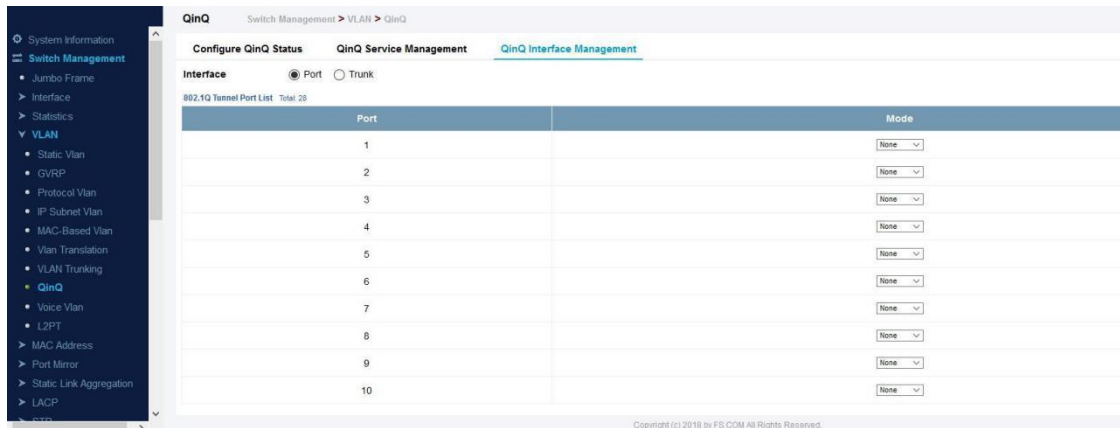
COMMAND USAGE

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

PARAMETERS

These parameters are displayed:

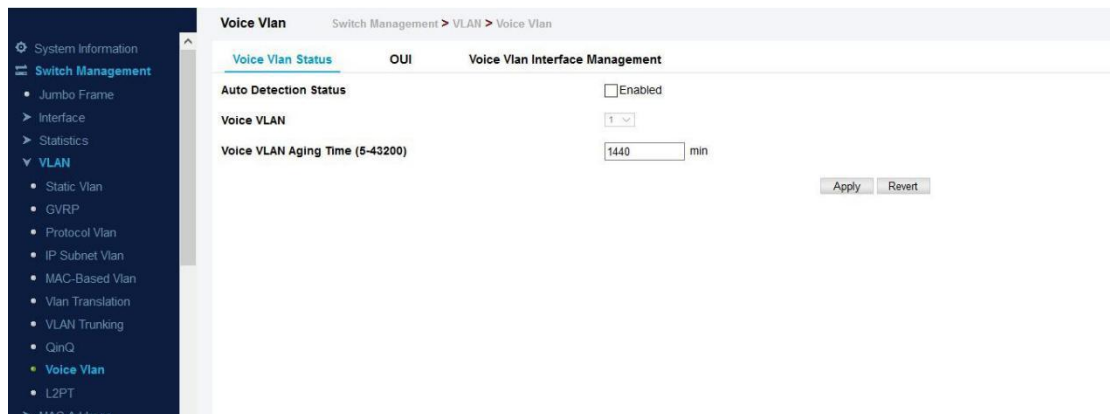
- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Port** – Port Identifier. (Range: 1-28)
- ◆ **Trunk** – Trunk Identifier. (Range: 1-12)
- ◆ **Mode** – Sets the VLAN membership mode of the port.
- **None** – The port operates in its normal VLAN mode. (This is the default.)
- **Access** – Configures Qinq tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
- **Uplink** – Configures Qinq tunneling for an uplink port to another device within the service provider network.



Voice Vlan

Switch Management > VLAN > Voice Vlan > Voice Vlan Status page is used to configure the voice vlan.

All ports are set to VLAN hybrid mode by default. Prior to enabling VoIP for a port first ensure that VLAN membership is not set to access mode.



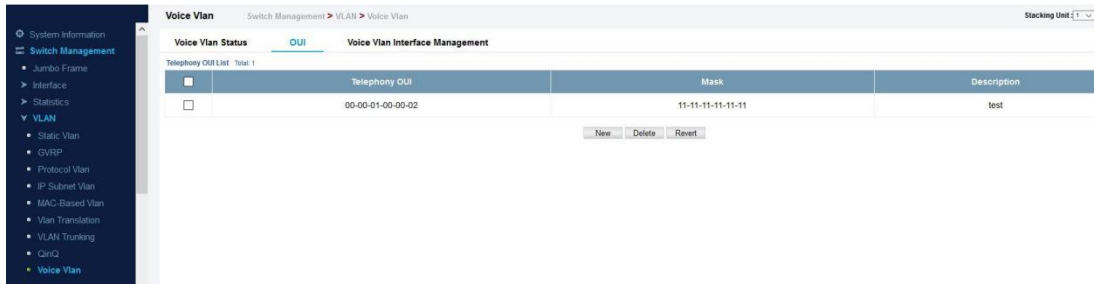
◆ **Auto Detection Status** – Enables the automatic detection of VoIP traffic on switch ports. (Default: Disabled)

◆ **Voice VLAN** – Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported and it must already be created on the switch. (Range: 1-4094)

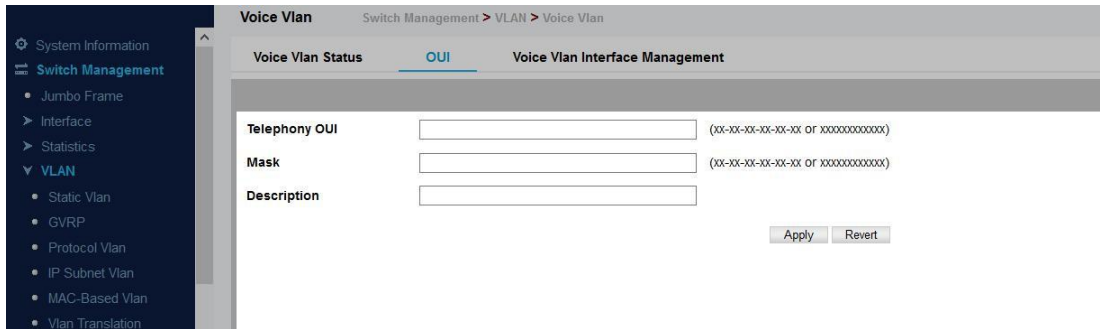
◆ **Voice VLAN Aging Time** – The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (Range: 5-43200 minutes; Default: 1440 minutes)

Note: The Voice VLAN ID cannot be modified when the global Auto Detection Status is enabled.

Switch Management > VLAN > Voice Vlan > OUI page is used to configure the Organizational Unique Identifier (OUI) in the source MAC address of received packets.



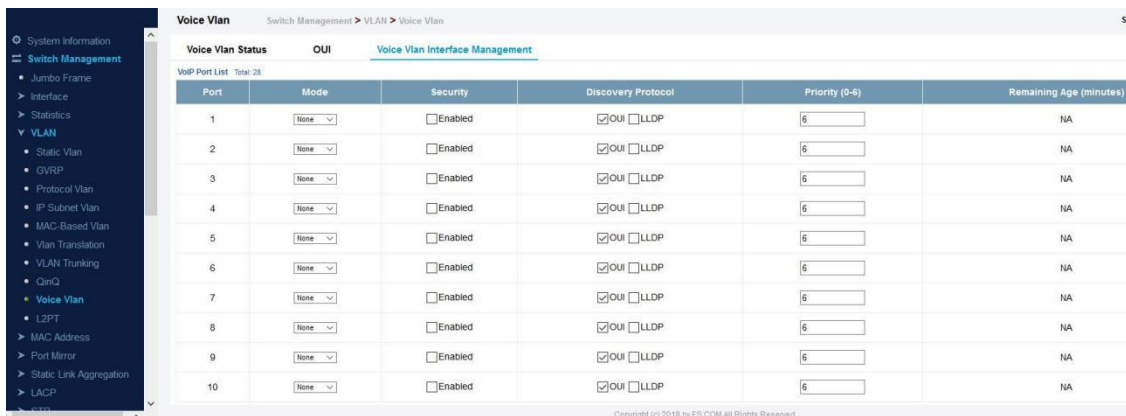
To create a OUI, press New button.



- ◆ **Telephony OUI** – Specifies a MAC address range to add to the list. Enter the MAC address in format 01-23-45-67-89-AB.
- ◆ **Mask** – Identifies a range of MAC addresses. Setting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Setting a mask of FF-FF-FF-FF-FF-FF specifies a single MAC address. (Default: FF-FF-FF-00-00-00)
- ◆ **Description** – User-defined text that identifies the VoIP devices

To delete a OUI, select the OUI and press delete button.

Switch Management > VLAN > Voice Vlan > Voice Vlan Interface Management page is used to configure ports for voice vlan, you need to set the mode (Auto or Manual), specify the discovery method to use, and set the traffic priority. You can also enable security filtering to ensure that only voice vlan traffic is forwarded on the Voice VLAN.



All ports are set to VLAN hybrid mode by default. Prior to enabling VoIP for a port (by setting

the VoIP mode to Auto or Manual as described below), first ensure that VLAN membership is not set to access mode.

◆ **Mode** – Specifies if the port will be added to the Voice VLAN when VoIP traffic is detected. (Default: None)

■ **None** – The Voice VLAN feature is disabled on the port. The port will not detect VoIP traffic or be added to the Voice VLAN.

■ **Auto** – The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port. You must select a method for detecting VoIP traffic, either OUI or 802.1AB (LLDP). When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list.

■ **Manual** – The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

◆ **Security** – Enables security filtering that discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped. (Default: Disabled)

◆ **Discovery Protocol** – Selects a method to use for detecting VoIP traffic on the port. (Default: OUI)

■ **OUI** – Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to vendors and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

■ **LLDP** – Uses LLDP (IEEE 802.1AB) to discover voice vlan devices attached to the port. LLDP checks that the “telephone bit” in the system capability TLV is turned on.

◆ **Priority** – Defines a CoS priority for port traffic on the Voice VLAN. The priority of any received voice vlan packet is overwritten with the new priority when the Voice VLAN feature is active for the port. (Range: 0-6; Default: 6)

◆ **Remaining Age** – Number of minutes before this entry is aged out.

The Remaining Age starts to count down when the OUI’s MAC address expires from the MAC address table. Therefore, the MAC address aging time should be added to the overall aging time. For example, if you configure the MAC address table aging time to 30 seconds, and the voice VLAN aging time to 5 minutes, then after 5.5 minutes, a port will be removed from voice VLAN when voice vlan traffic is no longer received on the port. Alternatively, if you clear the MAC address table manually, then the switch will also start counting down the Remaining Age.

L2PT

When L2PT is not used, protocol packets (such as STP) are flooded to 802.1Q access ports on the same edge switch, but filtered from 802.1Q tunnel ports. This creates disconnected protocol domains in the customer’s network. L2PT can be used to pass various types of protocol packets belonging to the same customer transparently across a service provider’s

network. In this way, normally segregated network segments can be configured to function inside a common protocol domain.

L2PT encapsulates protocol packets entering ingress ports on the service provider's edge switch, replacing the destination MAC address with a proprietary MAC address (for example, the spanning tree protocol uses 10-12-CF-00-00-02), a reserved address for other specified protocol types (as defined in IEEE 802.1ad – Provider Bridges), or a user-defined address. All intermediate switches carrying this traffic across the service provider's network treat these encapsulated packets in the same way as normal data, forwarding them across to the tunnel's egress port. The egress port decapsulates these packets, restores the proper protocol and MAC address information, and then floods them onto the same VLANs at the customer's remote site (via all of the appropriate tunnel ports and access ports²⁵ connected to the same metro VLAN). The way in which L2PT processes packets is based on the following criteria – (1) packet is received on a QinQ uplink port, (2) packet is received on a QinQ access port, or (3) received packet is Cisco-compatible L2PT (i.e., as indicated by a proprietary MAC address).

Processing protocol packets defined in IEEE 802.1ad – Provider Bridges

When an IEEE 802.1ad protocol packet is received on an uplink port (i.e., an 802.1Q tunnel ingress port connecting the edge switch to the service provider network) with the destination address 01-80-C2-00-00-00,0B~0F (C-VLAN tag), it is forwarded to all QinQ uplink ports and QinQ access ports in the same S-VLAN for which L2PT is enabled for that protocol. with the destination address 01-80-C2-00-00-01~0A (S-VLAN tag), it is filtered, decapsulated, and processed locally by the switch if the protocol is supported. When a protocol packet is received on an access port (i.e., an 802.1Q trunk port connecting the edge switch to the local customer network) with the destination address 01-80-C2-00-00-00,0B~0F (C-VLAN), and L2PT is enabled on the port, the frame is forwarded to all QinQ uplink ports and QinQ access ports on which L2PT is enabled for that protocol in the same S-VLAN. L2PT is disabled on the port, the frame is decapsulated and processed locally by the switch if the protocol is supported. with destination address 01-80-C2-00-00-01~0A (S-VLAN), the frame is filtered, decapsulated, and processed locally by the switch if the protocol is supported.

Processing Cisco-compatible protocol packets

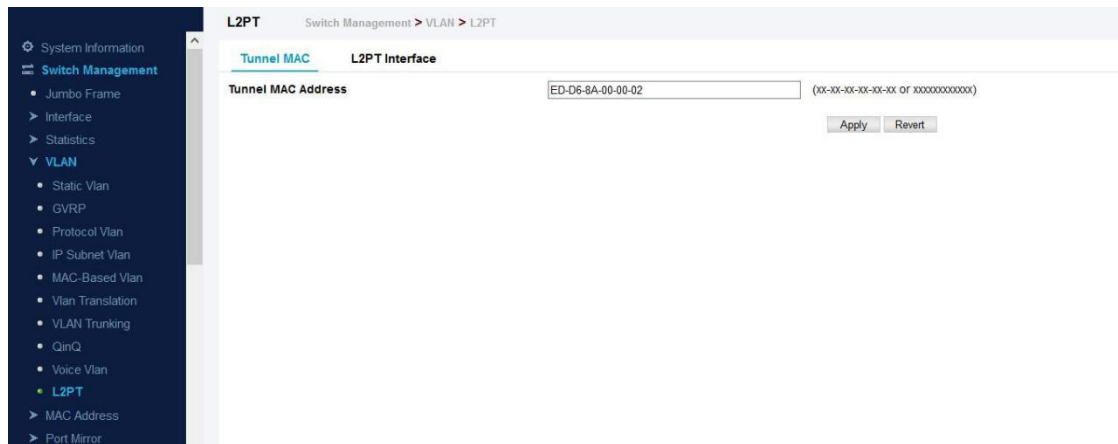
When a Cisco-compatible L2PT packet is received on an uplink port, and recognized as a CDP/VTP/STP/PVST+ protocol packet (where STP means STP/RSTP/MSTP), it is forwarded to the following ports in the same S-VLAN: (a) all access ports for which L2PT has been disabled, and (b) all uplink ports. recognized as a Generic Bridge PDU Tunneling (GBPT) protocol packet (i.e., having the destination address 01-00-0C-CD-CD-D0), it is forwarded to the following ports in the same S-VLAN:

other access ports for which L2PT is enabled after decapsulating the packet and restoring the proper protocol and MAC address information. all uplink ports. When a Cisco-compatible L2PT packet is received on an access port, and recognized as a CDP/VTP/STP/PVST+ protocol packet, and L2PT is enabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is enabled, and (b) uplink ports after rewriting the destination address to make it a GBPT protocol packet (i.e., setting the destination address to 01-00-0C-CD-CD-D0). L2PT is disabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is disabled, and

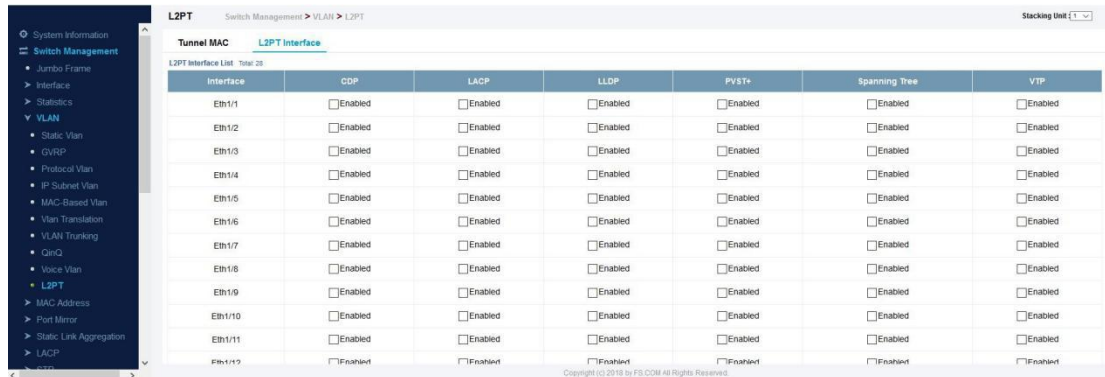
(b) all uplink ports. recognized as a GBPT protocol packet (i.e., having the destination address 01-00-0C-CD-CD-D0), and L2PT is enabled on this port, it is forwarded to other access ports in the same S-VLAN for which L2PT is enabled. L2PT is disabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is disabled, and (b) all uplink ports.

For L2PT to function properly.

Switch Management > VLAN > L2PT > Tunnel MAC page is used to configure the mac address used in L2PT packet header.



Switch Management > VLAN > L2PT > L2PT interface page is used to configure the interface process L2PT and what I2 protocols will be processed.



MAC Address

Dynamic MAC Learning

Switch Management > MAC Address > Dynamic MAC Learning > Show Dynamic Mac page is used to display the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated

port. Otherwise, the traffic is flooded to all ports.

PARAMETERS

These parameters are displayed:

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

Dynamic MAC Learning Stacking Unit: 1

Switch Management > MAC Address > Dynamic MAC Learning

[Show Dynamic MAC](#) [Clear Dynamic MAC](#) [Configure Aging](#) [Learning Status](#)

Query by:

Sort Key: MAC Address

MAC Address: (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)

VLAN: 1

Interface: Port 1 Trunk 1

Dynamic MAC Address List Total: 18

MAC Address	VLAN	Interface	Type	Life Time
00-00-01-03-00-11	1	Unit 1 / Port 22	Learn	Delete on Timeout
00-00-22-00-04-02	1	Unit 1 / Port 22	Learn	Delete on Timeout
00-70-02-11-00-04	1	Unit 1 / Port 22	Learn	Delete on Timeout
00-70-02-11-00-0A	1	Unit 1 / Port 22	Learn	Delete on Timeout
34-E6-D7-7B-98-8E	1	Unit 1 / Port 22	Learn	Delete on Timeout
54-E1-AD-FA-7A-7D	1	Unit 1 / Port 22	Learn	Delete on Timeout
5C-B9-01-0C-87-C8	1	Unit 1 / Port 22	Learn	Delete on Timeout

Switch Management > MAC Address > Dynamic MAC Learning > Clear Dynamic MAC page is used to remove any learned entries from the forwarding database.

PARAMETERS

These parameters are displayed:

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

Dynamic MAC Learning Stacking Unit: 1

Switch Management > MAC Address > Dynamic MAC Learning

[Show Dynamic MAC](#) [Clear Dynamic MAC](#) [Configure Aging](#) [Learning Status](#)

Clear by: All

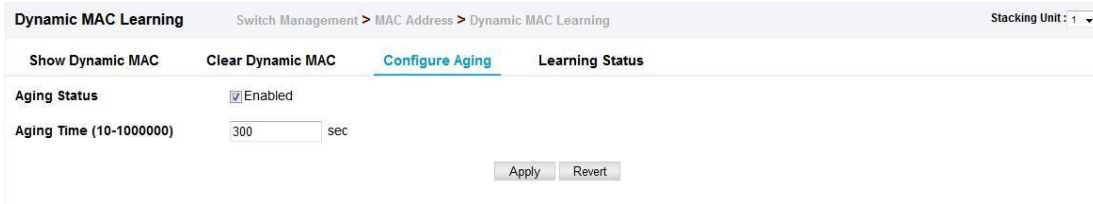
Changing the Aging Time

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

PARAMETERS

These parameters are displayed:

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



Static Mac Setting

Switch Management > MAC Address > Static Mac Setting page is used to configure static MAC addresses. A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

COMMAND USAGE

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- ◆ Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- ◆ Static addresses will not be removed from the address table when a given interface link is down.
- ◆ A static address cannot be learned on another port until the address is removed from the table.

PARAMETERS

These parameters are displayed:

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

WEB INTERFACE

To configure a static MAC address:

1. Click Switch Management, MAC Address, Static Mac Setting.
2. Specify the VLAN, the port or trunk to which the address will be assigned, the MAC address, and the time to retain this entry.
3. Click Apply.

X Close

VLAN 1 ▼

Interface Port 1 ▼ Trunk ▼

MAC Address (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)

Static Status Permanent ▼

Static Mac Setting Switch Management > MAC Address > Static Mac Setting Stacking Unit : 1 ▼

Static MAC Address to Interface Mapping Table Total: 2

☐	MAC Address	VLAN	Interface	Type	Life Time
☐	00-11-22-33-44-55	1	Unit 1 / Port 1	Config	Permanent
☐	00-E0-0C-00-00-FD	1	CPU	CPU	Delete on Reset

MAC Notification

Switch Management > MAC Address > MAC Notification page is used to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed.

Parameters

These parameters are displayed:

Configure Global

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

Configure Interface

- ◆ Port – Port Identifier. (Range: 1-28/52)
- ◆ MAC Notification Trap – Enables MAC authentication traps on the current interface. (Default: Disabled)

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

Web Interface

To enable MAC address traps at the global level:

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

MAC Notification Switch Management > MAC Address > MAC Notification

Global
Configure Interface

MAC Notification Traps Enabled

MAC Notification Trap Interval (1-3600) sec

MAC Notification Switch Management > MAC Address > MAC Notification Stacking Unit: 1

Global
Configure Interface

Interface Port Trunk

Port List Total: 28
1 2 3

Port	MAC Notification Trap
1	<input type="checkbox"/> Enabled
2	<input type="checkbox"/> Enabled
3	<input type="checkbox"/> Enabled
4	<input type="checkbox"/> Enabled
5	<input type="checkbox"/> Enabled
6	<input type="checkbox"/> Enabled
7	<input type="checkbox"/> Enabled
8	<input type="checkbox"/> Enabled
9	<input type="checkbox"/> Enabled
10	<input type="checkbox"/> Enabled

Port Mirror

Local Port Mirror

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

COMMAND USAGE

- ◆ Traffic can be mirrored from one or more source ports to a destination port on the same switch (local port mirroring as described in this section), or from one or more source ports on remote switches to a destination port on this switch.
- ◆ Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- ◆ When mirroring VLAN traffic or packets based on a source MAC address, the target port cannot be set to the same target ports as that used for port mirroring by this command.

◆ When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.

◆ Note that Spanning Tree BPDU packets are not mirrored to the target port.

PARAMETERS

These parameters are displayed:

◆ **Source Port** – The port whose traffic will be monitored.

◆ **Target Port** – The port that will mirror the traffic on the source port.

◆ **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)



RSPAN

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

COMMAND USAGE

◆ Traffic can be mirrored from one or more source ports to a destination port on the same switch, or from one or more source ports on remote switches to a destination port on this switch (remote port mirroring as described in this section).

◆ *Configuration Guidelines*

Take the following step to configure an RSPAN session:

1. Use the VLAN Static List to reserve a VLAN for use by RSPAN (marking the “Remote VLAN” field on this page. (Default VLAN 1 is prohibited.)
2. Set up the source switch on the RSPAN configuration page by specifying the mirror session, the switch’s role (Source), the RSPAN VLAN, and the uplink port1. Then specify the source port(s), and the traffic type to monitor (Rx, Tx or Both).
3. Set up all intermediate switches on the RSPAN configuration page, entering the mirror session, the switch’s role (Intermediate), the RSPAN VLAN, and the uplink port(s).
4. Set up the destination switch on the RSPAN configuration page by specifying the mirror session, the switch’s role (Destination), the destination port, whether or not the traffic exiting this port will be tagged or untagged, and the RSPAN VLAN. Then specify each uplink port where the mirrored traffic is being received.

◆ *RSPAN Limitations*

The following limitations apply to the use of RSPAN on this switch:

■ **RSPAN Ports** – Only ports can be configured as an RSPAN source, destination, or uplink; static and dynamic trunks are not allowed. A port can only be configured as one type of RSPAN interface – source, destination, or uplink. Also, note that the source port and destination port cannot be configured on the same switch.

■ **Local/Remote Mirror** – The destination of a local mirror session (created on the Interface > Port > Mirror page) cannot be used as the destination for RSPAN traffic.

■ **Spanning Tree** – If the spanning tree is disabled, BPDUs will not be flooded onto the RSPAN VLAN.

■ **MAC address learning** is not supported on RSPAN uplink ports when RSPAN is enabled on the switch. Therefore, even if spanning tree is enabled after RSPAN has been configured, MAC address learning will still not be re-started on the RSPAN uplink ports.

■ **IEEE 802.1X** – RSPAN and 802.1X are mutually exclusive functions.

When 802.1X is enabled globally, RSPAN uplink ports cannot be configured, even though RSPAN source and destination ports can still be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally.

■ **Port Security** – If port security is enabled on any port, that port cannot be set as an RSPAN uplink port, even though it can still be configured as an RSPAN source or destination port. Also, when a port is configured as an RSPAN uplink port, port security cannot be enabled on that port.

PARAMETERS

These parameters are displayed:

◆ **Session** – A number identifying this RSPAN session. (Range: 1)

Only one mirror session is allowed, including both local and remote mirroring. If local mirroring is enabled, then no session can be configured for RSPAN.

◆ **Operation Status** – Indicates whether or not RSPAN is currently functioning.

◆ **Switch Role** – Specifies the role this switch performs in mirroring traffic.

■ **None** – This switch will not participate in RSPAN.

■ **Source** - Specifies this device as the source of remotely mirrored traffic.

■ **Intermediate** - Specifies this device as an intermediate switch, transparently passing mirrored traffic from one or more sources to one or more destinations.

■ **Destination** - Specifies this device as a switch configured with a destination port which is to receive mirrored traffic for this session.

◆ **Remote VLAN** – The VLAN to which traffic mirrored from the source port will be flooded. The VLAN specified in this field must first be reserved for the RSPAN application using the Switch Management > VLAN > Static Vlan page.

◆ **Uplink Port** – A port on any switch participating in RSPAN through which mirrored traffic is passed on to or received from the RSPAN VLAN. Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch. Only destination and uplink ports will be assigned by the switch as members of the RSPAN VLAN. Ports cannot be manually assigned to an RSPAN VLAN through the Switch Management > VLAN > Static Vlan page. Nor can GVRP dynamically add port members to an RSPAN VLAN. Also, note that the Switch Management > VLAN >

Static Vlan page will not display any members for an RSPAN VLAN, but will only show configured RSPAN VLAN identifiers.

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

Source Port Configuration List Total: 28

Source Port	Type
1	None
2	None
3	None
4	None
5	None
6	None
7	None

Static Link Aggregation

Static Trunk

Switch Management >Static Link Aggregation > Static Trunk page is used to create and delete static trunk group.

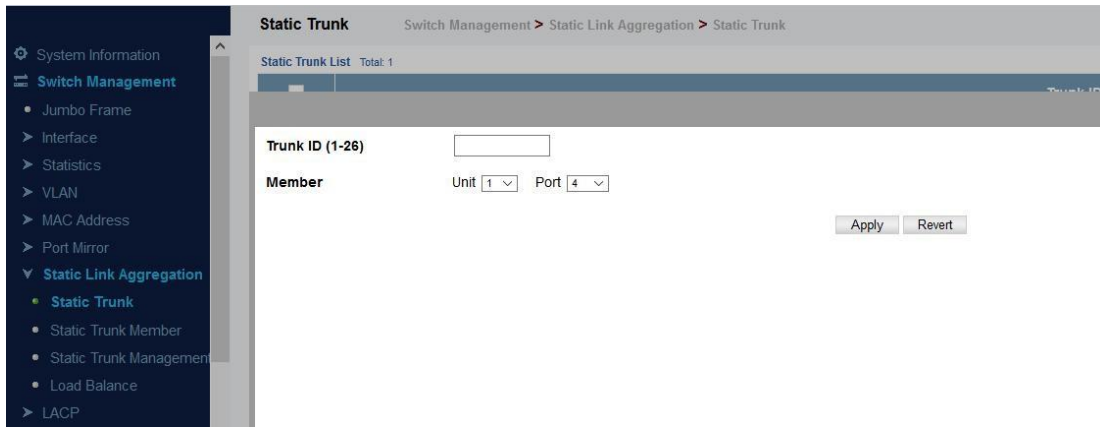
Static Trunk List Total: 1

Trunk ID
1

New Delete Revert

To create a static trunk group, press New button. You can create a trunk group with the first

member.



- ◆ **Trunk ID** – Trunk identifier. (Range: 1-12)
- ◆ **Member** – The initial trunk member. Use the Add Member page to
- Unit** – Unit identifier. (Range: 1)
- Port** – Port identifier. (Range: 1-28)

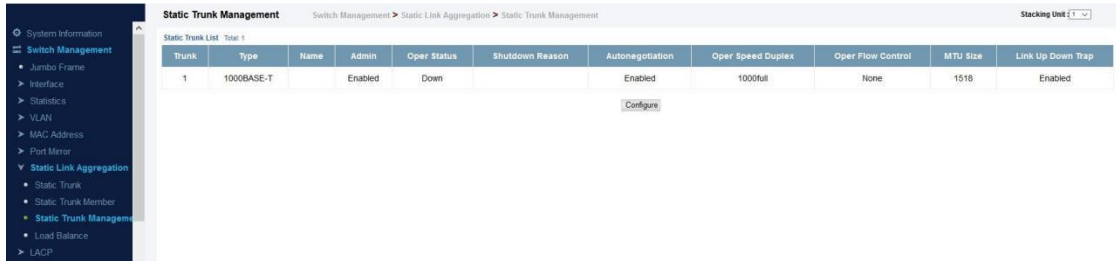
Static Trunk Member

Switch Management >Static Link Aggregation > Static Trunk member page is used to add and delete static trunk group member.

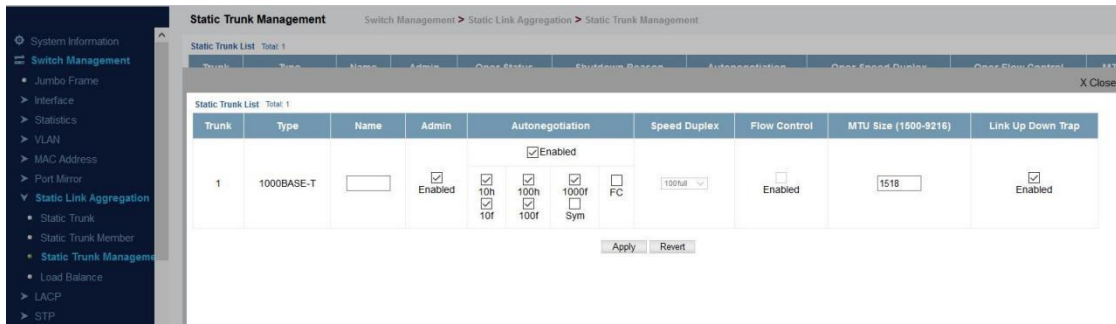


Static Trunk Management

Switch Management >Static Link Aggregation > Static Trunk Management page is used to configure the parameters of trunk group.

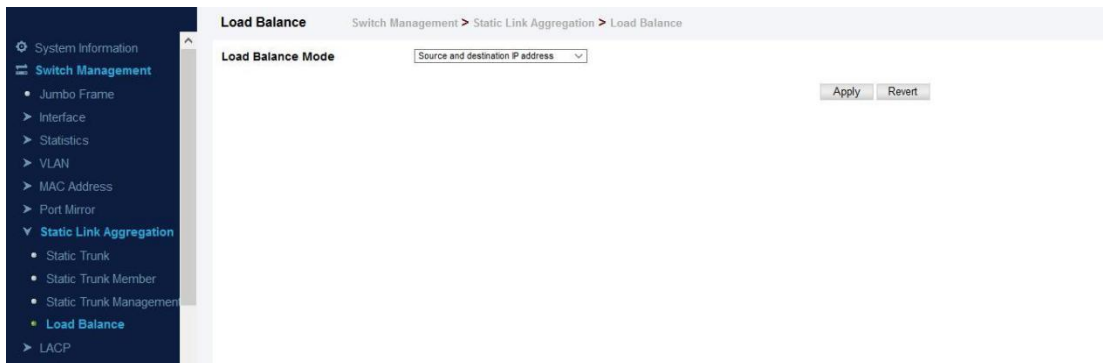


To configure the parameters, button configure button.



Load Balance

Switch Management >Static Link Aggregation > Load Balance page is used to configure the load balance mode of trunk group.



- ◆ This page applies to all static and dynamic trunks on the switch.
- ◆ To ensure that the switch traffic load is distributed evenly across all links in a trunk, select the source and destination addresses used in the load-balance calculation to provide the best result for trunk connections:
 - **Destination IP Address:** All traffic with the same destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.
 - **Destination MAC Address:** All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.
 - **Source and Destination IP Address:** All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router

trunk links where traffic through the switch is received from and destined for many different hosts.

■ **Source and Destination MAC Address:** All traffic with the same source and destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from and destined for many different hosts.

■ **Source IP Address:** All traffic with the same source IP address is output on the same link in a trunk. This mode works best for switch-to-router or switch-to-server trunk links where traffic through the switch is received from many different hosts.

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

LACP

- ◆ To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- ◆ If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- ◆ A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- ◆ If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- ◆ All ports on both ends of an LACP trunk must be configured for full duplex, and auto-negotiation.
- ◆ Ports are only allowed to join the same Link Aggregation Group (LAG) if (1) the LACP port system priority matches, (2) the LACP port admin key matches, and (3) the LAG admin key matches (if configured). However, if the LAG admin key is set, then the port admin key must be set to the same value for a port to be allowed to join that group.

Configure Aggregator

Switch Management >Static Link Aggregation > Load Balance page is used to configure parameters of aggregator.

Configure Aggregator Switch Management > LACP > Configure Aggregator Stacking Unit

Trunk	Admin Key (0-65535)	Timeout Mode	System Priority	System MAC Address
1	32768	Long Timeout	32768	EC-D6-8A-33-A2-7E
2	0	Long Timeout	32768	EC-D6-8A-33-A2-7E
3	0	Long Timeout	32768	EC-D6-8A-33-A2-7E
4	0	Long Timeout	32768	EC-D6-8A-33-A2-7E
5	0	Long Timeout	32768	EC-D6-8A-33-A2-7E
6	0	Long Timeout	32768	EC-D6-8A-33-A2-7E
7	0	Long Timeout	32768	EC-D6-8A-33-A2-7E
8	0	Long Timeout	32768	EC-D6-8A-33-A2-7E
9	0	Long Timeout	32768	EC-D6-8A-33-A2-7E
10	0	Long Timeout	32768	EC-D6-8A-33-A2-7E

Apply Revert

◆ **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default – Actor: 1, Partner: 0) By default, the Actor Admin Key is determined by port's link speed, and copied to Oper Key. The Partner Admin Key is assigned to zero, and the Oper Key is set based upon LACP PDUs received from the Partner.

◆ **Timeout Mode** – The timeout to wait for the next LACP data unit (LACPDU):

■ **Long Timeout** – Specifies a slow timeout of 90 seconds. (This is the default setting.)

■ **Short Timeout** – Specifies a fast timeout of 3 seconds.

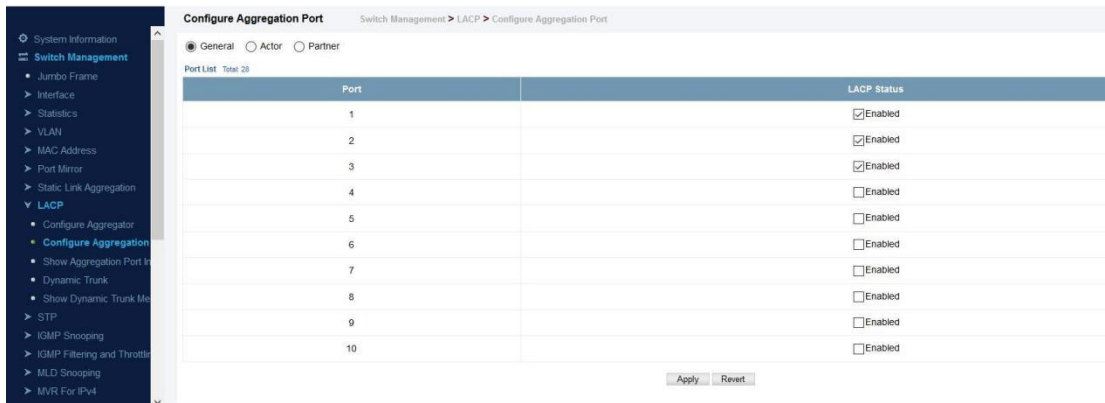
The timeout is set in the LACP timeout bit of the Actor State field in transmitted LACPDU. When the partner switch receives an LACPDU set with a short timeout from the actor switch, the partner adjusts the transmit LACPDU interval to 1 second. When it receives an LACPDU set with a long timeout from the actor, it adjusts the transmit LACPDU interval to 30 seconds. If the actor does not receive an LACPDU from its partner before the configured timeout expires, the partner port information will be deleted from the LACP group. When a dynamic port-channel member leaves a port-channel, the default timeout value will be restored on that port. When a dynamic port-channel is torn down, the configured timeout value will be retained. When the dynamic port-channel is constructed again, that timeout value will be used.

◆ **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768) System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.

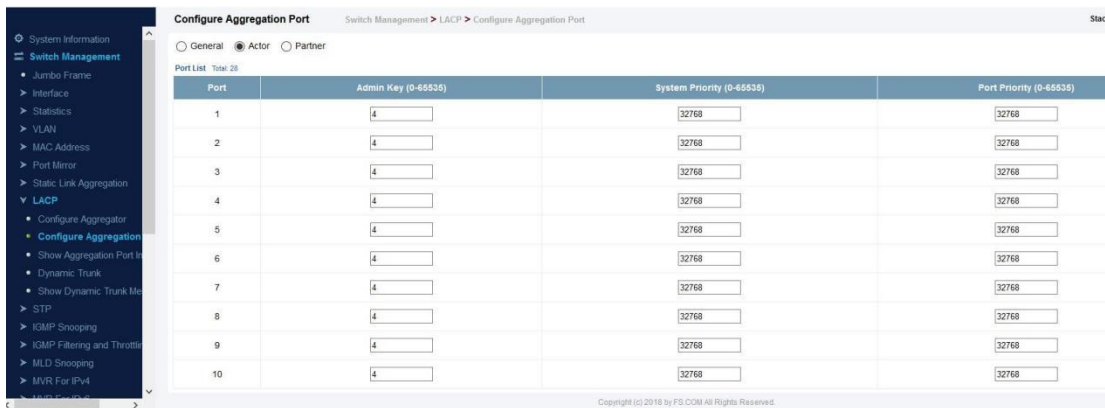
Configure Aggregation Port

Switch Management > LACP > Configure Aggregation Port page is used to enable LACP for a port, configure parameters of a local or remote port.

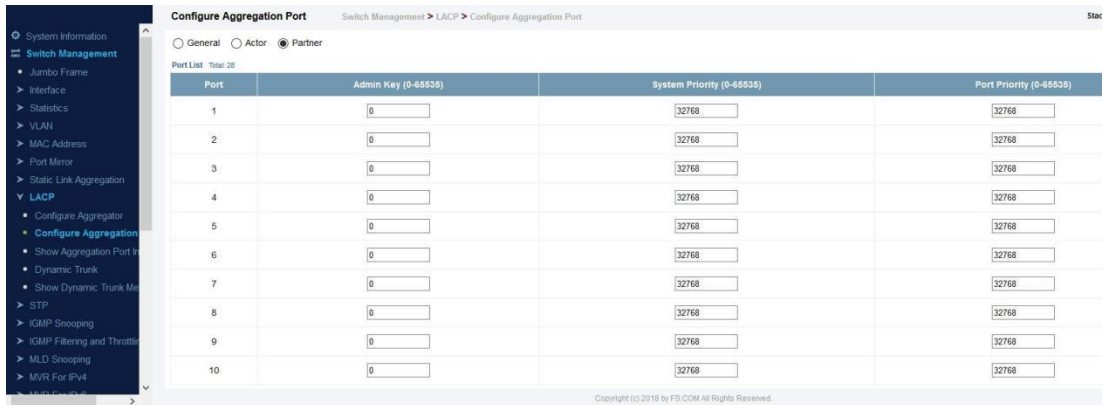
◆ Enable/disable port LACP



◆ LCAP parameters of a local port.



◆ LCAP parameters of a remote partner port.



◆ **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default – Actor: 1, Partner: 0) By default, the Actor Admin Key is determined by port's link speed, and copied to Oper Key. The Partner Admin Key is assigned to zero, and the Oper Key is set based upon LACP PDUs received from the Partner.

◆ **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768) System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.

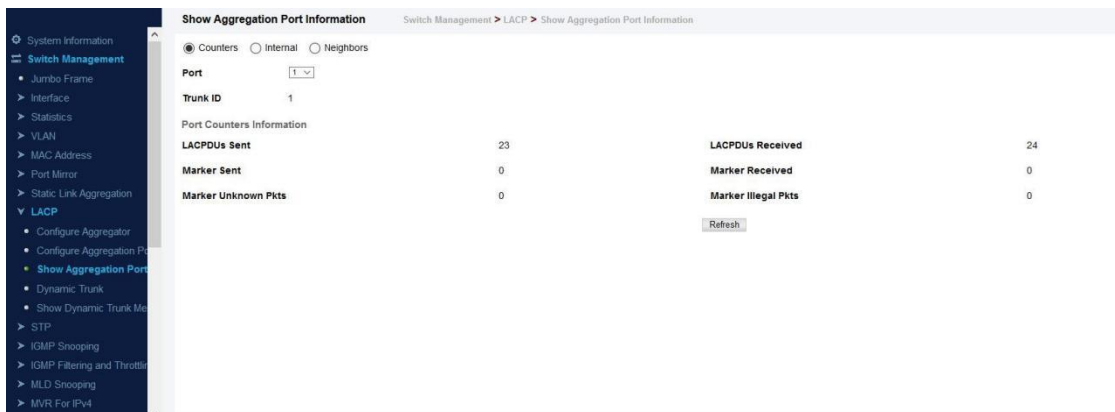
◆ **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- If an LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace an existing port member that has a lower priority.

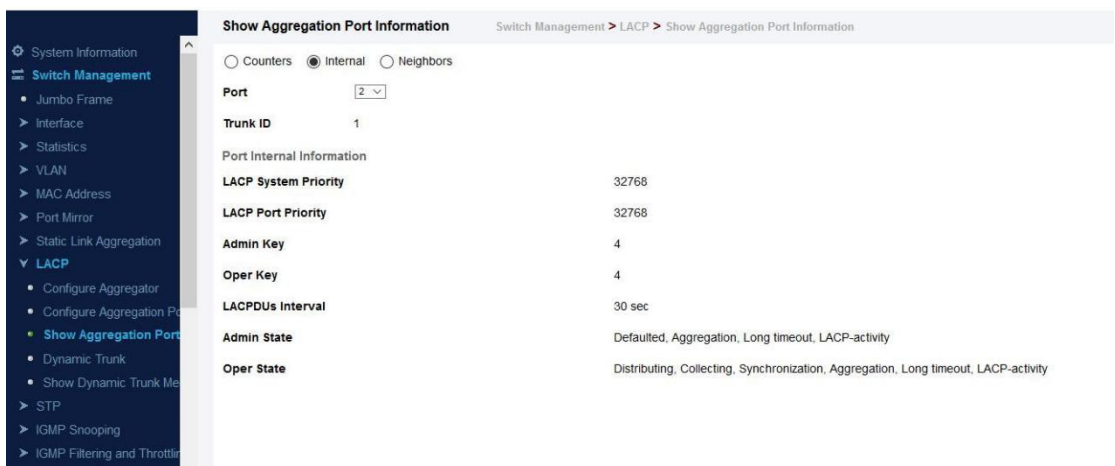
Show Aggregation Port Information

Switch Management > LACP > Show Aggregation Port Information page is used to display counters, information of local and remote port in LCAP group.

◆ Counters:



◆ Information of local port:



◆ Information of remote port:

Show Aggregation Port Information Switch Management > LACP > Show Aggregation Port Information

Counters
 Internal
 Neighbors

Port 2

Trunk ID 1

Port Neighbors Information

Partner Admin System ID	32768, 00-00-00-00-00-00
Partner Oper System ID	32768, EC-D6-8A-32-05-86
Partner Admin Port Number	2
Partner Oper Port Number	2
Port Admin Priority	32768
Port Oper Priority	32768
Admin Key	0
Oper Key	4
Admin State	Defaulted, Distributing, Collecting, Synchronization, Long timeout
Oper State	Distributing, Collecting, Synchronization, Aggregation, Long timeout, LACP-activity

Dynamic Trunk

Switch Management > LACP > Dynamic Trunk page is used to display and configure parameters of LCAP trunk group.

Dynamic Trunk Switch Management > LACP > Dynamic Trunk Stacking Unit (1)

Dynamic Trunk List Total: 1

Trunk	Type	Name	Admin	Oper Status	Shutdown Reason	Autonegotiation	Oper Speed Duplex	Oper Flow Control	MTU Size	Link Up Down Trap
1	1000BASE-T		Enabled	Up		Enabled	1000full	None	1518	Enabled

[Configure](#)

Show Dynamic Trunk Member

Switch Management > LACP > Show Dynamic Trunk Member page is used to display the current members of a LACP group.

Show Dynamic Trunk Member Switch Management > LACP > Show Dynamic Trunk Member

Trunk 1

Member List Total: 2

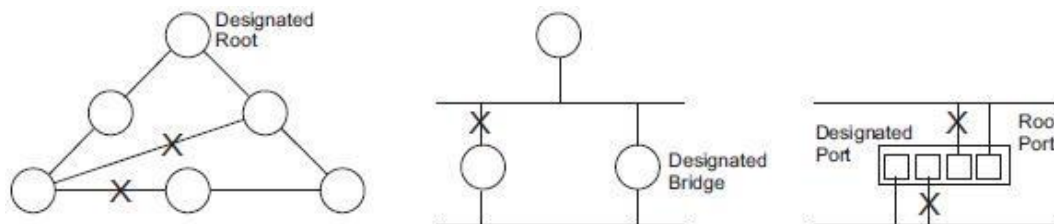
Member (Unit/Port)
1/1
1/2

STP

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

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

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

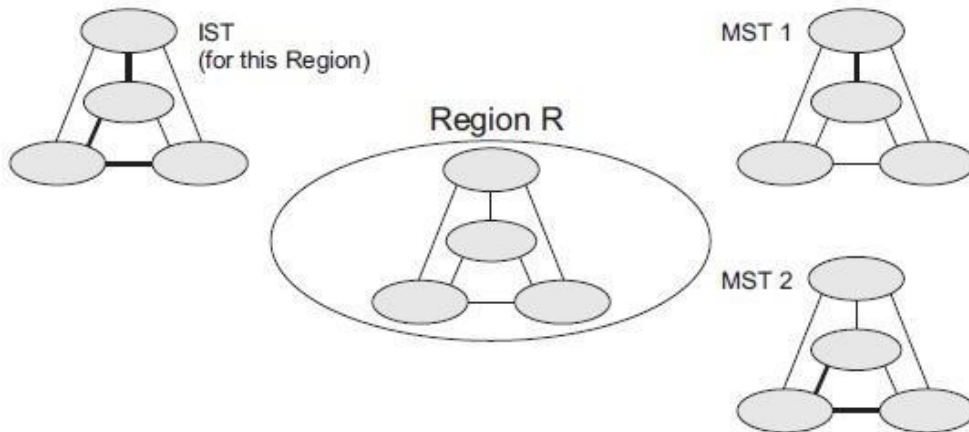


Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge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

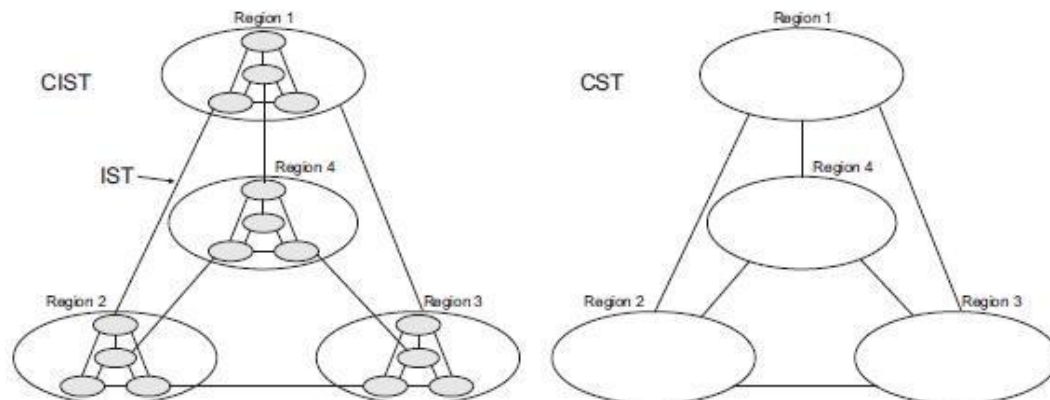
RSTP – RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves much faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning,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

MSTP – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. Using multiple spanning trees can provide multiple forwarding paths and enable load balancing. One or more VLANs can be

grouped into a Multiple Spanning Tree Instance (MSTI). MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. MSTP then builds a Internal Spanning Tree (IST) for the Region containing all commonly configured MSTP bridges.



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



MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols. Once you specify the VLANs to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

STP-RSTP

Switch Management > STP > STP-RSTP > Global Management page is used to configure global settings for the spanning tree that apply to the entire switch.

COMMAND USAGE

◆ Spanning Tree Protocol

This option uses RSTP set to STP forced compatibility mode. It uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

◆ Rapid Spanning Tree Protocol

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

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

■ **RSTP Mode** – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

◆ Multiple Spanning Tree Protocol

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

■ To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

■ A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

■ Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

PARAMETERS

These parameters are displayed:

Basic Configuration of Global Settings

◆ **Spanning Tree Status** – Enables/disables STA on this switch. (Default: Enabled)

◆ **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:

■ **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).

■ **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.

■ **MSTP:** Multiple Spanning Tree (IEEE 802.1s)

◆ **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)

■ **Default:** 32768

■ **Range:** 0-61440, in steps of 4096

■ **Options:** 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

◆ **BPDU Flooding** – Configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port.

■ **To VLAN:** Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID). This is the default.

■ **To All:** Floods BPDUs to all other ports on the switch. The setting has no effect if BPDU flooding is disabled on a port.

Advanced Configuration Settings

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

◆ **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

■ **Long:** Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)

■ **Short:** Specifies 16-bit based values that range from 1-65535.

◆ **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

When the Switch Becomes Root

◆ **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.

■ **Default:** 2

■ **Minimum:** 1

■ **Maximum:** The lower of 10 or $[(\text{Max. Message Age} / 2) - 1]$

◆ **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconverge. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)

■ **Default:** 20

■ **Minimum:** The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$

■ **Maximum:** The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$

◆ **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

■ Default: 15

■ Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$

■ Maximum: 30

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

Configuration Settings for MSTP

◆ **Max Instance Numbers** – The maximum number of MSTP instances to which this switch can be assigned.

◆ **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.

◆ **Region Revision⁴** – The revision for this MSTI. (Range: 0-65535; Default: 0)

◆ **Region Name⁴** – The name for this MSTI. (Maximum length: 32 characters; switch's MAC address)

◆ **Max Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

STP-RSTP Switch Management > STP > STP-RSTP

[Global Management](#) Configure Interface

Spanning Tree Status	<input checked="" type="checkbox"/> Enabled
Spanning Tree Type	RSTP ▾
Priority (0-61440, in steps of 4096)	<input type="text" value="32768"/>
BPDU Flooding	To VLAN ▾
Advanced:	
Path Cost Method	Long ▾
Transmission Limit (1-10)	<input type="text" value="3"/>
When the Switch Becomes Root:	
Hello Time (1-10)	<input type="text" value="2"/> sec
Maximum Age (6-40)	<input type="text" value="20"/> sec
Forward Delay (4-30)	<input type="text" value="15"/> sec

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

◆ **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree type is set to MSTP, and MAC address (where the address is taken from the switch system).

◆ **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.

◆ **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

◆ **Root Path Cost** – The path cost from the root port on this switch to the root device.

◆ **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.

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

STP-RSTP Switch Management > STP > STP-RSTP

[Global Management](#) [Configure Interface](#)

Spanning Tree Information

Spanning Tree Status	Enabled	Spanning Tree Type	RSTP
Designated Root	32768.000000001201	Bridge ID	32768.000000001201
Root Port	0	Max Age	20 sec
Root Path Cost	0	Hello Time	2 sec
Topology Changes	1	Forward Delay	15 sec
Last Topology Change	0 days, 0 hours, 15 minutes, 43 seconds		

[Configure](#)

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

PARAMETERS

These parameters are displayed:

◆ **Interface** – Displays a list of ports or trunks.

◆ **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled)

◆ **BPDU Flooding** - Enables/disables the flooding of BPDUs to other ports when global spanning tree is disabled or when spanning tree is disabled on a specific port. When flooding is enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port’s native VLAN as specified by the Spanning Tree BPDU Flooding attribute . (Default: Enabled)

◆ **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

■ Default: 128

■ Range: 0-240, in steps of 16

◆ **Admin Path Cost** – This parameter is used by the STA to determine the best path between

devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost takes precedence over port priority. (Range: 0 for auto-configuration, 1-65535 for the short path cost method, 1-200,000,000 for the long path cost method) By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 12: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

Table 13: Default STA Path Costs

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

◆ **Admin Link Type** – The link type attached to this interface.

■ **Point-to-Point** – A connection to exactly one other bridge.

■ **Shared** – A connection to two or more bridges.

■ **Auto** – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)

◆ **Root Guard** – STA allows a bridge with a lower bridge identifier (or same identifier and lower MAC address) to take over as the root bridge at any time. Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed. (Default: Disabled)

◆ **Admin Edge Port** – Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an endnode device. (Default: Auto)

- **Enabled** – Manually configures a port as an Edge Port.
- **Disabled** – Disables the Edge Port setting.
- **Auto** – The port will be automatically configured as an edge port if the edge delay time expires without receiving any RSTP or MSTP BPDUs. Note that edge delay time (802.1D-2004 17.20.4) equals the protocol migration time if a port's link type is point-to-point (which is 3 seconds as defined in IEEE 802.3D-2004 17.20.4); otherwise it equals the spanning tree's maximum age for configuration messages. An interface cannot function as an edge port under the following conditions:
 - If spanning tree mode is set to STP , edge-port mode cannot automatically transition to operational edge-port state using the automatic setting.
 - If loopback detection is enabled and a loopback BPDU is detected, the interface cannot function as an edge port until the loopback state is released.
 - If an interface is in forwarding state and its role changes, the interface cannot continue to function as an edge port even if the edge delay time has expired.
 - If the port does not receive any BPDUs after the edge delay timer expires, its role changes to designated port and it immediately enters forwarding state.
- ◆ **BPDU Guard** – This feature protects edge ports from receiving BPDUs. It prevents loops by shutting down an edge port when a BPDU is received instead of putting it into the spanning tree discarding state. In a valid configuration, configured edge ports should not receive BPDUs. If an edge port receives a BPDU an invalid configuration exists, such as a connection to an unauthorized device. The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port. (Default: Disabled)
- ◆ **BPDU Filter** – BPDU filtering allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. By default, STA sends BPDUs to all ports regardless of whether administrative edge is enabled on a port. BPDU filtering is configured on a per-port basis. (Default: Disabled)
- ◆ **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STPcompatible) to send on the selected interfaces. (Default: Disabled)

STP-RSTP Switch Management > STP > STP-RSTP

Global Management [Configure Interface](#)

Interface Port Trunk X Close

Port List Total: 26

Port	Spanning Tree	BPDU Flooding	Priority (0-240, in steps of 16)	Admin Path Cost (0-200000000, 0: Auto)	Admin Link Type	Root Guard	Admin Edge Port	BPDU Guard	BPDU Guard Auto Recovery	BPDU Guard Auto Recovery Interval (30-86400)	BPDU Filter	Migration	TC Propagate Stop
1	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
2	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
3	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
4	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
5	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
6	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
7	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled
8	Enabled	Enabled	128	0	Auto	Enabled	Auto	Enabled	Enabled	300	Enabled	Enabled	Enabled

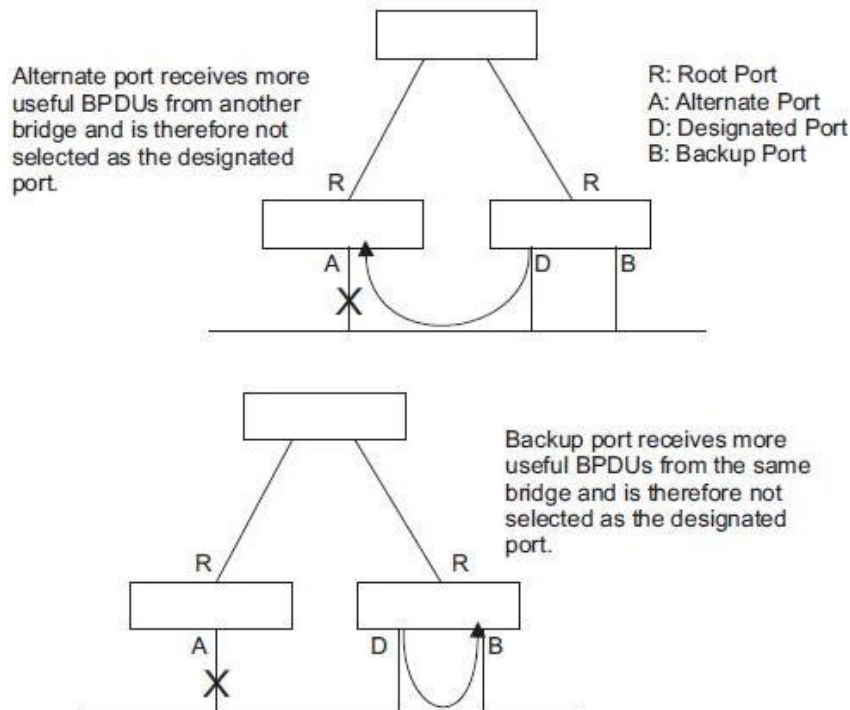
Switch Management > STP > STP-RSTP > Configure Interface page is used to display the current status of ports or trunks in the Spanning Tree.

PARAMETERS

These parameters are displayed:

- ◆ **Spanning Tree** – Shows if STA has been enabled on this interface.
- ◆ **BPDU Flooding** – Shows if BPDUs will be flooded to other ports when spanning tree is disabled globally on the switch or disabled on a specific port.
- ◆ **STA Status** – Displays current state of this port within the Spanning Tree:
 - **Discarding** - Port receives STA configuration messages, but does not forward packets.
 - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
 - **Forwarding** - Port forwards packets, and continues learning addresses. The rules defining port status are:
 - A port on a network segment with no other STA compliant bridging device is always forwarding.
 - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
 - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- ◆ **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- ◆ **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- ◆ **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- ◆ **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.

- ◆ **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- ◆ **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration .
- ◆ **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- ◆ **Port Role** – Roles are assigned according to whether the port is part of the active topology, that is the best port connecting a non-root bridge to the root bridge (i.e., **root port**), connecting a LAN through the bridge to the root bridge (i.e., **designated port**), is the MSTI regional root (i.e., **master port**), or is an **alternate** or **backup port** that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled port**) if a port has no role within the spanning tree.



STP-RSTP Stacking Unit 1

Global Management [Configure Interface](#)

Interface Port Trunk

Spanning Tree Port List Total: 26

Port	Spanning Tree	BPDU Flooding	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Enabled	Enabled	Discarding	0	0	32768.000000001201	128.1	10000	Point-to-Point	Disabled	Disabled
2	Enabled	Enabled	Discarding	0	0	32768.000000001201	128.2	10000	Point-to-Point	Disabled	Disabled
3	Enabled	Enabled	Discarding	0	0	32768.000000001201	128.3	10000	Point-to-Point	Disabled	Disabled
4	Enabled	Enabled	Discarding	0	0	32768.000000001201	128.4	10000	Point-to-Point	Disabled	Disabled
5	Enabled	Enabled	Discarding	0	0	32768.000000001201	128.5	10000	Point-to-Point	Disabled	Disabled
6	Enabled	Enabled	Discarding	0	0	32768.000000001201	128.6	10000	Point-to-Point	Disabled	Disabled
7	Enabled	Enabled	Discarding	0	0	32768.000000001201	128.7	10000	Point-to-Point	Disabled	Disabled
8	Enabled	Enabled	Discarding	0	0	32768.000000001201	128.8	10000	Point-to-Point	Disabled	Disabled
9	Enabled	Enabled	Discarding	0	0	32768.000000001201	128.9	10000	Point-to-Point	Disabled	Disabled
10	Enabled	Enabled	Discarding	0	0	32768.000000001201	128.10	10000	Point-to-Point	Disabled	Disabled

[Configure](#)

MSTP

Switch Management > STP > MSTP > MST List page is used to create an MSTP instance, or to add VLAN groups to an MSTP instance.

COMMAND USAGE

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 33 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

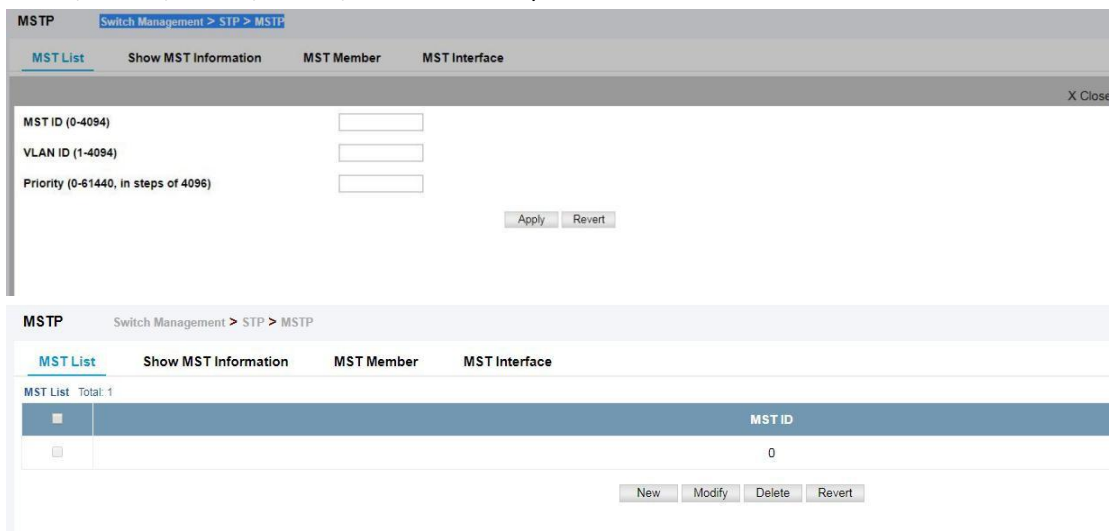
To use multiple spanning trees:

1. Set the spanning tree type to MSTP .
2. Enter the spanning tree priority for the selected MST instance on the Spanning Tree > MSTP (Configure Global - Add) page.
3. Add the VLANs that will share this MSTI on the Spanning Tree > MSTP (Configure Global - Add Member) page. To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

PARAMETERS

These parameters are displayed:

- ◆ **MST ID** – Instance identifier to configure. (Range: 0-4094)
- ◆ **VLAN ID** – VLAN to assign to this MST instance. (Range: 1-4093)
- ◆ **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)



The screenshot displays the MSTP configuration interface. The top section is titled 'MSTP' and includes a breadcrumb 'Switch Management > STP > MSTP'. Below this are tabs for 'MST List', 'Show MST Information', 'MST Member', and 'MST Interface'. The 'MST List' tab is active, showing a form with three input fields: 'MST ID (0-4094)', 'VLAN ID (1-4094)', and 'Priority (0-61440, in steps of 4096)'. There are 'Apply' and 'Revert' buttons at the bottom of the form. Below the form is a table titled 'MST List' with a total of 1 entry. The table has a header row with 'MST ID' and a data row with the value '0'. At the bottom of the table are buttons for 'New', 'Modify', 'Delete', and 'Revert'.

MSTP Switch Management > STP > MSTP

[MST List](#) [Show MST Information](#) [MST Member](#) [MST Interface](#)

MST Details List Total: 1

MST ID	Priority (0-61440, in steps of 4096)
0	<input type="text" value="32768"/>

MSTP Switch Management > STP > MSTP

[MST List](#) [Show MST Information](#) [MST Member](#) [MST Interface](#)

MST ID

Priority	32768	Designated Root	32768.0.00000000202
Bridge ID	32768.0.000000001201	Root Port	16
Max Age	20 sec	Root Path Cost	110000
Hello Time	2 sec	Configuration Changes	0
Forward Delay	15 sec	Last Topology Change	0 hrs 20 mins 54 seconds

MSTP Switch Management > STP > MSTP

[MST List](#) [Show MST Information](#) [MST Member](#) [MST Interface](#)

MST ID

VLAN ID (1-4094)

Switch Management > STP > MSTP > MST Interface page is used to configure the STA interface settings for an MST instance.

PARAMETERS

These parameters are displayed:

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

over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

The recommended range is listed in Table 12 .

The default path costs are listed in Table 13 .

MSTP Switch Management > STP > MSTP

MST List Show MST Information MST Member **MST Interface**

MST ID: 0

Interface: Port Trunk

Spanning Tree Port List Total: 26

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

To display MSTP parameters for a port or trunk:

MSTP Switch Management > STP > MSTP Stacking Unit: 1

MST List Show MST Information MST Member **MST Interface**

MST ID: 0

Interface: Port Trunk

Spanning Tree Port List Total: 26

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Discarding	0	110000	32768.0.000000001201	128.1	10000	Point-to-Point	Disabled	Disabled
2	Discarding	0	110000	32768.0.000000001201	128.2	10000	Point-to-Point	Disabled	Disabled
3	Discarding	0	110000	32768.0.000000001201	128.3	10000	Point-to-Point	Disabled	Disabled
4	Discarding	0	110000	32768.0.000000001201	128.4	10000	Point-to-Point	Disabled	Disabled
5	Discarding	0	110000	32768.0.000000001201	128.5	10000	Point-to-Point	Disabled	Disabled
6	Discarding	0	110000	32768.0.000000001201	128.6	10000	Point-to-Point	Disabled	Disabled
7	Discarding	0	110000	32768.0.000000001201	128.7	10000	Point-to-Point	Disabled	Disabled
8	Discarding	0	110000	32768.0.000000001201	128.8	10000	Point-to-Point	Disabled	Disabled
9	Discarding	0	110000	32768.0.000000001201	128.9	10000	Point-to-Point	Disabled	Disabled
10	Discarding	0	110000	32768.0.000000001201	128.10	10000	Point-to-Point	Disabled	Disabled

Loopback Detection

Switch Management > STP > Loopback Detection page is used to configure loopback detection on an interface. When loopback detection is enabled and a port or trunk receives it’s own BPDU, the detection agent drops the loopback BPDU, sends an SNMP trap, and places the interface in discarding mode. This loopback state can be released manually or automatically. If the interface is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:

- ◆ The interface receives any other BPDUs except for its own, or;
- ◆ The interfaces' link status changes to link down and then link up again, or;
- ◆ The interface ceases to receive its own BPDUs in a forward delay interval.

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **Status** – Enables loopback detection on this interface. (Default: Enabled)
- ◆ **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)
- ◆ **Release Mode** – Configures the interface for automatic or manual loopback release. (Default: Auto)
- ◆ **Release** – Allows an interface to be manually released from discard mode. This is only available if the interface is configured for manual release mode.
- ◆ **Action** – Sets the response for loopback detection to block user traffic or shut down the interface. (Default: Block)
- ◆ **Shutdown Interval** – The duration to shut down the interface. (Range: 60-86400 seconds; Default: 60 seconds) If an interface is shut down due to a detected loopback, and the release mode is set to "Auto," the selected interface will be automatically enabled when the shutdown interval has expired.

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

Loopback Detection Stacking Unit: 1

Switch Management > STP > Loopback Detection

Interface Port Trunk

Loopback Detection Port List Total: 26

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

IGMP Snooping

IGMP Snooping and Query – 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. IGMP Snooping conserves bandwidth on network segments where no node has expressed interest in receiving a specific multicast service. For switches that do not support multicast routing, or where multicast routing is already enabled on other switches in the local network segment, IGMP Snooping is the only service required to support multicast filtering. When using IGMPv3 snooping, service requests from IGMP Version 1, 2 or 3 hosts are all forwarded to the upstream router as IGMPv3 reports. The primary enhancement provided by IGMPv3 snooping is in keeping track of information about the specific multicast sources which downstream IGMPv3 hosts have requested or refused. The switch maintains information about both multicast groups and channels, where a group indicates a multicast flow for which the hosts have *not* requested a specific source

(the only option for IGMPv1 and v2 hosts unless statically configured on the switch), and a channel indicates a flow for which the hosts have requested service from a specific source. For IGMPv1/v2 hosts, the source address of a channel is always null (indicating that any source is acceptable), but for IGMPv3 hosts, it may include a specific address when requested. Only IGMPv3 hosts can request service from a specific multicast source. When downstream hosts request service from a specific source for a multicast service, these sources are all placed in the Include list, and traffic is forwarded to the hosts from each of these sources. IGMPv3 hosts may also request that service be forwarded from any source except for those specified. In this case, traffic is filtered from sources in the Exclude list, and forwarded from all other available sources. Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch. This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch. Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch. IGMP Snooping with Proxy Reporting – The switch supports last leave, and query suppression (as defined in DSL Forum TR-101, April 2006):

- ◆ When proxy reporting is disabled, all IGMP reports received by the switch are forwarded natively to the upstream multicast routers.
- ◆ Last Leave: Intercepts, absorbs and summarizes IGMP leaves coming from IGMP hosts. IGMP leaves are relayed upstream only when necessary, that is, when the last user leaves a multicast group.
- ◆ Query Suppression: Intercepts and processes IGMP queries in such a way that IGMP specific queries are never sent to client ports. The only deviation from TR-101 is that the marking of IGMP traffic initiated by the switch with priority bits as defined in R-250 is not supported.

General

Switch Management > IGMP Snooping > General page is used to configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

COMMAND USAGE

- ◆ **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.
- ◆ **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any

upstream multicast switch/router to ensure that it will continue to receive the multicast service.

PARAMETERS

These parameters are displayed:

◆ **IGMP Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled) When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence. When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

◆ **Proxy Reporting Status** – Enables IGMP Snooping with Proxy Reporting. (Default: Disabled)

When proxy reporting is enabled with this command, the switch performs “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device. When proxy reporting is disabled, all IGMP reports received by the switch are forwarded natively to the upstream multicast routers.

◆ **TCN Flood** – Enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. (Default: Disabled) When a spanning tree topology change occurs, the multicast membership information learned by switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, a switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with TC bit set (by the root bridge) will enter into “multicast flooding mode” for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned. If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a time out mechanism is used to delete all of the currently learned multicast channels. When a new uplink port starts up, the switch sends unsolicited reports for all currently learned channels out the new uplink port. By default, the switch immediately enters into “multicast flooding mode” when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive packet loss on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned. Otherwise, the time spent in flooding mode can be manually configured to reduce excessive loading. When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN. The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

◆ **TCN Query Solicit** – Sends out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. (Default: Disabled) When the root bridge in a

spanning tree receives a TCN for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (or query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred. When an upstream multicast router receives this solicitation, it immediately issues an IGMP general query. A query solicitation can be sent whenever the switch notices a topology change, even if it is not the root bridge in spanning tree.

◆ **Router Alert Option** – Discards any IGMPv2/v3 packets that do not include the Router Alert option. (Default: Disabled) As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value. To protect against this kind of attack, (1) routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option. (2) Also, when the switch is acting in the role of a multicast host (such as when using proxy routing), it should ignore version 2 or 3 queries that do not contain the Router Alert option.

◆ **Unregistered Data Flooding** – Floods unregistered multicast traffic into the attached VLAN. (Default: Disabled) Once the table used to store multicast entries for IGMP snooping and multicast routing is filled, no new entries are learned. If no router port is configured in the attached VLAN, and unregistered-flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

◆ **Forwarding Priority** – Assigns a CoS priority to all multicast traffic. (Range: 0-6, where 6 is the highest priority) This parameter can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

◆ **Version Exclusive** – Discards any received IGMP messages which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

◆ **IGMP Unsolicited Report Interval** – Specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. (Range: 1-65535 seconds, Default: 400 seconds) When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels via the new upstream interface. This command only applies when proxy reporting is enabled.

◆ **Router Port Expire Time** – The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535, Recommended Range: 300-500 seconds, Default: 300)

◆ **IGMP Snooping Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2) This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

◆ **Querier Status** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. This feature is not supported for IGMPv3 snooping. (Default: Disabled)

General Switch Management > IGMP Snooping > General

IGMP Snooping Status	<input type="checkbox"/> Enabled
Proxy Reporting Status	<input type="checkbox"/> Enabled
TCN Flood	<input type="checkbox"/> Enabled
TCN Query Solicit	<input type="checkbox"/> Enabled
Router Alert Option	<input type="checkbox"/> Enabled
Unregistered Data Flooding	<input type="checkbox"/> Enabled
Forwarding Priority (0-7)	<input type="checkbox"/> <input type="text" value=""/>
Version Exclusive	<input type="checkbox"/> Enabled
IGMP Unsolicited Report Interval (1-65535)	<input type="text" value="400"/> seconds
Router Port Expire Time (1-65535)	<input type="text" value="300"/> seconds
IGMP Snooping Version (1-3)	<input type="text" value="2"/>
Querier Status	<input type="checkbox"/> Enabled

Current Multicast

Switch Management > IGMP Snooping> Current Multicast Router page is used to statically show an interface to a multicast router/switch.

Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, the interface (and a specified VLAN) can be manually configured to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

COMMAND USAGE

IGMP Snooping must be enabled globally on the switch before a multicast router port can take effect.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4093)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Trunk** – Specifies the interface attached to a multicast router.

Current Multicast Router Switch Management > IGMP Snooping > Current Multicast Router

VLAN

Multicast Router Interface Information Total: 3

Interface	Type	Expire
Unit 1 / port 1	Static	
Unit 1 / port 10	Static	
Unit 1 / port 11	Static	

Static Multicast Router

Switch Management > IGMP Snooping > Static Multicast Router page is used to statically attach an interface to a multicast router/switch. Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, the interface (and a specified VLAN) can be manually configured to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

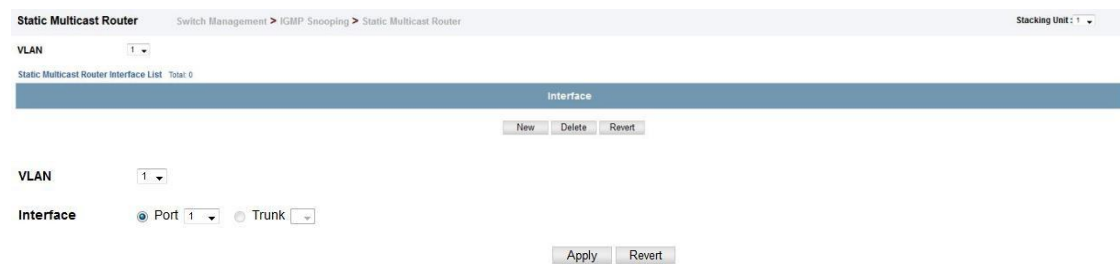
COMMAND USAGE

IGMP Snooping must be enabled globally on the switch before a multicast router port can take effect.

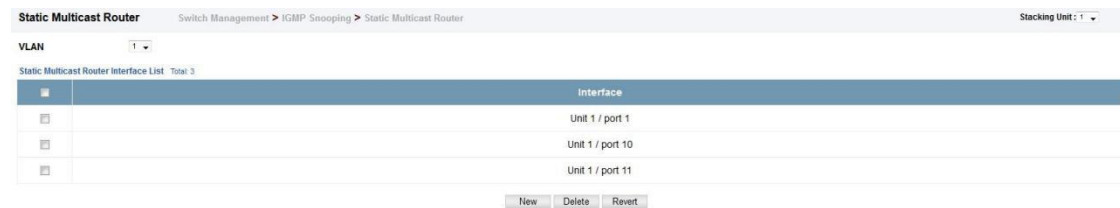
PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4093)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Trunk** – Specifies the interface attached to a multicast router.



To show the static interfaces attached to a multicast router:



Static Member

Switch Management > IGMP Snooping > Static Member page is used to statically assign a multicast service to an interface. Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages. However, for certain applications that require tighter control, it may be necessary to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

COMMAND USAGE

- ◆ Static multicast addresses are never aged out.

- ◆ When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4093)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Trunk** – Specifies the interface assigned to a multicast group.
- ◆ **Multicast IP** – The IP address for a specific multicast service.

Static Member Switch Management > IGMP Snooping > Static Member Stacking Unit: 1

VLAN 1

IGMP Member Interface List Total: 3

	Interface	Multicast IP
<input type="checkbox"/>	Unit 1 / Port 1	224.1.1.1
<input type="checkbox"/>	Unit 1 / Port 2	224.1.1.2
<input type="checkbox"/>	Unit 1 / Port 3	224.1.1.3

New Delete Revert

VLAN 1

Interface Port 1 Trunk

Multicast IP

Apply Revert

To show the static interfaces assigned to a multicast service:

Static Member Switch Management > IGMP Snooping > Static Member Stacking Unit: 1

VLAN 1

IGMP Member Interface List Total: 3

	Interface	Multicast IP
<input type="checkbox"/>	Unit 1 / Port 1	224.1.1.1
<input type="checkbox"/>	Unit 1 / Port 2	224.1.1.2
<input type="checkbox"/>	Unit 1 / Port 3	224.1.1.3

New Delete Revert

VLAN Information

Switch Management > IGMP Snooping > VLAN Information page is used to configure IGMP snooping attributes for a VLAN.

COMMAND USAGE

Multicast Router Discovery

There have been many mechanisms used in the past to identify multicast routers. This has led to interoperability issues between multicast routers and snooping switches from different vendors. In response to this problem, the Multicast Router Discovery (MRD) protocol has been developed for use by IGMP snooping and multicast routing devices. MRD is used to discover which interfaces are attached to multicast routers, allowing IGMP-enabled devices to determine where to send multicast source and group membership messages. (MRD is specified in draft-ietf-magma-mrdisc-07.) Multicast source data and group membership reports must be received by all multicast routers on a segment. Using the group membership protocol query messages to discover multicast routers is insufficient due to query suppression. MRD therefore provides a standardized way to identify multicast routers without relying on any particular multicast routing protocol. Multicast Router Discovery uses the following three message types to discover multicast routers:

- ◆ **Multicast Router Advertisement** – Advertisements are sent by routers to advertise that IP

multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the occurrence of these events:

- Upon the expiration of a periodic (randomized) timer.
- As a part of a router's start up procedure.
- During the restart of a multicast forwarding interface.
- On receipt of a Solicitation message.
- ◆ **Multicast Router Solicitation** – Devices send Solicitation messages in order to solicit Advertisement messages from multicast routers. These messages are used to discover multicast routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an Advertisement.
- ◆ **Multicast Router Termination** – These messages are sent when a router stops IP multicast routing functions on an interface. Termination messages are sent by multicast routers when:
 - Multicast forwarding is disabled on an interface.
 - An interface is administratively disabled.
 - The router is gracefully shut down.

Advertisement and Termination messages are sent to the All-Snoopers multicast address. Solicitation messages are sent to the All-Routers multicast address.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – ID of configured VLANs. (Range: 1-4093)
- ◆ **IGMP Snooping Status** – When enabled, the switch will monitor network traffic on the indicated VLAN interface to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled) When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence. When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.
- ◆ **Version Exclusive** – Discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled) If version exclusive is disabled on a VLAN, then this setting is based on the global setting configured on the Multicast > IGMP Snooping > General page. If it is enabled on a VLAN, then this setting takes precedence over the global setting.
- ◆ **Immediate Leave Status** – Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled) If immediate leave is not used, a multicast router (or querier) will send a group-specific query message when an IGMPv2 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified time out period. Note that this time out is set to Last Member Query Interval * Robustness Variable (fixed at 2) as defined in RFC 2236. If immediate leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping. This

attribute is only effective if IGMP snooping is enabled, and IGMPv2 snooping is used.

◆ **Multicast Router Discovery** – MRD is used to discover which interfaces are attached to multicast routers. (Default: Enabled)

◆ **General Query Suppression** – Suppresses general queries except for ports attached to downstream multicast hosts. (Default: Disabled) By default, general query messages are flooded to all ports, except for the multicast router through which they are received. If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

◆ **Proxy Reporting** – Enables IGMP Snooping with Proxy Reporting. (Default: Based on global setting) When proxy reporting is enabled with this command, the switch performs “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.

◆ **Interface Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2) This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

◆ **Query Interval** – The interval between sending IGMP proxy general queries. (Range: 2-31744 seconds; Default: 125 seconds) An IGMP general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined. This command applies when the switch is serving as the querier, or as a proxy host when IGMP snooping proxy reporting is enabled .

◆ **Query Response Interval** – The maximum time the system waits for a response to proxy general queries. (Range: 10-31744 tenths of a second; Default: 10 seconds) This command applies when the switch is serving as the querier, or as a proxy host when IGMP snooping proxy reporting is enabled .

◆ **Last Member Query Interval** – The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31740 tenths of a second in multiples of 10; Default: 1 second) When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP groupspecific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router. A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more burst traffic. This attribute will take effect only if IGMP snooping proxy reporting is enabled or IGMP querier is enabled .

◆ **Last Member Query Count** – The number of IGMP proxy groupspecific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. (Range: 1-255; Default: 2) This attribute will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled.

◆ **Proxy Query Address** – A static source address for locally generated query and report

messages used by IGMP Proxy Reporting. (Range: Any valid IP unicast address; Default: 0.0.0.0) IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports. Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.

To resolve this problem, the source address in proxied IGMP query messages can be replaced with any valid unicast address (other than the router’s own address).

Rules Used for Proxy Reporting

When IGMP Proxy Reporting is disabled, the switch will use a null IP address for the source of IGMP query and report messages unless a proxy query address has been set. When IGMP Proxy Reporting is enabled, the source address is based on the following criteria:

- If a proxy query address is configured, the switch will use that address as the source IP address in general and group-specific query messages sent to downstream hosts, and in report and leave messages sent upstream from the multicast router port.
- If a proxy query address is not configured, the switch will use the VLAN’s IP address as the IP source address in general and groupspecific query messages sent downstream, and use the source address of the last IGMP message received from a downstream host in report and leave messages sent upstream from the multicast router port.

VLAN Information Switch Management > IGMP Snooping > VLAN Information

IGMP Snooping VLAN List Total: 1

VLAN	IGMP Snooping Status	Immediate Leave Status	Query Interval	Query Response Interval	Last Member Query Interval	Last Member Query Count	Proxy (Query) Address	Proxy Reporting	Multicast Router Discovery	General Query Suppression	Version Exclusive	Interface Version
1	Disabled	Disabled	125	100	10	2	0.0.0.0	Using global status (Disabled)	Disabled	Disabled	Using global status (Disabled)	Using global version (2)

[Configure](#)

VLAN 1

IGMP Snooping Status Enabled

Version Exclusive Using Global Status

Immediate Leave Status Enabled By-Group

Multicast Router Discovery Enabled

General Query Suppression Enabled

Proxy Reporting Using Global Status

Interface Version Using Global Version

Query Interval (2-31744) 125 seconds

Query Response Interval (10-31740) 100 (1/10 seconds, multiple of 10)

Last Member Query Interval (1-31744) 10 (1/10 seconds, multiple of 10)

Last Member Query Count (1-255) 2

Proxy (Query) Address 10.20.30.40

[Apply](#) [Revert](#)

To show the interface settings for IGMP snooping:

VLAN Information Switch Management > IGMP Snooping > VLAN Information

IGMP Snooping VLAN List Total: 1

VLAN	IGMP Snooping Status	Immediate Leave Status	Query Interval	Query Response Interval	Last Member Query Interval	Last Member Query Count	Proxy (Query) Address	Proxy Reporting	Multicast Router Discovery	General Query Suppression	Version Exclusive	Interface Version
1	Enabled	Disabled	125	100	10	2	10.20.30.40	Using global status (Disabled)	Enabled	Disabled	Using global status (Disabled)	Using global version (2)

Configure Interface

Switch Management > IGMP Snooping > Configure Interface page is used to configure an interface to drop IGMP query packets.

PARAMETERS

These parameters are displayed:

◆ **IGMP Query Drop** – Configures an interface to drop any IGMP query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

Configure Interface Stacking Unit: 1

Interface Port Trunk

Port List Total: 50 1 2 3 4 5

Port	IGMP Query Drop	Multicast Data Drop	IGMP Authentication
1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
2	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
4	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
5	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
6	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
7	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
8	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
9	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
10	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled

Forwarding Entry

Switch Management > IGMP Snooping > Forwarding Entry page is used to display the forwarding entries learned through IGMP Snooping.

COMMAND USAGE

To display information about multicast groups, IGMP Snooping must first be enabled on the switch .

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – An interface on the switch that is forwarding traffic to downstream ports for the specified multicast group address.
- ◆ **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
- ◆ **Interface** – A downstream port or trunk that is receiving traffic for the specified multicast group. This field may include both dynamically and statically configured multicast router ports.
- ◆ **Up Time** – Time that this multicast group has been known.
- ◆ **Expire** – Time until this entry expires.
- ◆ **Count** – The number of times this address has been learned by IGMP snooping.

Forwarding Entry Switch Management > IGMP Snooping > Forwarding Entry

IGMP Snooping Forwarding Entry List Total: 5

VLAN	Group Address	Source Address	Interface	Up Time	Expire	Count
<input type="button" value="Clear"/> Click this button to clear all IGMP Snooping dynamic groups.						

Query Statistics

Switch Management > IGMP Snooping > Query Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of IGMP groups active on this interface.

Output Statistics

- ◆ **Report** – The number of IGMP membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

Query Statistics	
Switch Management > IGMP Snooping > Query Statistics	
VLAN	1
Query Statistics	
Other Querier	None
Other Querier Expire	00(m):00(s)
Other Querier Uptime	00(h):00(m):00(s)
Self Querier	None
Self Querier Expire	00(m):00(s)
Self Querier Uptime	00(h):00(m):00(s)
General Query Received	0
General Query Sent	0
Specific Query Received	0
Specific Query Sent	0
Warn Rate Limit	0 sec.
V1 Warning Count	0
V2 Warning Count	0

VLAN Statistics

Switch Management > IGMP Snooping > Vlan Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)

Query Statistics

- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.

◆ **Group** – The number of IGMP groups active on this interface.

Output Statistics

◆ **Report** – The number of IGMP membership reports sent from this interface.

◆ **Leave** – The number of leave messages sent from this interface.

◆ **G Query** – The number of general query messages sent from this interface.

◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

VLAN Statistics Switch Management > IGMP Snooping > VLAN Statistics

VLAN 1 ▾

Input Statistics

Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	0
Leave	0
G Query	0
G(-S)-S Query	0

Clear Refresh

Port Statistics

Switch Management > IGMP Snooping > Port Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

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

Query Statistics

◆ **Querier IP Address** – The IP address of the querier on this interface.

◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.

◆ **General Query Received** – The number of general queries received on this interface.

◆ **General Query Sent** – The number of general queries sent from this interface.

◆ **Specific Query Received** – The number of specific queries received on this interface.

◆ **Specific Query Sent** – The number of specific queries sent from this interface.

◆ **Number of Reports Sent** – The number of reports sent from this interface.

◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

◆ **Report** – The number of IGMP membership reports received on this interface.

◆ **Leave** – The number of leave messages received on this interface.

◆ **G Query** – The number of general query messages received on this interface.

◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.

◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group

report received.

- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of IGMP groups active on this interface.

Output Statistics

- ◆ **Report** – The number of IGMP membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

Port Statistics Switch Management > IGMP Snooping > Port Statistics

Port:

Input Statistics		Drop	
Report	0	Join Success	0
Leave	0	Group	0
G Query	0		
G(-S)-S Query	0		
Output Statistics			
Report	0		
Leave	0		
G Query	0		
G(-S)-S Query	0		

Trunk Statics

Switch Management > IGMP Snooping > Trunk Statistics page is used to display IGMP snooping protocol-related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

- ◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.

◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.

◆ **Join Success** – The number of times a multicast group was successfully joined.

◆ **Group** – The number of IGMP groups active on this interface.

Output Statistics

◆ **Report** – The number of IGMP membership reports sent from this interface.

◆ **Leave** – The number of leave messages sent from this interface.

◆ **G Query** – The number of general query messages sent from this interface.

◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

Trunk Statistics Switch Management > IGMP Snooping > Trunk Statistics

Trunk: 1

Input Statistics			
Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		
Output Statistics			
Report	0	Drop	0
Leave	0	Group	0
G Query	0		
G(-S)-S Query	0		

Clear Refresh

IGMP Filtering and Throttling

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join. IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more addresses, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped. IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Filter General

Switch Management > IGMP Filtering and Throttling > Filter General page is used to enable

IGMP filtering and throttling globally on the switch.

PARAMETERS

These parameters are displayed:

◆ **IGMP Filter Status** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)

Filter General Switch Management > IGMP Filtering and Throttling > Filter General

IGMP Filter Status Enabled

Apply Revert

Filter Profile

Switch Management > IGMP Filtering and Throttling > Filter Profile page is used to create an IGMP profile and set its access mode. Then use the (Add Multicast Group Range) page to configure the multicast groups to filter.

COMMAND USAGE

Specify a range of multicast groups by entering a start and end IP address; or specify a single multicast group by entering the same IP address for the start and end of the range.

PARAMETERS

These parameters are displayed:

Add

◆ **Profile ID** – Creates an IGMP profile. (Range: 1-4294967295)

◆ **Access Mode** – Sets the access mode of the profile; either permit or deny. (Default: Deny)

When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when the multicast group is not in the controlled range.

Add Multicast Group Range

◆ **Profile ID** – Selects an IGMP profile to configure.

◆ **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.

◆ **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

Filter Profile Switch Management > IGMP Filtering and Throttling > Filter Profile

IGMP Snooping Filter Profile List Total: 2

	Profile ID	Action Mode
<input type="checkbox"/>	1	Deny
<input type="checkbox"/>	2	Deny

New Delete Revert

Profile ID (1-4294967295)

Access Mode

Apply Revert

To show the IGMP filter profiles:

1. Click Switch Management > IGMP Filtering and Throttling > Filter Profile.

Filter Profile Switch Management > IGMP Filtering and Throttling > Filter Profile

IGMP Snooping Filter Profile List Total: 2

<input type="checkbox"/>	Profile ID	Action Mode
<input type="checkbox"/>	1	Deny
<input type="checkbox"/>	2	Deny

New Delete Revert

Filter Range

Switch Management > IGMP Filtering and Throttling > Filter Range page is used to create an IGMP range and set its access mode. Then use the (new Multicast Group Range) page to configure the multicast groups to filter.

COMMAND USAGE

Specify a range of multicast groups by entering a start and end IP address; or specify a single multicast group by entering the same IP address for the start and end of the range.

PARAMETERS

These parameters are displayed:

new

◆ **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.

◆ **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

Filter Range Switch Management > IGMP Filtering and Throttling > Filter Range

Profile ID

Multicast IP Address Range List Total: 2

<input type="checkbox"/>	Start Multicast IP Address	End Multicast IP Address
<input type="checkbox"/>	224.1.1.1	224.1.1.6
<input type="checkbox"/>	224.1.1.10	224.1.1.16

New Delete Revert

Profile ID

Start Multicast IP Address

End Multicast IP Address

Apply Revert

To show the multicast groups configured for an IGMP filter Range:

Filter Range Switch Management > IGMP Filtering and Throttling > Filter Range

Profile ID

Multicast IP Address Range List Total: 2

<input type="checkbox"/>	Start Multicast IP Address	End Multicast IP Address
<input type="checkbox"/>	224.1.1.1	224.1.1.6
<input type="checkbox"/>	224.1.1.10	224.1.1.16

New Delete Revert

Configure Filter Interface

Switch Management > IGMP Filtering and Throttling > Configure Filter Interface page is used to assign an IGMP filter profile to interfaces on the switch, or to throttle multicast traffic by

limiting the maximum number of multicast groups an interface can join at the same time.

COMMAND USAGE

◆ **IGMP throttling** sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

PARAMETERS

These parameters are displayed:

◆ **Interface** – Port or trunk identifier.

An IGMP profile or throttling setting can be applied to a port or trunk. When ports are configured as trunk members, the trunk uses the settings applied to the first port member in the trunk.

◆ **Profile ID** – Selects an existing profile to assign to an interface.

◆ **Max Multicast Groups** – Sets the maximum number of multicast groups an interface can join at the same time. (Range: 1-255; Default: 255)

◆ **Current Multicast Groups** – Displays the current multicast groups the interface has joined.

◆ **Throttling Action Mode** – Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny)

■ **Deny** - The new multicast group join report is dropped.

■ **Replace** - The new multicast group replaces an existing group.

◆ **Throttling Status** – Indicates if the throttling action has been implemented on the interface. (Options: True or False)

Configure Filter Interface Stacking Unit:

Switch Management > IGMP Filtering and Throttling > Configure Filter Interface

IGMP Filter and Throttling Port List Total: 50

Port	Profile ID	Max Multicast Groups (1-255)	Current Multicast Groups	Throttling Action Mode	Throttling Status
1	(none)	255	0	Deny	False
2	(none)	255	0	Deny	False
3	(none)	255	0	Deny	False
4	(none)	255	0	Deny	False
5	(none)	255	0	Deny	False
6	(none)	255	0	Deny	False
7	(none)	255	0	Deny	False
8	(none)	255	0	Deny	False
9	(none)	255	0	Deny	False
10	(none)	255	0	Deny	False

Apply Revert

MLD Snooping

Multicast Listener Discovery (MLD) snooping operates on IPv6 traffic and performs a similar function to IGMP snooping for IPv4. That is, MLD snooping dynamically configures switch ports to limit IPv6 multicast traffic so that it is forwarded only to ports with users that want to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs.

There are two versions of the MLD protocol, version 1 and version 2. MLDv1 control packets include Listener Query, Listener Report, and Listener Done messages (equivalent to IGMPv2 query, report, and leave messages). MLDv2 control packets include MLDv2 query and report

messages, as well as MLDv1 report and done messages. Remember that IGMP Snooping and MLD Snooping are independent functions, and can therefore both function at the same time.

General

Switch Management > MLD Snooping > General page is used to configure the switch to forward multicast traffic intelligently. Based on the MLD query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

- ◆ **MLD Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. (Default: Disabled)
- ◆ **Querier Status** – When enabled, the switch can serve as the querier for MLDv2 snooping if elected. The querier is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled) An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses this IPv6 address as the query source address. The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.
- ◆ **Robustness** – MLD Snooping robustness variable. A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report. (Range: 2-10 Default: 2)
- ◆ **Query Interval** – The interval between sending MLD general queries. (Range: 60-125 seconds; Default: 125 seconds) This attribute applies when the switch is serving as the querier. An MLD general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.
- ◆ **Query Max Response Time** – The maximum response time advertised in MLD general queries. (Range: 5-25 seconds; Default: 10 seconds) This attribute controls how long the host has to respond to an MLD Query message before the switch deletes the group if it is the last member.
- ◆ **Router Port Expiry Time** – The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired. (Range: 300-500 seconds; Default: 300 seconds)
- ◆ **MLD Snooping Version** – The protocol version used for compatibility with other devices on the network. This is the MLD version the switch uses to send snooping reports. (Range: 1-2; Default: 2)
- ◆ **Unknown Multicast Mode** – The action for dealing with unknown multicast packets. Options include:
 - **Flood** – Floods any received IPv6 multicast packets that have not been requested by a host to all ports in the VLAN.
 - **To Router Port** – Forwards any received IPv6 multicast packets that have not been requested by a host to ports that are connected to a detected multicast router. (This is the default action.)

General Switch Management > MLD Snooping > General

MLD Snooping Status	<input checked="" type="checkbox"/> Enabled
Querier Status	<input checked="" type="checkbox"/> Enabled
Robustness (2-10)	<input type="text" value="2"/>
Query Interval (60-125)	<input type="text" value="125"/> seconds
Query Max Response Time (5-25)	<input type="text" value="10"/> seconds
Router Port Expiry Time (300-500)	<input type="text" value="300"/> seconds
MLD Snooping Version (1-2)	<input type="text" value="2"/>
Unknown Multicast Mode	To Router Port ▾

Immediate Leave Status

Switch Management > MLD Snooping > Immediate Leave Status page is used to configure Immediate Leave status for a VLAN.

◆ **VLAN** – A VLAN identification number. (Range: 1-4094)

◆ **Immediate Leave Status** – Immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled) If MLD immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.

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

Immediate Leave Status Switch Management > MLD Snooping > Immediate Leave Status

VLAN	<input type="text" value="1"/> ▾
Immediate Leave Status	<input checked="" type="checkbox"/> Enabled

Current Multicast Router

Switch Management > MLD Snooping > Current Multicast Router page is used to statically show an interface to an IPv6 multicast router/switch.

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

Command Usage

MLD Snooping must be enabled globally on the switch before a multicast router port can take effect.

- ◆ **VLAN** – Selects the VLAN which is to propagate all IPv6 multicast traffic coming from the attached multicast router. (Range: 1-4094)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.

Current Multicast Router Switch Management > MLD Snooping > Current Multicast Router

VLAN

Multicast Router Interface Information Total: 1

Interface	Type
Unit 1 / Port 3	Static

Static Multicast Router

Switch Management> MLD Snooping> Static Multicast Router page is used to statically add an interface to an IPv6 multicast router/switch. Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

MLD Snooping must be enabled globally on the switch before a multicast router port can take effect.

- ◆ **VLAN** – Selects the VLAN which is to propagate all IPv6 multicast traffic coming from the attached multicast router. (Range: 1-4094)
- ◆ **Interface** – Activates the Port or Trunk scroll down list.

Static Multicast Router Switch Management > MLD Snooping > Static Multicast Router

VLAN

Static Multicast Router Interface List Total: 1

Interface
Unit 1 / port 3

VLAN

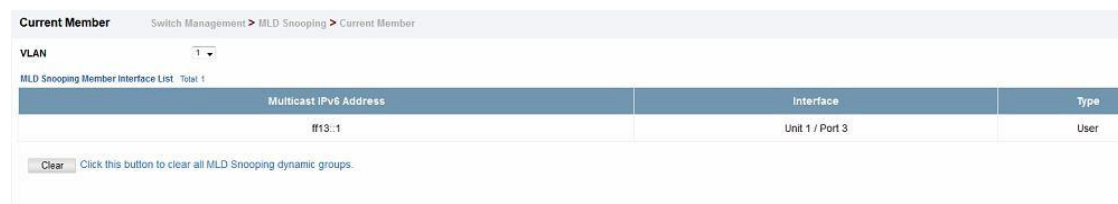
Interface Port 3 Trunk

Current Member

Switch Management > MLD Snooping > Current Member page is used to statically show an IPv6 multicast service to an interface. Multicast filtering can be dynamically configured using MLD snooping and query messages. However, for certain applications that require tighter control, it may be necessary to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Command Usage

- ◆ Static multicast addresses are never aged out.
- ◆ When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.
- ◆ **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)
- ◆ **Multicast IPv6 Address** – The IP address for a specific multicast service.
- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Trunk** – Specifies the interface assigned to a multicast group.
- ◆ **Type (Show Current Member)** – Shows if this multicast stream was statically configured by the user, discovered by MLD Snooping, or is a data stream to which no other ports are subscribing (i.e., the stream is flooded onto VLAN instead of being trapped to the CPU for processing, or is being processed by MVR6).



Multicast IPv6 Address	Interface	Type
ff13::1	Unit 1 / Port 3	User

Static Member

Switch Management > MLD Snooping > Static Member page is used to statically add an IPv6 multicast service to an interface. Multicast filtering can be dynamically configured using MLD snooping and query messages. However, for certain applications that require tighter control, it may be necessary to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Command Usage

- ◆ Static multicast addresses are never aged out.
- ◆ When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Parameters

These parameters are displayed:

- ◆ **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)
- ◆ **Multicast IPv6 Address** – The IP address for a specific multicast service.

- ◆ **Interface** – Activates the Port or Trunk scroll down list.
- ◆ **Port or Trunk** – Specifies the interface assigned to a multicast group.
- ◆ **Type (Show Current Member)** – Shows if this multicast stream was statically configured by the user, discovered by MLD Snooping, or is a data stream to which no other ports are subscribing (i.e., the stream is flooded onto VLAN instead of being trapped to the CPU for processing, or is being processed by MVR6).

Static Member Stacking Unit: 1

VLAN: 1

MLD Member Interface List Total: 1

	Multicast IPv6 Address	Interface
<input type="checkbox"/>	ff13::1	Unit 1 / port 3

New Delete Revert

VLAN: 1

Multicast IPv6 Address:

Interface: Port 3 Trunk 1

Apply Revert

Group Information

Switch Management > MLD Snooping > Group Information page is used to display and set known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.

Parameters

These parameters are displayed:

- ◆ **VLAN** – VLAN identifier. (Range: 1-4094)
- ◆ **Interface** – Port or trunk identifier.
- ◆ **Group Address** – The IP address for a specific multicast service.
- ◆ **Type** – The means by which each group was learned – MLD Snooping or MulticastData.
- ◆ **Filter Mode** – The filter mode is used to summarize the total listening state of a multicast address to a minimum set such that all nodes' listening states are respected. In Include mode, the router only uses the request list, indicating that the reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the hosts' source-list. In Exclude mode, the router uses both the request list and exclude list, indicating that the reception of packets sent to the given multicast address is requested from all IP source addresses, except for those listed in the exclude source-list and for any other sources where the source timer status has expired.
- ◆ **Filter Timer Elapse** – The Filter timer is only used when a specific multicast address is in Exclude mode. It represents the time for the multicast address filter mode to expire and change to Include mode.
- ◆ **Request List** – Sources included on the router's request list.
- ◆ **Exclude List** – Sources included on the router's exclude list.

Group Information Switch Management > MLD Snooping > Group Information

VLAN:

Interface: Port Trunk

Group Address:

Type: Static

Filter Mode: Include

Include List Total: 0

IPv6 Address

Statistics

Switch Management > MLD Snooping > Statistics pages is used to display MLD Snooping protocol-related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface.

Output Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.

- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface.

To display statistics for MLD Snooping input:

Statistics Switch Management > MLD Snooping > Statistics

Type Input Output Query Summary Clear

Input Statistics Total: 54

Interface	Report	Leave	G Query	G(-S)-S Query	Drop	Join Success	Group
Eth 1/3	0	0	0	0	0	0	1
Eth 1/4	0	0	0	0	0	0	0
Eth 1/5	0	0	0	0	0	0	0
Eth 1/6	0	0	0	0	0	0	0
Eth 1/7	0	0	0	0	0	0	0
Eth 1/8	0	0	0	0	0	0	0
Eth 1/9	0	0	0	0	0	0	0
Eth 1/10	0	0	0	0	0	0	0
Eth 1/11	0	0	0	0	0	0	0
Eth 1/12	0	0	0	0	0	0	0
Eth 1/13	0	0	0	0	0	0	0
Eth 1/14	0	0	0	0	0	0	0

To display statistics for MLD Snooping output:

Statistics Switch Management > MLD Snooping > Statistics

Type Input Output Query Summary Clear

Output Statistics Total: 54

Interface	Report	Leave	G Query	G(-S)-S Query	Drop	Group
Eth 1/3	0	0	20	0	0	1
Eth 1/4	0	0	20	0	0	0
Eth 1/5	0	0	20	0	0	0
Eth 1/6	0	0	20	0	0	0
Eth 1/7	0	0	20	0	0	0
Eth 1/8	0	0	20	0	0	0
Eth 1/9	0	0	20	0	0	0
Eth 1/10	0	0	20	0	0	0
Eth 1/11	0	0	20	0	0	0
Eth 1/12	0	0	20	0	0	0
Eth 1/13	0	0	20	0	0	0
Eth 1/14	0	0	20	0	0	0

To display statistics for MLD Snooping Query:

Statistics Switch Management > MLD Snooping > Statistics

Type Input Output Query Summary Clear

VLAN

Query Statistics

Other Querier Address	None
Other Querier Expire	0(m):0(s)
Other Querier Uptime	0(h):0(m):0(s)
Self Querier Address	fe80::200:22ff:fe00:402
Self Querier Expire Time	1(m):57(s)
Self Querier Uptime	0(h):40(m):13(s)
General Query Received	0
General Query Sent	21
Specific Query Received	0
Specific Query Sent	0

To display statistics for MLD Snooping Summary:

Type Input Output Query Summary Clear

Interface VLAN

Unit / Port

Trunk

Summary Statistics

Number of Groups	1
Querier	
Other Querier	None
Other Uptime	0(h):0(m):0(s)
Other Expire	0(m):0(s)
Self Addr	fe80::200:22ff:fe00:402
Self Expire	0(m):48(s)
Self Uptime	0(h):43(m):29(s)
Transmit	
General	22
Report & Leave	
Host Addr	fe80::200:22ff:fe00:402
Unsolicit Expire	0 sec
Transmit Report	
	0

To display statistics for MLD Snooping Summary:

Statistics Switch Management > MLD Snooping > Statistics

Type Input Output Query Summary Clear

Interface All

VLAN

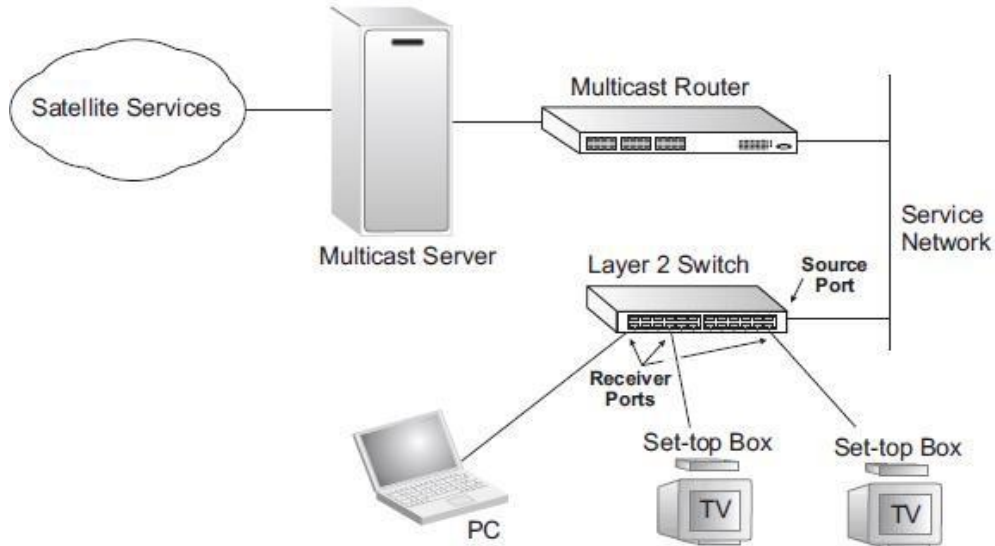
Unit / Port

Trunk

MVR for IPv4

Multicast VLAN Registration (MVR) is a protocol that controls access to a single network-wide VLAN most commonly used for transmitting multicast traffic (such as television channels or video-on-demand) across a service provider’s network. Any multicast traffic entering an MVR VLAN is sent to all attached subscribers. This protocol can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. This makes it possible to support common multicast services over a wide part of the network without having to use any multicast

routing protocol. MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).



Configure Global

Switch Management > MVR For IPv4 > Configure Global page is used to configure proxy switching and the robustness variable.

PARAMETERS

These parameters are displayed:

- ◆ **Proxy Switching** – Configures MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. (Default: Enabled)
- When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
- Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
- When the source port receives report and leave messages, it only forwards them to other source ports.
- When receiver ports receive any query messages, they are dropped.
- When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.

- When MVR proxy switching is disabled:
- Any membership reports received from receiver/source ports are forwarded to all source ports.
- When a source port receives a query message, it will be forwarded to all downstream receiver ports.
- When a receiver port receives a query message, it will be dropped.
- ◆ **Robustness Value** – Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. (Range: 1-255; Default: 2)
- This parameter is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- This parameter only takes effect when MVR proxy switching is enabled.
- ◆ **Proxy Query Interval** – Configures the interval at which the receiver port sends out general queries. (Range: 2-31744 seconds; Default: 125 seconds)
- This parameter sets the general query interval at which active receiver ports send out general queries.
- This interval is only effective when proxy switching is enabled.
- ◆ **Source Port Mode** – Configures the switch to forward any multicast streams within the parameters set by a profile, or to only forward multicast streams which the source port has dynamically joined.
- **Always Forward** – By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.
- **Dynamic** – When dynamic mode is enabled, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

Configure Global	
Switch Management > MVR For IPv4 > Configure Global	
Proxy Switching	<input checked="" type="checkbox"/> Enabled
Robustness Value (1-255)	<input type="text" value="2"/>
Proxy Query Interval (2-31744)	<input type="text" value="125"/> sec
Source Port Mode	Always Forward ▾
<input type="button" value="Apply"/> <input type="button" value="Revert"/>	

Configure Domain

Switch Management > MVR For IPv4 > Configure Domain page is used to enable MVR globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **MVR Status** – When MVR is enabled on the switch, any multicast data associated with an MVR group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)
- ◆ **MVR VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR. MVR source ports should be configured as members of the MVR VLAN (see "Adding Static Members to VLANs"), but MVR receiver ports should not be manually configured as members of this VLAN. (Default: 1)
- ◆ **MVR Running Status** – Indicates whether or not all necessary conditions in the MVR environment are satisfied. Running status is Active as long as MVR is enabled, the specified MVR VLAN exists, and a source port with a valid link has been configured (see "Configuring MVR Interface Status").
- ◆ **MVR Current Learned Groups** – The number of MVR groups currently assigned to this domain.
- ◆ **Forwarding Priority** – The CoS priority assigned to all multicast traffic forwarded into this domain. (Range: 0-6, where 6 is the highest priority) This parameter can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.
- ◆ **Upstream Source IP** – The source IP address assigned to all MVR control packets sent upstream on the specified domain. By default, all MVR reports sent upstream use a null source IP address.

Configure Domain Switch Management > MVR For IPv4 > Configure Domain

Domain ID	1
MVR Status	<input type="checkbox"/> Enabled
MVR VLAN	1
MVR Running Status	Inactive
MVR Current Learned Groups	0
Forwarding Priority (0-7)	<input type="checkbox"/> <input style="width: 40px;" type="text"/>
Upstream Source IP	<input style="width: 150px;" type="text" value="0.0.0.0"/>

Show Configure Profile

Switch Management > MVR For IPv4 > Show Configure Profile pages is used to display the multicast group address for required services to one or more MVR domains.

COMMAND USAGE

- ◆ Use the Show Configure Profile page to statically show all multicast group addresses that will join the MVR VLAN. Any multicast data associated with an MVR group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
- ◆ The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams.

MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

◆ IGMP snooping and MVR share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

PARAMETERS

These parameters are displayed:

Configure Profile

◆ **Profile Name** – The name of a profile containing one or more MVR group addresses.

(Range: 1-21 characters)

◆ **Start IP Address** – Starting IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

◆ **End IP Address** – Ending IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Associate Profile



	Profile Name	Start IP Address - End IP Address
<input type="checkbox"/>	profile1	224.1.1.1 - 224.1.1.6
<input type="checkbox"/>	profile2	224.1.2.10 - 224.1.2.100

Add Configure Profile

Switch Management > MVR For IPv4 > Add Configure Profile page is used to assign the multicast group address for required services to one or more MVR domains.

COMMAND USAGE

◆ Use the Add Configure Profile page to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated with an MVR group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.

◆ The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

◆ IGMP snooping and MVR share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

PARAMETERS

These parameters are displayed:

Configure Profile

◆ **Profile Name** – The name of a profile containing one or more MVR group addresses.

(Range: 1-21 characters)

◆ **Start IP Address** – Starting IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

◆ **End IP Address** – Ending IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Associate Profile

(Range: 1-21 characters)

Add Configure Profile Switch Management > MVR For IPv4 > Add Configure Profile

Profile Name

Start IP Address

End IP Address

Add Associate Profile Switch Management > MVR For IPv4 > Add Associate Profile

Domain ID

Profile Name

Show Associate Profile

Switch Management > MVR For IPv4 > Show Associate Profile pages is used to show the multicast group address for required services to one or more MVR domains.

COMMAND USAGE

- ◆ Use the Show Associate Profile page to statically show all multicast group addresses that will join the MVR VLAN. Any multicast data associated with an MVR group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
- ◆ The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- ◆ IGMP snooping and MVR share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

PARAMETERS

These parameters are displayed:

Configure Profile

- ◆ **Profile Name** – The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
- ◆ **Start IP Address** – Starting IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- ◆ **End IP Address** – Ending IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Associate Profile

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)

To show the MVR group address profiles assigned to a domain:

Show Associate Profile Switch Management > MVR For IPv4 > Show Associate Profile

Domain ID

Domain Associated Profile List Total: 2

<input type="checkbox"/>	Profile Name	Start IP Address	End IP Address
<input type="checkbox"/>	profile1	224.1.1.1	224.1.1.6
<input type="checkbox"/>	profile2	224.1.2.10	224.1.2.100

Add Associate Profile

Switch Management > MVR For IPv4 > Add Associate Profile page is used to assign the multicast group address for required services to one or more MVR domains.

COMMAND USAGE

- ◆ Use the Add Associate Profile page to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated with an MVR group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
- ◆ The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- ◆ IGMP snooping and MVR share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

PARAMETERS

These parameters are displayed:

Associate Profile

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-21 characters)

Add Associate Profile Switch Management > MVR For IPv4 > Add Associate Profile

Domain ID

Profile Name

Configure Interface

Switch Management > MVR For IPv4 > Configure Interface page is used to configure each interface that participates in the MVR protocol as a source port or receiver port. If you are sure that only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

COMMAND USAGE

- ◆ A port configured as an MVR receiver or source port can join or leave multicast groups

configured under MVR. However, note that these ports can also use IGMP snooping to join or leave any other multicast groups using the standard rules for multicast filtering.

- ◆ Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. MVR allows a receiver port to dynamically join or leave multicast groups within an MVR VLAN. Multicast groups can also be statically assigned to a receiver port. Receiver ports should not be statically configured as a member of the MVR VLAN. If so configured, its MVR status will be inactive. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode.

- ◆ One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for configured MVR groups or for groups which have been statically assigned. All source ports must belong to the MVR VLAN. Subscribers should not be directly connected to source ports.

- ◆ Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a query message to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.

- Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface.

- Immediate leave does not apply to multicast groups which have been statically assigned to a port.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)

- ◆ **Port/Trunk** – Interface identifier.

- ◆ **Type** – The following interface types are supported:

- **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR VLAN. Note that the source port must be manually configured as a member of the MVR VLAN.

- **Receiver** – A subscriber port that can receive multicast data sent through the MVR VLAN. Any port configured as an receiver port will be dynamically added to the MVR VLAN when it forwards an IGMP report or join message from an attached host requesting any of the designated multicast services supported by the MVR VLAN. Just remember that only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned.

- **Non-MVR** – An interface that does not participate in the MVR VLAN. (This is the default type.)

- ◆ **Forwarding Status** – Shows if MVR traffic is being forwarded or discarded.

- ◆ **MVR Status** – Shows the MVR status. MVR status for source ports is “Active” if MVR is globally enabled on the switch. MVR status for receiver ports is “Active” only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.

- ◆ **Immediate Leave** – Configures the switch to immediately remove an interface from a

multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR receiver.)

Configure Interface Switch Management > MVR For IPv4 > Configure Interface Stacking Unit: 1

uomain id 1

Interface Port Trunk

Port List Total: 59

Port	Type	Forwarding Status	MVR Status	Immediate Leave
1	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
2	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
3	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
4	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
5	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
6	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
7	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
8	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
9	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group
10	Non-MVR	Discarding	Inactive	<input type="checkbox"/> By-Group

Show Static Group Member

Switch Management > MVR For IPv4 > Show Static Group Member page is used to statically show multicast groups for a port or trunk which will receive long-term multicast streams associated with a stable set of hosts.

COMMAND USAGE

- ◆ Multicast groups can be statically assigned to a receiver port using this configuration page.
- ◆ The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- ◆ Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned.
- ◆ The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Interface** – Port or trunk identifier.
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Group IP Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR group range configured on the Configure General page.

Show Static Group Member Switch Management > MVR For IPv4 > Show Static Group Member

Domain ID

Interface Port Trunk

MVR Static Group Member List Total: 1

VLAN	Group IP Address
1	224.1.1.1

Add Static Group Member

Switch Management > MVR For IPv4 > Add Static Group Member page is used to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

COMMAND USAGE

- ◆ Multicast groups can be statically assigned to a receiver port using this configuration page.
- ◆ The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- ◆ Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned.
- ◆ The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Interface** – Port or trunk identifier.
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Group IP Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR group range configured on the Configure General page.



Show Member

Switch Management > MVR For IPv4 > Show Member page is used to show the multicast groups either statically or dynamically assigned to the MVR receiver groups on each interface.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Group IP Address** – Multicast groups assigned to the MVR VLAN.
- ◆ **VLAN** – The VLAN through which the service is received. Note that this may be different from the MVR VLAN if the group address has been statically assigned.
- ◆ **Port** – Shows the interfaces with subscribers for multicast services provided through the MVR VLAN.
- ◆ **Up Time** – Time this service has been forwarded to attached clients.
- ◆ **Expire** – Time before this entry expires if no membership report is received from currently active or new clients.

◆ **Count** – The number of multicast services currently being forwarded from the MVR VLAN.

Switch Management > MVR For IPv4 > Show Member

Domain ID: 1

MVR Member List Total: 3

Group IP Address	VLAN	Port	Up Time	Expire	Count
224.1.1.1	2		00:00:03:12		2 (Port)
	2	Unit 1 / Port 25 (Source)			
	1	Unit 1 / Port 26 (Receiver)	00:00:03:12		0 (Host)

Clear MVR group

Show Query Statistics

Switch Management > MVR For IPv4 > Show Query Statistics page is used to display MVR protocol related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface.

Output Statistics

- ◆ **Report** – The number of IGMP membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.

◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

Switch Management > MVR For IPv4 > Show Query Statistics

Domain ID: 1

Query Statistics

Querier IP Address	None
Querier Expire Time	00(h):01(m):26(s)
General Query Received	0
General Query Sent	2
Specific Query Received	0
Specific Query Sent	0
Number of Reports Sent	1
Number of Leaves Sent	0

Clear All Click this button to clear all MVR statistics of the domain.

Refresh

Show VLAN Statistics

Switch Management > MVR For IPv4 > Show VLAN Statistics page is used to display MVR protocol related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.

◆ **Group** – The number of MVR groups active on this interface.

Output Statistics

◆ **Report** – The number of IGMP membership reports sent from this interface.

◆ **Leave** – The number of leave messages sent from this interface.

◆ **G Query** – The number of general query messages sent from this interface.

◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

Show VLAN Statistics			
Switch Management > MVR For IPv4 > Show VLAN Statistics			
Domain ID	1		
VLAN	2		
Input Statistics			
Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	1
G(-S)-S Query	0		
Output Statistics			
Report	1		
Leave	0		
G Query	2		
G(-S)-S Query	0		
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>			

Show Port Statistics

Switch Management > MVR For IPv4 > Show Port Statistics page is used to display MVR protocol related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

◆ **Domain ID** – An independent multicast domain. (Range: 1-5)

◆ **VLAN** – VLAN identifier. (Range: 1-4093)

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

◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

◆ **Querier IP Address** – The IP address of the querier on this interface.

◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.

◆ **General Query Received** – The number of general queries received on this interface.

◆ **General Query Sent** – The number of general queries sent from this interface.

◆ **Specific Query Received** – The number of specific queries received on this interface.

◆ **Specific Query Sent** – The number of specific queries sent from this interface.

◆ **Number of Reports Sent** – The number of reports sent from this interface.

◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

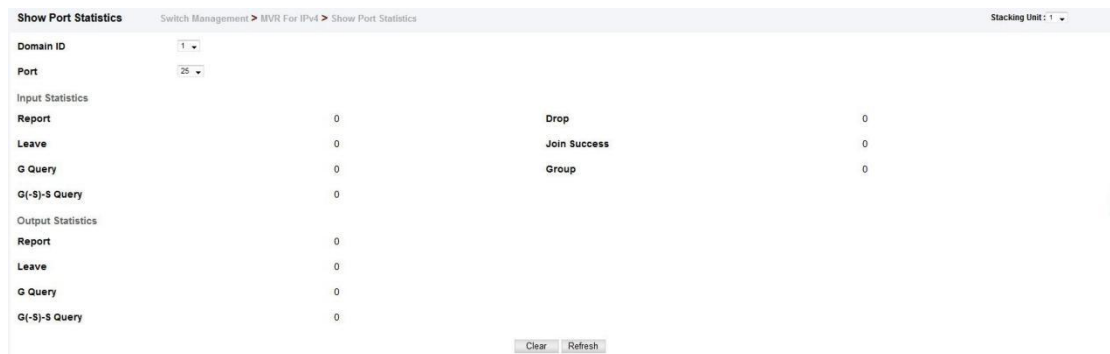
Input Statistics

◆ **Report** – The number of IGMP membership reports received on this interface.

- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface.

Output Statistics

- ◆ **Report** – The number of IGMP membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.



Show Trunk Statistics

Switch Management > MVR For IPv4 > Show Trunk Statistics page is used to display MVR protocol-related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

- ◆ **Querier IP Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of IGMP membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR groups active on this interface.

Output Statistics

- ◆ **Report** – The number of IGMP membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

Show Trunk Statistics			
Switch Management > MVR For IPv4 > Show Trunk Statistics			
Domain ID	1		
Trunk	1		
Input Statistics			
Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		
Output Statistics			
Report	2		
Leave	0		
G Query	0		
G(-S)-S Query	0		
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>			

MVR For IPv6

MVR6 functions in a manner similar to that described for MRV

Configure Global

Switch Management > MVR For IPv6 > Configure Global page is used to configure proxy switching and the robustness variable.

PARAMETERS

These parameters are displayed:

- ◆ **Proxy Switching** – Configures MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. (Default: Enabled)

- When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
- Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
- When the source port receives report and leave messages, it only forwards them to other source ports.
- When receiver ports receive any query messages, they are dropped.
- When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
- When MVR proxy switching is disabled:
 - Any membership reports received from receiver/source ports are forwarded to all source ports.
 - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
 - When a receiver port receives a query message, it will be dropped.
- ◆ **Robustness Value** – Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. (Range: 1-10; Default: 2)
 - This parameter is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
 - This parameter only takes effect when MVR6 proxy switching is enabled.
- ◆ **Proxy Query Interval** – Configures the interval at which the receiver port sends out general queries. (Range: 2-31744 seconds; Default: 125 seconds)
 - This parameter sets the general query interval at which active receiver ports send out general queries.
 - This interval is only effective when proxy switching is enabled.
- ◆ **Source Port Mode** – Configures the switch to forward any multicast streams within the parameters set by a profile, or to only forward multicast streams which the source port has dynamically joined.
 - **Always Forward** – By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.
 - **Dynamic** – When dynamic mode is enabled, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

Configure Global Switch Management > MVR For IPv6 > Configure Global

Proxy Switching Enabled

Robustness Value (1-10)

Proxy Query Interval (2-31744) sec

Source Port Mode

Configure Domain

Switch Management > MVR For IPv6 > Configure Domain page is used to enable MVR6 globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID**— An independent multicast domain. (Range: 1-5)
- ◆ **MVR6 Status** – When MVR6 is enabled on the switch, any multicast data associated with an MVR6 group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)
- ◆ **MVR6 VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR6. MVR6 source ports should be configured as members of the MVR6 VLAN, but MVR6 receiver ports should not be manually configured as members of this VLAN. (Default: 1)
- ◆ **MVR6 Running Status** – Indicates whether or not all necessary conditions in the MVR6 environment are satisfied. Running status is Active as long as MVR6 is enabled, the specified MVR6 VLAN exists, and a source port with a valid link has been configured.
- ◆ **MVR6 Current Learned Groups** – The number of MVR6 groups currently assigned to this domain.
- ◆ **Upstream Source IPv6** – The source IPv6 address assigned to all MVR6 control packets sent upstream on the specified domain. This parameter must be a full IPv6 address including the network prefix and host address bits. By default, all MVR6 reports sent upstream use a null source IP address.

All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

WEB INTERFACE

To configure settings for an MVR6 domain:

1. Click Switch Management > MVR For IPv6 > Configure Domain.
2. Select a domain from the scroll-down list.
3. Enable MVR6 for the selected domain, select the MVR6 VLAN, set the forwarding priority to be assigned to all ingress multicast traffic, and set the source IP address for all control packets sent upstream as required.

4. Click Apply.

Configure Domain Switch Management > MVR For IPv6 > Configure Domain

Domain ID	1
MVR6 Status	<input checked="" type="checkbox"/> Enabled
MVR6 VLAN	2
MVR6 Running Status	Inactive
MVR6 Current Learned Groups	0
Forwarding Priority (0-7)	<input type="text" value=""/>
Upstream Source IPv6	<input type="text" value="::"/>

Show Configure Profile

Switch Management > MVR For IPv6 > Show Configure Profile page is used to assign the multicast group address for required services to one or more MVR6 domains.

COMMAND USAGE

◆ Use the Configure Profile page to statically configure all multicast group addresses that will join the MVR6 VLAN. Any multicast data associated with an MVR6 group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.

◆ All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

◆ The MVR6 group address range assigned to a profile cannot overlap with the group address range of any other profile.

◆ MVR6 domains can be associated with more than one MVR6 profile. But since MVR6 domains cannot share the group range, an MVR6 profile can only be associated with one MVR6 domain.

PARAMETERS

These parameters are displayed:

Configure Profile

◆ **Profile Name** – The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)

◆ **Start IPv6 Address** – Starting IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

◆ **End IPv6 Address** – Ending IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

Associate Profile

◆ **Domain ID** – An independent multicast domain. (Range: 1-5)

◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-20 characters)

Switch Management > MVR For IPv6 > Show Configure Profile

MVR6 Profile List Total: 2

<input type="checkbox"/>	Profile Name	Start IPv6 Address	End IPv6 Address
<input type="checkbox"/>	profile1	ff13::1	ff13::9
<input type="checkbox"/>	profile2	ff13::12	ff13::19

Add Configure Profile

Switch Management > MVR For IPv6 > Add Configure Profile page is used to assign the multicast group address for required services to one or more MVR6 domains.

COMMAND USAGE

- ◆ Use the Configure Profile page to statically configure all multicast group addresses that will join the MVR6 VLAN. Any multicast data associated with an MVR6 group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
- ◆ All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)
- ◆ The MVR6 group address range assigned to a profile cannot overlap with the group address range of any other profile.
- ◆ MVR6 domains can be associated with more than one MVR6 profile. But since MVR6 domains cannot share the group range, an MVR6 profile can only be associated with one MVR6 domain.

PARAMETERS

These parameters are displayed:

Configure Profile

- ◆ **Profile Name** – The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)
- ◆ **Start IPv6 Address** – Starting IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.
- ◆ **End IPv6 Address** – Ending IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

Associate Profile

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-20 characters)

Switch Management > MVR For IPv6 > Add Configure Profile

Add Configure Profile

Profile Name

Start IPv6 Address

End IPv6 Address

Show Associate Profile

Switch Management > MVR For IPv6 > Show Associate Profile page is used to show the multicast group address for required services to one or more MVR6 domains.

COMMAND USAGE

- ◆ Use the Configure Profile page to statically configure all multicast group addresses that will join the MVR6 VLAN. Any multicast data associated with an MVR6 group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
- ◆ All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)
- ◆ The MVR6 group address range assigned to a profile cannot overlap with the group address range of any other profile.
- ◆ MVR6 domains can be associated with more than one MVR6 profile. But since MVR6 domains cannot share the group range, an MVR6 profile can only be associated with one MVR6 domain.

PARAMETERS

These parameters are displayed:

Associate Profile

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-20 characters)



	Profile Name	Start IPv6 Address	End IPv6 Address
<input type="checkbox"/>	profile1	ff13::1	ff13::9
<input type="checkbox"/>	profile2	ff13::12	ff13::19

Add Associate Profile

Switch Management > MVR For IPv6 > Add Associate Profile page is used to assign the multicast group address for required services to one or more MVR6 domains.

COMMAND USAGE

- ◆ Use the Configure Profile page to statically configure all multicast group addresses that will join the MVR6 VLAN. Any multicast data associated with an MVR6 group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
- ◆ All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8

colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

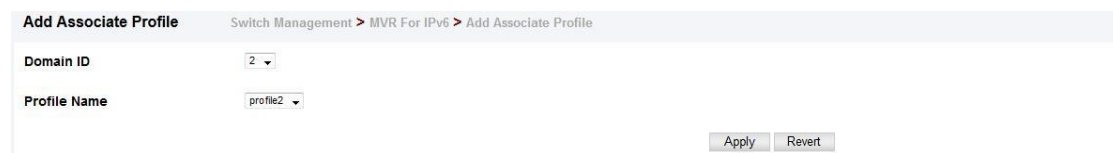
- ◆ The MVR6 group address range assigned to a profile cannot overlap with the group address range of any other profile.
- ◆ MVR6 domains can be associated with more than one MVR6 profile. But since MVR6 domains cannot share the group range, an MVR6 profile can only be associated with one MVR6 domain.

PARAMETERS

These parameters are displayed:

Associate Profile

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-20 characters)



Configure Interface

Switch Management > MVR For IPv6 > Configure Interface page is used to configure each interface that participates in the MVR6 protocol as a source port or receiver port. If you are sure that only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

COMMAND USAGE

- ◆ A port configured as an MVR6 receiver or source port can join or leave multicast groups configured under MVR6.
- ◆ Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR6 VLAN. MVR6 allows a receiver port to dynamically join or leave multicast groups within an MVR6 VLAN. Multicast groups can also be statically assigned to a receiver port. Receiver ports should not be statically configured as a member of the MVR6 VLAN. If so configured, its MVR6 status will be inactive. Also, note that VLAN membership for MVR6 receiver ports cannot be set to access mode.
- ◆ One or more interfaces may be configured as MVR6 source ports. A source port is able to both receive and send data for configured MVR6 groups or for groups which have been statically assigned. All source ports must belong to the MVR6 VLAN. Subscribers should not be directly connected to source ports.
- ◆ Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the

group list.

■ Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface.

■ Immediate leave does not apply to multicast groups which have been statically assigned to a port.

PARAMETERS

These parameters are displayed:

◆ **Domain ID** – An independent multicast domain. (Range: 1-5)

◆ **Port/Trunk** – Interface identifier.

◆ **Type** – The following interface types are supported:

■ **Non-MVR6** – An interface that does not participate in the MVR6 VLAN. (This is the default type.)

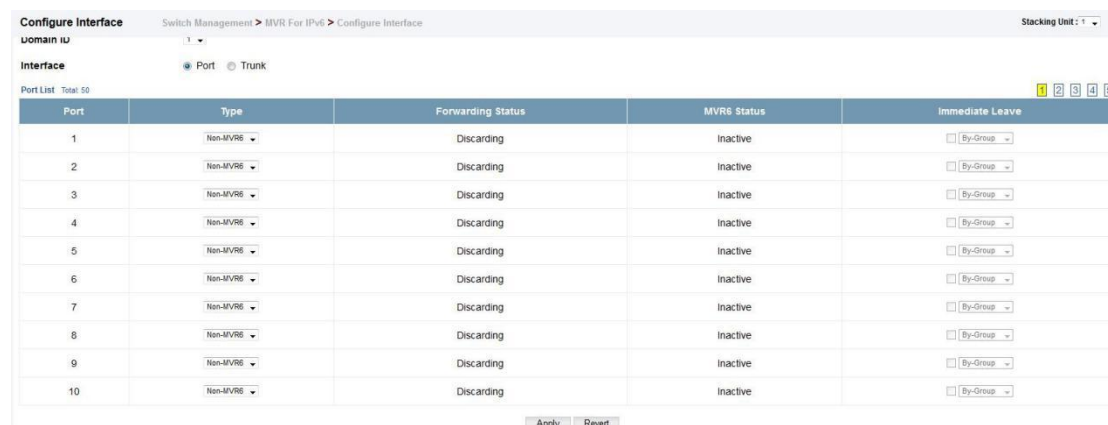
■ **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR6 VLAN. Note that the source port must be manually configured as a member of the MVR6 VLAN.

■ **Receiver** – A subscriber port that can receive multicast data sent through the MVR6 VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode.

◆ **Forwarding Status** – Shows if multicast traffic is being forwarded or blocked.

◆ **MVR6 Status** – Shows the MVR6 status. MVR6 status for source ports is “Active” if MVR6 is globally enabled on the switch. MVR6 status for receiver ports is “Active” only if there are subscribers receiving multicast traffic from one of the MVR6 groups, or a multicast group has been statically assigned to an interface.

◆ **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR6 receiver.)



Port	Type	Forwarding Status	MVR6 Status	Immediate Leave
1	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> [By-Group]
2	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> [By-Group]
3	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> [By-Group]
4	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> [By-Group]
5	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> [By-Group]
6	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> [By-Group]
7	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> [By-Group]
8	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> [By-Group]
9	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> [By-Group]
10	Non-MVR6	Discarding	Inactive	<input type="checkbox"/> [By-Group]

Show Static Group Member

Switch Management > MVR For IPv6 > Show Static Group Member page is used to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

COMMAND USAGE

- ◆ Multicast groups can be statically assigned to a receiver port using this configuration page.
- ◆ All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)
- ◆ The MVR6 VLAN cannot be specified as the receiver VLAN for static bindings.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Interface** – Port or trunk identifier.
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Group IPv6 Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR6 group range configured on the Configure General page.

Switch Management > MVR For IPv6 > Show Static Group Member

Domain ID:

Interface: Port Trunk

MVR6 Static Group Member List Total: 1

	VLAN	Group IPv6 Address
<input type="checkbox"/>	2	ff13::2

Add Static Group Member

Switch Management > MVR For IPv6 > Add Static Group Member page is used to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

COMMAND USAGE

- ◆ Multicast groups can be statically assigned to a receiver port using this configuration page.
- ◆ All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)
- ◆ The MVR6 VLAN cannot be specified as the receiver VLAN for static bindings.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Interface** – Port or trunk identifier.
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Group IPv6 Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR6 group range configured on the Configure General page.

Add Static Group Member Switch Management > MVR For IPv6 > Add Static Group Member

Domain ID

Interface Port Trunk

VLAN

Group IPv6 Address

Show Member

Switch Management > MVR For IPv6 > Show Member page is used to show the multicast groups either statically or dynamically assigned to the MVR6 receiver groups on each interface.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **Group IPv6 Address** – Multicast groups assigned to the MVR6 VLAN.
- ◆ **VLAN** – The VLAN through which the service is received. Note that this may be different from the MVR6 VLAN if the group address has been statically assigned.
- ◆ **Port** – Indicates the source address of the multicast service, or displays an asterisk if the group address has been statically assigned (these entries are marked as “Source”). Also shows the interfaces with subscribers for multicast services provided through the MVR6 VLAN (these entries are marked as “Receiver”).
- ◆ **Up Time** – Time this service has been forwarded to attached clients.
- ◆ **Expire** – Time before this entry expires if no membership report is received from currently active or new clients.
- ◆ **Count** – The number of multicast services currently being forwarded from the MVR6 VLAN.

Show Member Switch Management > MVR For IPv6 > Show Member

Domain ID

MVR6 Member List Total: 0

Group IPv6 Address	VLAN	Port	Up Time	Expire	Count
<input type="button" value="Clear MVR6 group"/>					

Show Query Statistics

Switch Management > MVR For IPv6 > Show Query Statistics page is used to display MVR6 protocol-related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-12)

◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

- ◆ **Querier IPv6 Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of MLD membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR6 groups active on this interface.

Output Statistics

- ◆ **Report** – The number of MLD membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

Show Query Statistics
Switch Management > MVR For IPv6 > Show Query Statistics

Domain ID	1 ▾
Query Statistics	
Querier IPv6 Address	∞
Querier Expire Time	00(h):00(m):00(s)
General Query Received	0
General Query Sent	0
Specific Query Received	0
Specific Query Sent	0
Number of Reports Sent	0
Number of Leaves Sent	0

Clear All
Click this button to clear all MVR6 statistics of the domain.

Refresh

Show VLAN Statistics

Switch Management > MVR For IPv6 > Show VLAN Statistics page is used to display MVR6 protocol-related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-12)
- ◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

- ◆ **Querier IPv6 Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of MLD membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR6 groups active on this interface.

Output Statistics

- ◆ **Report** – The number of MLD membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

Show VLAN Statistics Switch Management > MVR For IPv6 > Show VLAN Statistics

Domain ID:

VLAN:

Input Statistics

Report	0	Drop	0
Done	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	0		
Done	0		
G Query	0		
G(-S)-S Query	0		

Show Port Statistics

Switch Management > MVR For IPv6 > Show Port Statistics page is used to display MVR6 protocol-related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

- ◆ **Domain ID** – An independent multicast domain. (Range: 1-5)
- ◆ **VLAN** – VLAN identifier. (Range: 1-4093)
- ◆ **Port** – Port identifier. (Range: 1-12)
- ◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

- ◆ **Querier IPv6 Address** – The IP address of the querier on this interface.
- ◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.
- ◆ **General Query Received** – The number of general queries received on this interface.
- ◆ **General Query Sent** – The number of general queries sent from this interface.
- ◆ **Specific Query Received** – The number of specific queries received on this interface.
- ◆ **Specific Query Sent** – The number of specific queries sent from this interface.
- ◆ **Number of Reports Sent** – The number of reports sent from this interface.
- ◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- ◆ **Report** – The number of MLD membership reports received on this interface.
- ◆ **Leave** – The number of leave messages received on this interface.
- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.

◆ **Group** – The number of MVR6 groups active on this interface.

Output Statistics

◆ **Report** – The number of MLD membership reports sent from this interface.

◆ **Leave** – The number of leave messages sent from this interface.

◆ **G Query** – The number of general query messages sent from this interface.

◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

Show Port Statistics			
Switch Management > MVR For IPv6 > Show Port Statistics			
Domain ID	2		
Port	3		
Input Statistics			
Report	0	Drop	0
Done	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		
Output Statistics			
Report	0		
Done	0		
G Query	0		
G(-S)-S Query	0		
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>			

Show Trunk Statistics

Switch Management > MVR For IPv6 > Show Trunk Statistics page is used to display MVR6 protocol-related statistics for the specified interface.

PARAMETERS

These parameters are displayed:

◆ **Domain ID** – An independent multicast domain. (Range: 1-5)

◆ **VLAN** – VLAN identifier. (Range: 1-4093)

◆ **Port** – Port identifier. (Range: 1-12)

◆ **Trunk** – Trunk identifier. (Range: 1-12)

Query Statistics

◆ **Querier IPv6 Address** – The IP address of the querier on this interface.

◆ **Querier Expire Time** – The time after which this querier is assumed to have expired.

◆ **General Query Received** – The number of general queries received on this interface.

◆ **General Query Sent** – The number of general queries sent from this interface.

◆ **Specific Query Received** – The number of specific queries received on this interface.

◆ **Specific Query Sent** – The number of specific queries sent from this interface.

◆ **Number of Reports Sent** – The number of reports sent from this interface.

◆ **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

◆ **Report** – The number of MLD membership reports received on this interface.

◆ **Leave** – The number of leave messages received on this interface.

- ◆ **G Query** – The number of general query messages received on this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- ◆ **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.
- ◆ **Join Success** – The number of times a multicast group was successfully joined.
- ◆ **Group** – The number of MVR6 groups active on this interface.

Output Statistics

- ◆ **Report** – The number of MLD membership reports sent from this interface.
- ◆ **Leave** – The number of leave messages sent from this interface.
- ◆ **G Query** – The number of general query messages sent from this interface.
- ◆ **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

Show Trunk Statistics			
Switch Management > MVR For IPv6 > Show Trunk Statistics			
Domain ID	2		
Trunk	1		
Input Statistics			
Report	0	Drop	0
Done	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		
Output Statistics			
Report	0		
Done	0		
G Query	0		
G(-S)-S Query	0		
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>			

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers. Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Configure Global

Switch Management > LLDP > Configure Global page is used to set attributes for general functions such as globally enabling LLDP on the switch, setting the message ageout time, and setting the frequency for broadcasting general advertisements or reports about changes in the LLDP MIB.

PARAMETERS

These parameters are displayed:

- ◆ **LLDP** – Enables LLDP globally on the switch. (Default: Enabled)
- ◆ **Transmission Interval** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)
- ◆ **Hold Time Multiplier** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4) The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner. TTL in seconds is based on the following rule: minimum value ((Transmission Interval * Holdtime Multiplier), or 65535) Therefore, the default TTL is $4 * 30 = 120$ seconds.
- ◆ **Delay Interval** – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds)
The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission. This attribute must comply with the rule: $(4 * \text{Delay Interval}) \leq \text{Transmission Interval}$
- ◆ **Reinitialization Delay** – Configures the delay before attempting to reinitialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds) When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.
- ◆ **Notification Interval** – Configures the allowed interval for sending SNMP notifications about LLDP MIB changes. (Range: 5-3600 seconds; Default: 5 seconds) This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management. Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of `IldpStatsRemTableLastChangeTime` to detect any `IldpRemTablesChange` notification-events missed due to throttling or transmission loss.
- ◆ **MED Fast Start Count** – Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDPMED Fast Start mechanism. (Range: 1-10 packets; Default: 4 packets) The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDPMED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

Configure Global Switch Management > LLDP > Configure Global

LLDP	<input checked="" type="checkbox"/> Enabled
Transmission Interval (5-32768)	<input type="text" value="30"/> sec
Hold Time Multiplier (2-10)	<input type="text" value="4"/>
Delay Interval (1-8192)	<input type="text" value="2"/> sec
Reinitialization Delay (1-10)	<input type="text" value="2"/> sec
Notification Interval (5-3600)	<input type="text" value="5"/> sec
MED Fast Start Count (1-10)	<input type="text" value="4"/>

Note: The Transmission Interval must be greater than or equal to 4 times the Delay Interval.

Interface General

Switch Management > LLDP> Interface General page is used to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received, whether SNMP notifications are sent, and the type of information advertised.

PARAMETERS

These parameters are displayed:

- ◆ **Admin Status** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, TxRx, Disabled; Default: TxRx)
- ◆ **SNMP Notification** – Enables the transmission of SNMP trap notifications about LLDP and LLDP-MED changes. (Default: Disabled) This option sends out SNMP trap notifications to designated target stations at the interval specified by the Notification Interval in the preceding section. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/ TIA-1057), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs. For information on defining SNMP trap destinations, Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of `IldpStatsRemTableLastChangeTime` to detect any `IldpRemTablesChange` notification-events missed due to throttling or transmission loss.
- ◆ **MED Notification** – Enables the transmission of SNMP trap notifications about LLDP-MED changes. (Default: Disabled)
- ◆ **Basic Optional TLVs** – Configures basic information included in the TLV field of advertised messages.
- **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprisespecific

or other starting points for the search, such as the Interface or Entity MIB.

Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV. Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

■ **Port Description** – The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

■ **System Capabilities** – The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

■ **System Description** – The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

■ **System Name** – The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name. To configure the system name.

◆ **802.1 Organizationally Specific TLVs** – Configures IEEE 802.1 information included in the TLV field of advertised messages.

■ **Protocol Identity** – The protocols that are accessible through this interface.

■ **VLAN ID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.

■ **VLAN Name** – The name of all VLANs to which this interface has been assigned.

■ **Port and Protocol VLAN ID** – The port-based protocol VLANs configured on this interface.

◆ **802.3 Organizationally Specific TLVs** – Configures IEEE 802.3 information included in the TLV field of advertised messages.

■ **Link Aggregation** – The link aggregation capabilities, aggregation status of the link, and the IEEE 802.3 aggregated port identifier if this interface is currently a link aggregation member.

■ **Max Frame Size** – The maximum frame size.

■ **MAC/PHY Configuration/Status** – The MAC/PHY configuration and status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

◆ **MED TLVs** – Configures general information included in the MED TLV field of advertised messages.

■ **Capabilities** – This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

■ **Inventory** – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

■ **Location** – This option advertises location identification details.

■ **Network Policy** – This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper

network policy configurations frequently result in voice quality degradation or complete service disruption.

◆ **MED-Location Civic Address** – Configures information for the location of the attached device included in the MED TLV field of advertised messages, including the country and the device type.

■ **Country** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

■ **Device entry refers to** – The type of device to which the location applies:

- Location of DHCP server.
- Location of network element closest to client.
- Location of client. (This is the default.)

CA-Type

Switch Management > LLDP > CA-Type page is used to specify the physical location of the device attached to an interface.

COMMAND USAGE

◆ Use the Civic Address type (CA-Type) to advertise the physical location of the device attached to an interface, including items such as the city, street number, building and room information. The address location is specified as a type and value pair, with the civic address type defined in RFC 4776. The following table describes some of the CA type numbers and provides examples.

CA Type	Description	CA Value Example
1	National subdivisions (state, canton, province)	California
2	County, parish	Orange
3	City, township	Irvine
4	City division, borough, city district	West Irvine
5	Neighborhood, block	Riverside
6	Group of streets below the neighborhood level	Exchange
18	Street suffix or type	Avenue

19	House number	320
20	House number suffix	A
21	Landmark or vanity address	Tech Center
26	Unit (apartment, suite)	Apt 519
27	Floor	5
28	Room	509B

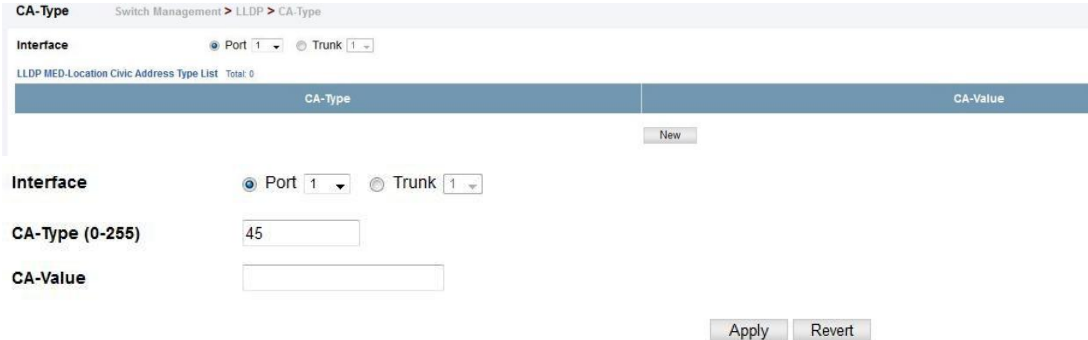
◆ Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.

PARAMETERS

These parameters are displayed in the web interface:

◆ **CA-Type** – Descriptor of the data civic address value. (Range: 0-255)

◆ **CA-Value** – Description of a location. (Range: 1-32 characters)



Show Local Information

Switch Management > LLDP > Show Local Information page is used to display information about the switch, such as its MAC address, chassis ID, management IP address, and port information.

PARAMETERS

These parameters are displayed:

Global Settings

◆ **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.

ID Basis	Reference
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Interface alias	IfAlias (IETF RFC 2863)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)

Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Locally assigned	locally assigned

◆ **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.

◆ **System Name** – A string that indicates the system’s administratively assigned name.

◆ **System Description** – A textual description of the network entity. This field is also displayed by the **show system** command.

◆ **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.

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

◆ **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. Refer to the preceding table.

◆ **Management Address** – The management address associated with the local system. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Interface Settings

The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.

◆ **Port/Trunk Description** – A string that indicates the port or trunk description. If RFC 2863 is implemented, the ifDescr object should be used for this field.

◆ **Port/Trunk ID** – A string that contains the specific identifier for the port or trunk from which this LLDPDU was transmitted.

Show Local Information	
Switch Management > LLDP > Show Local Information	
<input checked="" type="radio"/> General <input type="radio"/> Port <input type="radio"/> Port Details <input type="radio"/> Trunk <input type="radio"/> Trunk Details	
LLDP Local Device Information	
Chassis Type	MAC Address
Chassis ID	00-00-22-00-04-02
System Name	
System Description	S3900-48T4S
System Capabilities Supported	Bridge, Router
System Capabilities Enabled	Bridge, Router
Management Address	00-00-22-00-04-02 (MAC address)

Show Remote Information

Switch Management > LLDP > Show Remote Information page is used to display information about devices connected directly to the switch's ports which are advertising information through LLDP, or to display detailed information about an LLDP-enabled device connected to a specific port on the local switch.

PARAMETERS

These parameters are displayed:

Port

- ◆ **Local Port** – The local port to which a remote LLDP-capable device is attached.
- ◆ **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- ◆ **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- ◆ **System Name** – A string that indicates the system's administratively assigned name.

Port Details

- ◆ **Port** – Port identifier on local switch.
- ◆ **Remote Index** – Index of remote device attached to this port.
- ◆ **Local Port** – The local port to which a remote LLDP-capable device is attached.
- ◆ **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.
- ◆ **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- ◆ **System Name** – A string that indicates the system's assigned name.
- ◆ **System Description** – A textual description of the network entity.
- ◆ **Port Type** – Indicates the basis for the identifier that is listed in the Port ID field.

ID Basis	Reference
Interface alias	IfAlias (IETF RFC 2863)
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Agent circuit ID	agent circuit ID (IETF RFC 3046)
Locally assigned	locally assigned

- ◆ **Port Description** – A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- ◆ **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.

- ◆ **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.
- ◆ **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled.
- ◆ **Management Address List** – The management addresses for this device. Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Port Details – 802.1 Extension Information

- ◆ **Remote Port VID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.
- ◆ **Remote Port-Protocol VLAN List** – The port-based protocol VLANs configured on this interface, whether the given port (associated with the remote system) supports port-based protocol VLANs, and whether the port-based protocol VLANs are enabled on the given port associated with the remote system.
- ◆ **Remote VLAN Name List** – VLAN names associated with a port.
- ◆ **Remote Protocol Identity List** – Information about particular protocols that are accessible through a port. This object represents an arbitrary local integer value used by this agent to identify a particular protocol identity, and an octet string used to identify the protocols associated with a port of the remote system.

Port Details – 802.3 Extension Port Information

- ◆ **Remote Port Auto-Neg Supported** – Shows whether the given port (associated with remote system) supports auto-negotiation.
- ◆ **Remote Port Auto-Neg Adv-Capability** – The value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) which is associated with a port on the remote system.

Bit	Capability
0	other or unknown
1	10BASE-T half duplex mode
2	10BASE-T full duplex mode
3	100BASE-T4
4	100BASE-TX half duplex mode
5	100BASE-TX full duplex mode
6	100BASE-T2 half duplex mode
7	100BASE-T2 full duplex mode
8	PAUSE for full-duplex links
9	Asymmetric PAUSE for full-duplex links
10	Symmetric PAUSE for full-duplex links
11	Asymmetric and Symmetric PAUSE for full-duplex links
12	1000BASE-X, -LX, -SX, -CX half duplex mode

13	1000BASE-X, -LX, -SX, -CX full duplex mode
14	1000BASE-T half duplex mode
15	1000BASE-T full duplex mode

◆ **Remote Port Auto-Neg Status** – Shows whether port autonegotiation is enabled on a port associated with the remote system.

◆ **Remote Port MAU Type** – An integer value that indicates the operational MAU type of the sending device. This object contains the integer value derived from the list position of the corresponding dot3MauType as listed in IETF RFC 3636 and is equal to the last number in the respective dot3MauType OID.

Port Details – 802.3 Extension Power Information

◆ **Remote Power Class** – The port Class of the given port associated with the remote system (PSE – Power Sourcing Equipment or PD – Powered Device).

◆ **Remote Power MDI Status** – Shows whether MDI power is enabled on the given port associated with the remote system.

◆ **Remote Power Pairs** – “Signal” means that the signal pairs only are in use, and “Spare” means that the spare pairs only are in use.

◆ **Remote Power MDI Supported** – Shows whether MDI power is supported on the given port associated with the remote system.

◆ **Remote Power Pair Controllable** – Indicates whether the pair selection can be controlled for sourcing power on the given port associated with the remote system.

◆ **Remote Power Classification** – This classification is used to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points and others, will be classified according to their power requirements.

Port Details – 802.3 Extension Trunk Information

◆ **Remote Link Aggregation Capable** – Shows if the remote port is not in link aggregation state and/or it does not support link aggregation.

◆ **Remote Link Aggregation Status** – The current aggregation status of the link.

◆ **Remote Link Port ID** – This object contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component associated with the remote system. If the remote port is not in link aggregation state and/or it does not support link aggregation, this value should be zero.

Port Details – 802.3 Extension Frame Information

◆ **Remote Max Frame Size** – An integer value indicating the maximum supported frame size in octets on the port component associated with the remote system.

Port Details – LLDP-MED Capability 8

◆ **Device Class** – Any of the following categories of endpoint devices:

■ **Class 1** – The most basic class of endpoint devices.

■ **Class 2** – Endpoint devices that supports media stream capabilities.

■ **Class 3** – Endpoint devices that directly supports end users of the IP communication systems.

■ **Network Connectivity Device** – Devices that provide access to the IEEE 802 based LAN

infrastructure for LLDP-MED endpoint devices. These may be any LAN access device including LAN switch/router, IEEE 802.1 bridge, IEEE 802.3 repeater, IEEE 802.11 wireless access point, or any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.

◆ **Supported Capabilities** – The supported set of capabilities that define the primary function(s) of the port:

- LLDP-MED Capabilities
- Network Policy
- Location Identification
- Extended Power via MDI – PSE
- Extended Power via MDI – PD
- Inventory

◆ **Current Capabilities** – The set of capabilities that define the primary function(s) of the port which are currently enabled.

Port Details – Network Policy

◆ **Application Type** – The primary application(s) defined for this network policy:

- Voice
- Voice Signaling
- Guest Signaling
- Guest Voice Signaling
- Softphone Voice
- Video Conferencing
- Streaming Video
- Video Signaling

◆ **Tagged Flag** – Indicates whether the specified application type is using a tagged or untagged VLAN.

◆ **Layer 2 Priority** – The Layer 2 priority to be used for the specified application type. This field may specify one of eight priority levels (0-7), where a value of 0 represents use of the default priority.

◆ **Unknown Policy Flag** – Indicates that an endpoint device wants to explicitly advertise that this policy is required by the device, but is currently unknown.

◆ **VLAN ID** – The VLAN identifier (VID) for the port as defined in IEEE 802.1Q. A value of zero indicates that the port is using priority tagged frames, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

◆ **DSCP Value** – The DSCP value to be used to provide Diffserv node behavior for the specified application type. This field may contain one of 64 code point values (0-63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Port Details – Location Identification

◆ **Location Data Format** – Any of these location ID data formats:

- Coordinate-based LCI9 – Defined in RFC 3825, includes latitude resolution, latitude, longitude resolution, longitude, altitude type, altitude resolution, altitude, and datum.
- Civic Address LCI9 – Includes What, Country code, CA type, CA length and CA value.
- ECS ELIN – Emergency Call Service Emergency Location Identification Number supports traditional PSAP-based Emergency Call Service in North America.

◆ **Country Code** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

◆ **What** – The type of device to which the location applies as described for the field entry.
Port Details – Inventory8

◆ **Hardware Revision** – The hardware revision of the end-point device.

◆ **Software Revision** – The software revision of the end-point device.

◆ **Manufacture Name** – The manufacturer of the end-point device

◆ **Asset ID** – The asset identifier of the end-point device. End-point devices are typically assigned asset identifiers to facilitate inventory management and assets tracking.

◆ **Firmware Revision** – The firmware revision of the end-point device.

◆ **Serial Number** – The serial number of the end-point device.

◆ **Model Name** – The model name of the end-point device.

◆ **Asset ID** – The asset identifier of the end-point device.

Switch Management > LLDP > Show Remote Information

Stacking Unit: 1

Port Port Details Trunk Trunk Details

LLDP Remote Device Port List Total: 1

Local Port	Chassis ID	Port ID	System Name
Eth 1/26	00-01-00-00-02-01	00-01-00-00-02-19	

Show Statistics

Switch Management > LLDP > Show Statistics page is used to display statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

PARAMETERS

These parameters are displayed:

General Statistics on Remote Devices

◆ **Neighbor Entries List Last Updated** – The time the LLDP neighbor entry list was last updated.

◆ **New Neighbor Entries Count** – The number of LLDP neighbors for which the remote TTL has not yet expired.

◆ **Neighbor Entries Deleted Count** – The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.

◆ **Neighbor Entries Dropped Count** – The number of times which the remote database on this switch dropped an LLDPDU because of insufficient resources.

◆ **Neighbor Entries Age-out Count** – The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

Port/Trunk

◆ **Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.

◆ **Frames Invalid** – A count of all LLDPDUs received with one or more detectable errors.

◆ **Frames Received** – Number of LLDP PDUs received.

◆ **Frames Sent** – Number of LLDP PDUs transmitted.

◆ **TLVs Unrecognized** – A count of all TLVs not recognized by the receiving LLDP local agent.

◆ **TLVs Discarded** – A count of all LLDPDUs received and then discarded due to insufficient memory space, missing or out-of-sequence attributes, or any other reason.

◆ **Neighbor Ageouts** – A count of the times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

Show Statistics	
Switch Management > LLDP > Show Statistics	
<input checked="" type="radio"/> General <input type="radio"/> Port <input type="radio"/> Trunk	
LLDP Device Statistics	
Neighbor Entries List Last Updated	5724 sec
New Neighbor Entries Count	3
Neighbor Entries Deleted Count	1
Neighbor Entries Dropped Count	0
Neighbor Entries Age-out Count	0

ERPS

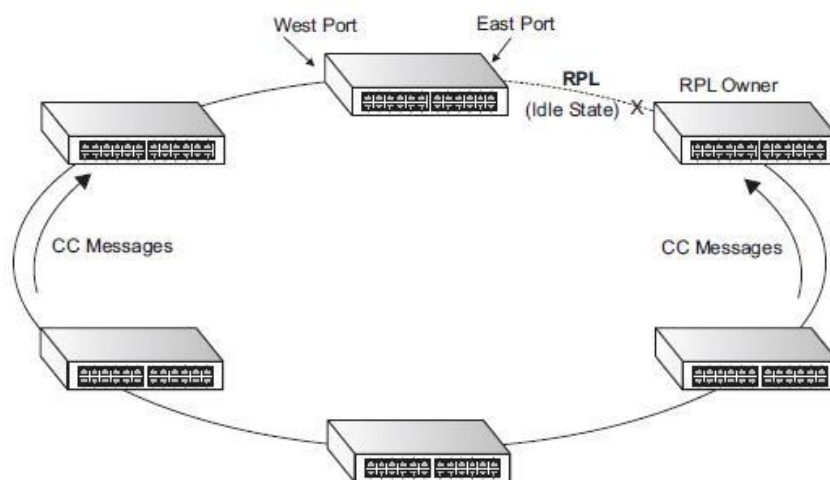
The ITU G.8032 recommendation specifies a protection switching mechanism and protocol for Ethernet layer network rings. Ethernet rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in G.8032 achieve highly reliable and stable protection; and never form loops, which would fatally affect network operation and service availability. The G.8032 recommendation, also referred to as Ethernet Ring Protection Switching (ERPS), can be used to increase the availability and robustness of Ethernet rings. An Ethernet ring built using ERPS can provide resilience at a lower cost and than that provided by SONET or EAPS rings. ERPS is more economical than EAPS in that only one physical link is required between each node in the ring. However, since it can tolerate only one break in the ring, it is not as robust as EAPS. ERPS supports up to 255 nodes in the ring structure. ERPS requires a higher convergence time when more than 16 nodes are used, but should always run under than 500 ms.

Operational Concept

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this link is blocked to traffic. One designated node, the RPL owner, is responsible for blocking traffic over the RPL. When a ring failure occurs, the RPL owner is responsible for unblocking the RPL, allowing this link to be used for traffic. Ring nodes may be in one of two states:

Idle – normal operation, no link/node faults detected in ring
 Protection – Protection switching in effect after identifying a signal fault
 In Idle state, the physical topology has all nodes connected in a ring. The logical topology guarantees that all nodes are connected without a loop by blocking the RPL. Each link is monitored by its two adjacent nodes using Connectivity Fault Management (CFM) protocol messages. Protection switching (opening the RPL to traffic) occurs when a signal failure message generated by the Connectivity Fault Management (CFM) protocol is declared on one of the ring links, and the detected failure has a higher priority than any other request; or a Ring – Automatic Protection Switching

protocol request (R-APS, as defined in Y.1731) is received which has a higher priority than any other local request. A link/node failure is detected by the nodes adjacent to the failure. These nodes block the failed link and report the failure to the ring using R-APS (SF) messages. This message triggers the RPL owner to unblock the RPL, and all nodes to flush their forwarding database. The ring is now in protection state, but it remains connected in a logical topology. When the failed link recovers, the traffic is kept blocked on the nodes adjacent to the recovered link. The nodes adjacent to the recovered link transmit R-APS (NR - no request) message indicating they have no local request. When the RPL owner receives an R-APS (NR) message it starts the Wait-To-Recover (WTR) timer. Once WTR timer expires, the RPL owner blocks the RPL and transmits an R-APS (NR, RB - ring blocked) message. Nodes receiving this message flush the forwarding database and unblock their previously blocked ports. The ring is now returned to Idle state.



Configure Global

Switch Management > ERPS > Configure Global page is used to globally enable or disable ERPS on the switch.

PARAMETERS

These parameters are displayed:

◆ **ERPS Status** – Enables ERPS on the switch. (Default: Disabled) ERPS must be enabled globally on the switch before it can be enabled on an ERPS ring.

Configure Global		Switch Management > ERPS > Configure Global	
ERPS Status	<input checked="" type="checkbox"/> Enabled	Apply	Revert

Domain

Switch Management > ERPS > Domain pages is used to add ERPS ring.

Domain Switch Management > ERPS > Domain

Domain List Total: 1

Domain Name

Domain ID (1-255)

Apply Revert

Domain Switch Management > ERPS > Domain

Domain List Total: 1

	Domain Name	ID	Admin Status	Ver	MEG Level	Control VLAN	Node State	Type	Revertive	W/E	Interface	Port State	Local SF	Local FS	Local MS	MEP	RPL
<input type="checkbox"/>	myr	2	Enabled	2	1	10	Protection	RPL Owner	Yes	West	Eth 1/5	Blocking	Yes	No	No		Yes
										East	Eth 1/1	Blocking	Yes	No	No		No

New Delete Revert

Domain Details

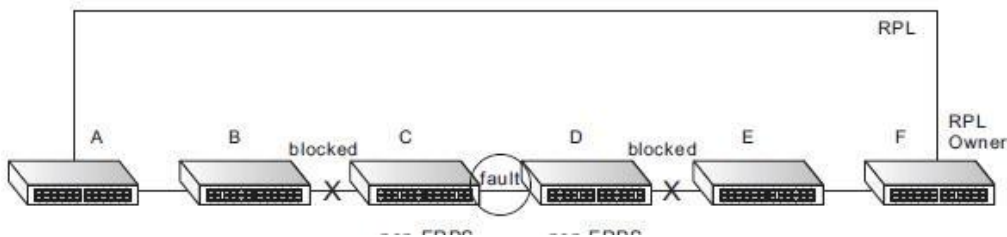
Switch Management > ERPS > Domain Details pages is used to configure details of ERPS ring. An ERPS ring containing one Control VLAN and one or more protected Data VLANs must be configured, and the global ERPS function enabled on the Switch before a ring can start running. Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter the active state.

Limitations

When configuring a ring port, note that these ports cannot be part of a spanning tree, nor can they be members of a static or dynamic trunk.

Non-ERPS Device Protection

◆ The RPL owner node detects a failed link when it receives R-APS (SF - signal fault) messages from nodes adjacent to the failed link. The owner then enters protection state by unblocking the RPL. However, using this standard recovery procedure may cause a non-ERPS device to become isolated when the ERPS device adjacent to it detects a continuity check message (CCM) loss event and blocks the link between the non-ERPS device and ERPS device. CCMs are propagated by the Connectivity Fault Management (CFM) protocol. If the standard recovery procedure were used as shown in the following figure, and node E detected CCM loss, it would send an RAPS (SF) message to the RPL owner and block the link to node D, isolating that non-ERPS device.



When non-ERPS device protection is enabled on the ring, the ring ports on the RPL owner node and non-owner nodes will not be blocked when signal loss is detected by CCM loss events.

◆ When non-ERPS device protection is enabled on an RPL owner node, it will send

non-standard health-check packets to poll the ring health when it enters the protection state. It does not use the normal procedure of waiting to receive an R-APS (NR - no request) message from nodes adjacent to the recovered link. Instead, it waits to see if the non-standard health-check packets loop back. If they do, indicating that the fault has been resolved, the RPL will be blocked. After blocking the RPL, the owner node will still transmit an R-APS (NR, RB - ring blocked) message. ERPS-compliant nodes receiving this message flush their forwarding database and unblock previously blocked ports. The ring is now returned to Idle state.

PARAMETERS

These parameters are displayed:

Add

◆ **Domain Name** – Name of an ERPS ring. (Range: 1-12 characters)

Show

◆ **Domain Name** – Name of a configured ERPS ring.

◆ **Node State** – Shows the following ERPS states:

■ **Init** – The ERPS ring has started but has not yet determined the status of the ring.

■ **Idle** – If all nodes in a ring are in this state, it means that all the links in the ring are up. This state will switch to protection state if a link failure occurs.

■ **Protection** – If a node in this state, it means that a link failure has occurred. This state will switch to idle state if all the failed links recover.

◆ **MEG Level** – The maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.

◆ **Admin Status** – Shows whether ERPS is enabled on the switch.

◆ **West Port** – Shows the west ring port for this node.

◆ **East Port** – Shows the east ring port for this node.

◆ **RPL Owner** – Shows if this node is the RPL owner.

◆ **Control VLAN** – Shows the Control VLAN ID.

◆ **Non ERPS Device Protection** – Shows if non-standard health-check packets are sent when in protection state.

Configure Details

◆ **Domain Name** – Name of a configured ERPS ring.

◆ **Admin Status** – Activates the current ERPS ring. Before enabling a ring, the global ERPS function should be enabled, the east and west ring ports configured on each node, the RPL owner specified, and the control VLAN configured. Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter idle state if no signal failures are detected.

◆ **MEG Level** – The maintenance entity group (MEG) level which provides a communication channel for ring automatic protection switching (R-APS) information. (Range: 0-7) This parameter is used to ensure that received R-APS PDUs are directed for this ring. A unique level should be configured for each local ring if there are many R-APS PDUs passing through this switch.

◆ **Node ID** – A MAC address unique to the ring node. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

◆ **Node State** – Refer to the parameters for the Show page.

◆ **West Port** – Connects to next ring node to the west. Each node must be connected to two neighbors on the ring. For convenience, the ports connected are referred to as east and west ports. Alternatively, the closest neighbor to the east should be the next node in the ring in a clockwise direction, and the closest neighbor to the west should be the next node in the ring in a counter-clockwise direction. Note that a ring port cannot be configured as a member of a spanning tree, a dynamic trunk, or a static trunk. Once configured, this field shows the ring port for this node, and the interface state:

■ **Blocking** – The transmission and reception of traffic is blocked and the forwarding of R-APS messages is blocked, but the transmission of locally generated R-APS messages is allowed and the reception of all R-APS messages is allowed.

■ **Forwarding** – The transmission and reception of traffic is allowed; transmission, reception and forwarding of R-APS messages is allowed.

■ **Down** – The interface is not linked up.

■ **Unknown** – The interface is not in a known state.

◆ **East Port** – Connects to next ring node to the east.

◆ **RPL Port** – If node is connected to the RPL, this shows by which interface.

◆ **RPL Owner** – Configures a ring node to be the Ring Protection Link (RPL) owner.

◆ **Holdoff Timer** – The hold-off timer is used to filter out intermittent link faults. Faults will only be reported to the ring protection mechanism if this timer expires. (Range: 0-10000 milliseconds, in steps of 100 milliseconds) In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. Its purpose is to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer. When a new defect or more severe defect occurs (new Signal Failure), this event will not be reported immediately to the protection switching mechanism if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the timer expires, whether a defect still exists or not, the timer will be checked. If one does exist, that defect will be reported to the protection switching mechanism. The reported defect need not be the same one that started the timer.

◆ **Guard Timer** – The guard timer is used to prevent ring nodes from receiving outdated R-APS messages. During the duration of the guard timer, all received R-APS messages are ignored by the ring protection control process, giving time for old messages still circulating on the ring to expire. (Range: 10-2000 milliseconds, in steps of 10 milliseconds) The guard timer duration should be greater than the maximum expected forwarding delay for an R-APS message to pass around the ring. A side-effect of the guard timer is that during its duration, a node will be unaware of new or existing ring requests transmitted from other nodes.

◆ **WTR Timer** – The wait-to-restore timer is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. (Range: 5-12 minutes) If the switch goes into ring protection state due to a signal failure, after the failure condition is cleared, the RPL owner will start the wait-to-restore timer and wait until it expires to verify that the ring has stabilized before blocking the RPL and returning to the Idle (normal operating) state.

◆ **Control VLAN** – A dedicated VLAN used for sending and receiving E-APS protocol messages. (Range: 1-4093) Configure one control VLAN for each ERPS ring. First create the VLAN to be used as the control VLAN, add the ring ports for the east and west interface as tagged members to this VLAN, and then use this parameter to add it to the ring. The

following restrictions are recommended to avoid creating a loop in the network or other problems which may occur under some situations:

■ The Control VLAN must not be configured as a Layer 3 interface (with an IP address), a dynamic VLAN (with GVRP enabled), nor as a private VLAN.

■ In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN.

■ Also, the ring ports of the Control VLAN must be tagged. Once the ring has been activated, the configuration of the control VLAN cannot be modified. Use the Admin Status parameter to stop the ERPS ring before making any configuration changes to the control VLAN.

◆ **Propagate TC** – Enables propagation of topology change messages from a secondary ring to the primary ring. (Default: Disabled) When a secondary ring detects a topology change, it can pass a message about this event to the major ring. When the major ring receives this kind of message from a secondary ring, it can clear the MAC addresses on its ring ports to help the secondary ring restore its connections more quickly through protection switching. When the MAC addresses are cleared, data traffic may flood onto the major ring. The data traffic will become stable after the MAC addresses are learned again. The major ring will not be broken, but the bandwidth of data traffic on the major ring may suffer for a short period of time due to this flooding behavior.

◆ **Sub Domain** – A secondary ERPS ring which uses this primary ring for sending control packets.

◆ **Major Domain** – The ERPS ring used for sending control packets. This switch can support up to two rings. However, ERPS control packets can only be sent on one ring. This parameter is used to indicate that the current ring is a secondary ring, and to specify the major ring which will be used to send ERPS control packets. The Ring Protection Link (RPL) is always the west port. So the physical port on a secondary ring must be the west port. In other words, if a domain has two physical ring ports, this ring can only be a major ring, not a secondary ring (or sub-domain) which can have only one physical ring port. The major domain therefore cannot be set if the east port is already configured.

◆ **Non-ERPS Device Protection** – Sends non-standard health-check packets when an owner node enters protection state without any link down event having been detected through Signal Fault messages. (Default: Disabled)

Domain Details	
Domain Name	mjr
Domain ID	2
Admin Status	<input checked="" type="checkbox"/> Enabled
Version	2
MEG Level (0-7)	1
Control VLAN	<input checked="" type="checkbox"/> 10
Node State	Protection
Node Type	RPL Owner
Revertive	<input checked="" type="checkbox"/> Enabled
Major Domain	<input type="checkbox"/>
Node ID	00-00-00-00-12-01 (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)
R-APS with VC	<input checked="" type="checkbox"/> Enabled
R-APS Def MAC	<input checked="" type="checkbox"/> Enabled
Propagate TC	<input type="checkbox"/> Enabled

Non-ERPS Dev Protect	<input type="checkbox"/> Enabled		
Holdoff Timer (0-10000)	<input type="text" value="0"/> ms		
Guard Timer (10-2000)	<input type="text" value="500"/> ms		
WTB Timer	5500 ms		
WTR Timer (5-12)	<input type="text" value="5"/> min		
WTB Expire			
WTR Expire			
West	<input checked="" type="checkbox"/> Enabled	East	<input checked="" type="checkbox"/> Enabled
Interface	<input type="text" value="Eth 1/5"/>	Interface	<input type="text" value="Eth 1/1"/>
Port State	Blocking	Port State	Blocking
Local SF	Yes	Local SF	Yes
Local FS	No	Local FS	No
Local MS	No	Local MS	No
MEP (1-8191)	<input type="checkbox"/>	MEP (1-8191)	<input type="checkbox"/>
RPL	Yes	RPL	No

Domain Operation

Switch Management > ERPS > Domain Operation pages is used to configure force or manual mode on ring ports.

Domain Operation Switch Management > ERPS > Domain Operation

Domain Name:

Operation:

Show Statistics

Switch Management > ERPS > Show Statistics pages is used to display or clear statistics information on ring ports.

Show Statistics Switch Management > ERPS > Show Statistics

Domain Name:

West

Interface: Eth 1/5

Local SF: 1

Local Clear SF: 0

	Sent	Received	Ignored
SF	0	0	0
NR	0	0	0
NR-RB	0	0	0
FS	0	0	0
MS	0	0	0
EVENT	0	0	0
HEALTH	0	0	0

East

Interface: Eth 1/1

Local SF	1		
Local Clear SF	0		
	Sent	Received	Ignored
SF	0	0	0
NR	0	0	0
NR-RB	0	0	0
FS	0	0	0
MS	0	0	0
EVENT	0	0	0
HEALTH	0	0	0

Loopback Detection

Switch Management > Loopback Detection page is used to configure loopback detection on an interface. When loopback detection is enabled and a port or trunk receives its own BPDU, the detection agent drops the loopback BPDU, sends an SNMP trap, and places the interface in discarding mode. This loopback state can be released manually or automatically. If the interface is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:

- ◆ The interface receives any other BPDU except for its own, or;
- ◆ The interfaces' link status changes to link down and then link up again, or;
- ◆ The interface ceases to receive its own BPDUs in a forward delay interval.

Configure Global

PARAMETERS

These parameters are displayed:

- ◆ **Status** – Enables loopback detection on this interface. (Default: Enabled)
- ◆ **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)
- ◆ **Release Mode** – Configures the interface for automatic or manual loopback release. (Default: Auto)
- ◆ **Release** – Allows an interface to be manually released from discard mode. This is only available if the interface is configured for manual release mode.
- ◆ **Action** – Sets the response for loopback detection to block user traffic or shut down the interface. (Default: Block)
- ◆ **Transmit Interval** – The duration to shut down the interface. (Range: 1-32767 seconds; Default: 60 seconds) If an interface is shut down due to a detected loopback, and the release mode is set to "Auto," the selected interface will be automatically enabled when the shutdown interval has expired.

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

Configure Global
Switch Management > Loopback Detection > Configure Global

Global Status Enabled

Transmit Interval (1-32767) sec

Recover Time (60-1000000) sec

Action

Trap

[Click this button to release all looped ports manually](#)

Configure Interface

Enable/disable port loopback detection

Configure Interface
Switch Management > Loopback Detection > Configure Interface
Stacking Unit : 1

Interface Port Trunk

Port List Total: 28 1 2 3

Port	Admin State	Operation State	Looped VLAN
1	<input type="checkbox"/> Enabled	Normal	None
2	<input type="checkbox"/> Enabled	Normal	None
3	<input type="checkbox"/> Enabled	Normal	None
4	<input type="checkbox"/> Enabled	Normal	None
5	<input type="checkbox"/> Enabled	Normal	None
6	<input type="checkbox"/> Enabled	Normal	None
7	<input type="checkbox"/> Enabled	Normal	None
8	<input type="checkbox"/> Enabled	Normal	None
9	<input type="checkbox"/> Enabled	Normal	None
10	<input type="checkbox"/> Enabled	Normal	None

UDLD

The switch can be configured to detect general loopback conditions caused by hardware problems or faulty protocol settings. When enabled, a control frame is transmitted on the participating ports, and the switch monitors inbound traffic to see if the frame is looped

back.

Usage Guidelines

- ◆ The default settings for the control frame transmit interval and recover time may be adjusted to improve performance for your specific environment. The shutdown mode may also need to be changed once you determine what kind of packets are being looped back.
- ◆ General loopback detection provided by the commands described in this section and loopback detection provided by the spanning tree protocol cannot both be enabled at the same time. If loopback detection is enabled for the spanning tree protocol, general loopback detection cannot be enabled on the same interface.
- ◆ When a loopback event is detected on an interface or when an interface is released from a shutdown state caused by a loopback event, a trap message is sent and the event recorded in the system log.
- ◆ Loopback detection must be enabled both globally and on an interface for loopback detection to take effect.

Configure Global

Switch Management > UDLD > Configure Global page is used to configure the UniDirectional Link Detection message probe interval, detection interval, and recovery interval.

Parameters

These parameters are displayed:

- ◆ **Message Interval** – Configures the message interval between UDLD probe messages for ports in the advertisement phase and determined to be bidirectional. (Range: 7-90 seconds; Default: 15 seconds) UDLD probe messages are sent after linkup or detection phases. During the detection phase, messages are exchanged at the maximum rate of one per second. After that, if the protocol reaches a stable state and determines that the link is bidirectional, the message interval is increased to a configurable value based on a curve known as M1(t), a time-based function described in RFC 5171. If the link is deemed anything other than bidirectional at the end of the detection phase, this curve becomes a flat line with a fixed value of Mfast (7 seconds). If the link is instead deemed bidirectional, the curve will use Mfast for the first four subsequent message transmissions and then transition to an Mslow value for all other steady-state transmissions. Mslow is the value configured by this command.
- ◆ **Detection Interval** – Sets the amount of time the switch remains in detection state after discovering a neighbor. (Range: 5-255 seconds; Default: 5 seconds) When a neighbor device is discovered by UDLD, the switch enters “detection state” and remains in this state for specified detection-interval. After the detection-interval expires, the switch tries to decide whether or the link is unidirectional based on the information collected during the “detection state.”
- ◆ **Recovery Status** – Configures the switch to automatically recover from UDLD disabled port state after a period specified by the Recovery Interval. (Default: Disabled) When automatic recovery state is changed, any ports shut down by UDLD will be reset.
- ◆ **Recovery Interval** – Specifies the period after which to automatically recover from UDLD disabled port state. (Range: 30-86400 seconds; Default: 7 seconds) When the recovery

interval is changed, any ports shut down by UDLD will be reset.

Configure Global Switch Management > UDLD > Configure Global

Message Interval (7-90)	<input style="width: 80%;" type="text" value="15"/>	seconds
Detection Interval (5-255)	<input style="width: 80%;" type="text" value="5"/>	seconds
Recovery Status	<input checked="" type="checkbox"/> Enabled	
Recovery Interval (30-86400)	<input style="width: 80%;" type="text" value="300"/>	seconds

Configure Interface

Switch Management > UDLD > Configure Interface page is used to enable UDLD and aggressive mode which reduces the shut-down delay after loss of bidirectional connectivity is detected.

Parameters

These parameters are displayed:

- ◆ Port – Port identifier. (Range: 1-28/52)
- ◆ UDLD – Enables UDLD on a port. (Default: Disabled)
- UDLD requires that all the devices connected to the same LAN segment be running the protocol in order for a potential mis-configuration to be detected and for prompt corrective action to be taken.
- Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-synch neighbor, it (re)starts the detection process on its side of the connection and sends N echo messages in reply. (This mechanism implicitly assumes that N packets are sufficient to get through a link and reach the other end, even though some of them might get dropped during the transmission.) Since this behavior must be the same on all the neighbors, the sender of the echoes expects to receive an echo in reply. If the detection process ends without the proper echo information being received, the link is considered to be unidirectional.
- ◆ Aggressive Mode – Reduces the shut-down delay after loss of bidirectional connectivity is detected. (Default: Disabled) UDLD can function in two modes: normal mode and aggressive mode.
- In normal mode, determination of link status at the end of the detection process is always based on information received in UDLD messages: whether that's information about the exchange of proper neighbor identification or the absence of such. Hence, albeit bound by a timer, normal mode determinations are always based on gleaned information, and as such are "event-based." If no such information can be obtained (e.g., because of a bidirectional loss of connectivity), UDLD follows a conservative approach to minimize false positives during the detection process and deems a port to be in "undetermined" state. In other words, normal mode will shut down a port only if it can explicitly determine that the associated link is faulty for an extended period of time.

■ In aggressive mode, UDLD will also shut down a port if it loses bidirectional connectivity with the neighbor for the same extended period of time (as that mentioned above for normal mode) and subsequently fails repeated last-resort attempts to re-establish communication with the other end of the link. This mode of operation assumes that loss of communication with the neighbor is a meaningful network event in itself, and a symptom of a serious connectivity problem. Because this type of detection can be event-less, and lack of information cannot always be associated to an actual malfunction of the link, this mode is recommended only in certain scenarios (typically only on point-to-point links where no communication failure between two neighbors is admissible).

◆ Operation State – Shows the UDLD operational state (Disabled, Link down, Link up, Advertisement, Detection, Disabled port, Advertisement - Single neighbor, Advertisement - Multiple neighbors)

◆ Port State – Shows the UDLD port state (Unknown, Bidirectional, Unidirectional, Transmit-to-receive loop, Mismatch with neighbor state reported, Neighbor's echo is empty) The state is Unknown if the link is down or not connected to a UDLD-capable device. The state is Bidirectional if the link has a normal two-way connection to a UDLD-capable device. All other states indicate mis-wiring.

◆ Message Interval – The interval between UDLD probe messages used for the indicated operational state.

◆ Detection Interval – The period the switch remains in detection state after discovering a neighbor.

Configure Interface Switch Management > UDLD > Configure Interface Stacking Unit: 1

Port Configuration List Total: 28 1 2 3

Port	UDLD	Aggressive Mode	Operation State	Port State	Message Interval (seconds)	Detection Interval (seconds)
1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Disabled	Unknown	7	5
2	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Disabled	Unknown	7	5
3	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Disabled	Unknown	7	5
4	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Disabled	Unknown	7	5
5	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Disabled	Unknown	7	5
6	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Disabled	Unknown	7	5
7	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Disabled	Unknown	7	5
8	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Disabled	Unknown	7	5
9	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Disabled	Unknown	7	5
10	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Disabled	Unknown	7	5

Show Information

Switch Management > UDLD > Show Information page is used to show UDLD neighbor information, including neighbor state, expiration time, and protocol intervals.

Parameters

These parameters are displayed:

◆ Port – Port identifier. (Range: 1-28/52)

- ◆ Entry – Table entry number uniquely identifying the neighbor device discovered by UDLD on a port interface.
- ◆ Device ID – Device identifier of neighbor sending the UDLD packet.
- ◆ Port ID – The physical port the UDLD packet is sent from.
- ◆ Device Name – The device name of this neighbor.
- ◆ Neighbor State – Link status of neighbor device (Values: unknown, neighborsEchoIsEmpty, bidirectional, mismatchWithneighborStateReported, unidirectional).
- ◆ Expire – The amount of time remaining before this entry will expire.
- ◆ Message Interval – The interval between UDLD probe messages for ports in advertisement phase.
- ◆ Detection Interval – The period the switch remains in detection state after discovering a neighbor.

Show Information Switch Management > UDLD > Show Information Stacking Unit: 1

Port 1

UDLD Neighbor List Total: 0

Entry	Device ID	Port ID	Device Name	Neighbor State	Expire (seconds)	Message Interval (seconds)	Detection Interval (seconds)
Total: 0							

Congestion Control

The switch can set the maximum upload or download data transfer rate for any port. It can also control traffic storms by setting a maximum threshold for broadcast traffic or multicast traffic. It can also set bounding thresholds for broadcast and multicast storms which can be used to automatically trigger rate limits or to shut down a port.

Rate Limit

Interface > Congestion Control > Rate Limit page is used to apply rate limiting to ingress or egress ports. This function allows the network manager to control the maximum rate for traffic received or transmitted on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity.

Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

PARAMETERS

These parameters are displayed:

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

(Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports; 64 - 10,000,000 kbits per second for 10 Gigabit Ethernet ports)

Rate Limit Switch Management > Congestion Control > Rate Limit Stacking Unit : 1

Interface Port Trunk

Port Rate Limit List Total: 28 1 2 3

Port	Type	Input		Output	
		Status	Rate (kbits/sec) (64-10000000)	Status	Rate (kbits/sec) (64-10000000)
1	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>
2	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>
3	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>
4	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>
5	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>
6	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>
7	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>
8	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="1000000"/>

Storm Control

Interface > Congestion Control > Storm Control page is used to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt. You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

COMMAND USAGE

- ◆ Broadcast Storm Control is enabled by default.
- ◆ When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.
- ◆ Traffic storms can be controlled at the hardware level using Storm Control or at the software level using Automatic Traffic Control which triggers various control responses. However, only one of these control types can be applied to a port. Enabling hardware-level storm control on a port will disable automatic storm control on that port.
- ◆ The rate limits set by this function are also used by automatic storm control when the control response is set to rate control on the Auto Traffic Control (Configure Interface) page.
- ◆ Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 5000 Kbps, and the rate limit is set to 100000 Kbps on a Gigabit Ethernet port. Since 200000 Kbps is 1/5 of line speed, the received rate will actually be 1000 Kbps, or 1/5 of the 5000 Kbps limit set by the storm control command. It is therefore not advisable to use both of these commands on the same interface.

PARAMETERS

These parameters are displayed:

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

Storm Control Stacking Unit

Switch Management > Congestion Control > Storm Control

Interface Port Trunk

Port Storm Control List Total: 28 1 2 3

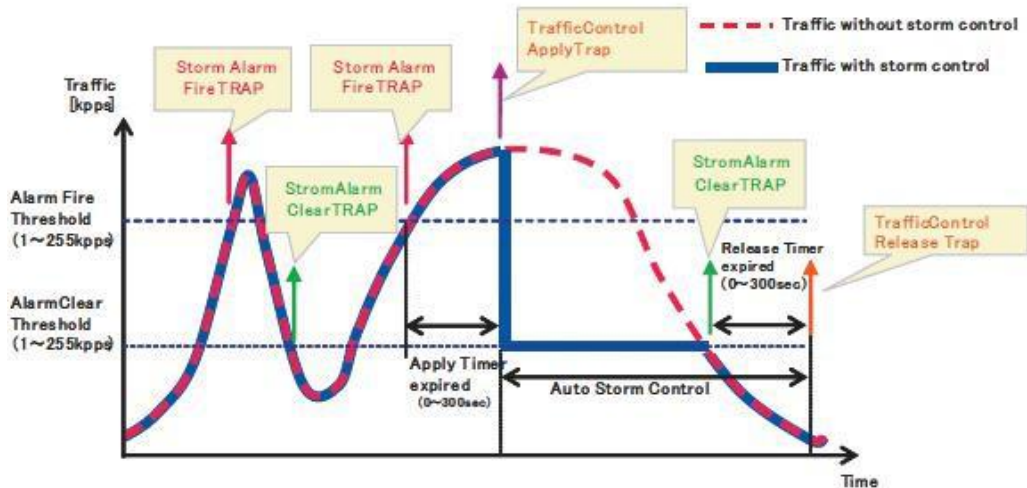
Port	Type	Unknown Unicast		Multicast		Broadcast	
		Status	Rate (packets/sec) (500-14880000)	Status	Rate (packets/sec) (500-14880000)	Status	Rate (packets/sec) (500-14880000)
1	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="500"/>
2	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="500"/>
3	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="500"/>
4	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="500"/>
5	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="500"/>
6	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="500"/>
7	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="500"/>
8	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="500"/>
9	1000BASE SFP	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="262143"/>	<input checked="" type="checkbox"/> Enabled	<input type="text" value="500"/>

Auto Traffic Control

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

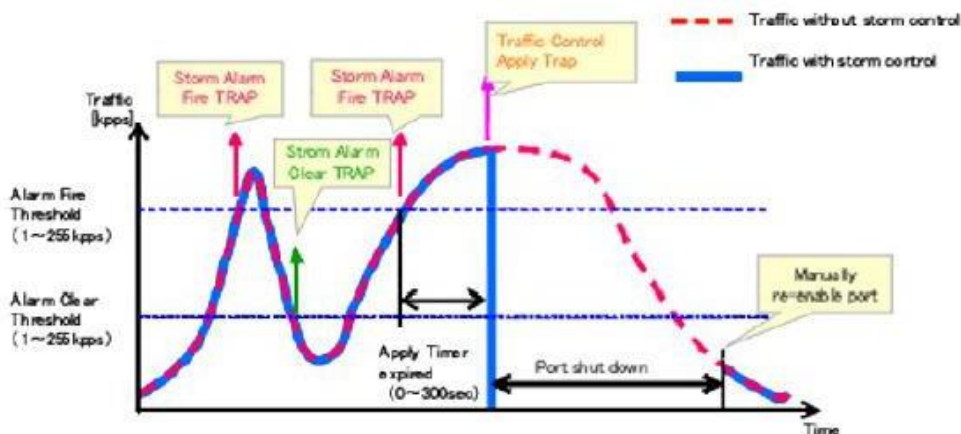
COMMAND USAGE

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



The key elements of this diagram are described below:

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



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

Functional Limitations

Automatic storm control is a software level control function. Traffic storms can also be

controlled at the hardware level using Port Broadcast Control or Port Multicast Control (as described). However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

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

COMMAND USAGE

◆ After the apply timer expires, the settings in the Interface > Congestion Control > Auto Traffic Control (Interface) page are used to determine if a control action will be triggered (as configured under the Action field) or a trap message sent (as configured under the Trap Storm Fire field).

◆ The release timer only applies to a Rate Control response set in the Action field of the ATC (Interface Configuration) page. When a port has been shut down by a control response, it must be manually re-enabled using the Manual Control Release .

PARAMETERS

These parameters are displayed in the web interface:

◆ **Broadcast Apply Timer** – The interval after the upper threshold has been exceeded at which to apply the control response to broadcast storms. (Range: 1-300 seconds; Default: 300 seconds)

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

◆ **Multicast Apply Timer** – The interval after the upper threshold has been exceeded at which to apply the control response to multicast storms. (Range: 1-300 seconds; Default: 300 seconds)

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

Auto Traffic Control
Switch Management > Congestion Control > Auto Traffic Control

Global
Interface

Broadcast Apply Timer (5-300)	<input type="text" value="300"/>	sec
Broadcast Release Timer (5-900)	<input type="text" value="900"/>	sec
Multicast Apply Timer (5-300)	<input type="text" value="300"/>	sec
Multicast Release Timer (5-900)	<input type="text" value="900"/>	sec

Interface > Congestion Control > Auto Traffic Control (Interface) page is used to set the

storm control mode (broadcast or multicast), the traffic thresholds, the control response, to automatically release a response of rate limiting, or to send related SNMP trap messages.

PARAMETERS

These parameters are displayed in the web interface:

◆ **Storm Control** – Specifies automatic storm control for broadcast traffic or multicast traffic.

◆ **Port** – Port identifier.

◆ **State** – Enables automatic traffic control for broadcast or multicast storms. (Default: Disabled)

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

◆ **Action** – When the Alarm Fire Threshold (upper threshold) is exceeded and the apply timer expires, one of the following control responses will be triggered.

■ **Rate Control** – The rate of ingress traffic is limited to the level set by the Alarm Clear Threshold. Rate limiting is discontinued only after the traffic rate has fallen beneath the Alarm Clear Threshold (lower threshold), and the release timer has expired. (This is the default response.)

■ **Shutdown** – The port is administratively disabled. A port disabled by automatic traffic control can only be manually re-enabled using the Manual Control Release attribute.

◆ **Auto Release Control** – Automatically stops a traffic control response of rate limiting when traffic falls below the alarm clear threshold and the release timer.

When traffic control stops, the event is logged by the system and a Traffic Release Trap can be sent. (Default: Disabled)

If automatic control release is not enabled and a control response of rate limiting has been triggered, you can manually stop the rate limiting response using the Manual Control Release attribute. If the control response has shut down a port, it can also be re-enabled using Manual Control Release.

◆ **Alarm Fire Threshold** – The upper threshold for ingress traffic beyond which a storm control response is triggered after the Apply Timer expires. (Range: 1-255 kilo-packets per second; Default: 128 Kpps) Once the traffic rate exceeds the upper threshold and the Apply Timer expires, a trap message will be sent if configured by the Trap Storm Fire attribute.

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

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

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

Auto Traffic Control Switch Management > Congestion Control > Auto Traffic Control Stacking Unit:

Global Interface

Storm Control Broadcast Multicast

Auto Traffic Control Broadcast List Total: 28 1 2 3

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

Stacking

Switch stacking technology allows the network engineer to make that stack of physical switches act like one switch. This technology allows for enhancements in all areas of network design, including high availability, scalability, management, and maintenance.

Master election strategy:

- Top priority - The switch gets ready to work firstly.
- Secondary priority - The switch setting master button.
- Lowest priority - The switch with the lowest mac adress.

Configure Master Button

Switch Management > Stacking > Configure Master Button page is used to set master button

on the switch.

Configure Master Button Switch Management > Stacking > Configure Master Button

Master Button List Total: 1

Unit	Master Button
1	<input type="checkbox"/> Enabled

Configure Stacking Button

Switch Management > Stacking > Configure Stacking Button page is used to convert switch mode between stacking and non-stacking.

Configure Stacking Button Switch Management > Stacking > Configure Stacking Button

Status Enabled

Current Status Enabled

Stacking Up Port 27

Stacking Down Port 28

Note: When the configured status is different from the current status, the configured status takes effect after reboot.

Renumber

Switch Management > Stacking > Renumber page is used to reset unit numbers.

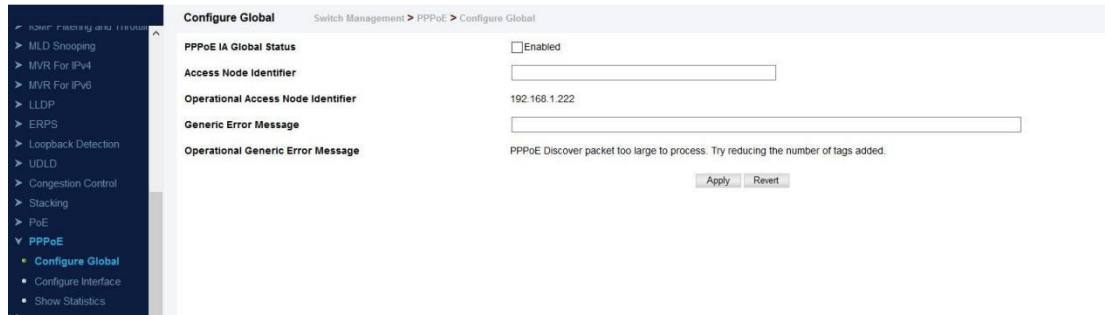
Renumber Switch Management > Stacking > Renumber

Click this button to reset the unit numbers.

PPPoE

Configure Global

Switch Management > PPPoE > Configure Global page is used to configure the global parameters.



◆ **PPPoE IA Global Status** – Enables the PPPoE Intermediate Agent globally on the switch. (Default: Disabled)

Note that PPPoE IA must be enabled globally before it can be enabled on an interface.

◆ **Access Node Identifier** – String identifying this switch as an PPPoE IA to the PPPoE server. (Range: 1-48 ASCII characters; Default: IP address of first IPv4 interface on the switch.) The switch uses the access-node-identifier to generate the circuit-id for PPPoE discovery stage packets sent to the BRAS, but does not modify the source or destination MAC address of these PPPoE discovery packets. These messages are forwarded to all trusted ports designated on the Configure Interface page.

◆ **Operational Access Node Identifier** – The configured access node identifier.

◆ **Generic Error Message** – An error message notifying the sender that the PPPoE Discovery packet was too large. (Range: 0-127; Default: PPPoE Discover packet too large to process. Try reducing the number of tags added.)

◆ **Operational Generic Error Message** – The configured generic error message.

Configure Interface

Switch Management > PPPoE > Configure Global page is used to configure the parameters of PPPoE interface.

Port	PPPoE IA Status	Trust Status	Vendor Tag Strip	Circuit ID	Operation Circuit ID	Remote ID	Operation Remote ID	Remote ID Delimiter	Delimiter ASCII (0-255)
3	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled		1/3 vid		EC-D6-8A-33-A2-81	<input type="checkbox"/> Enabled	35
4	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled		1/4 vid		EC-D6-8A-33-A2-82	<input type="checkbox"/> Enabled	35
5	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled		1/5 vid		EC-D6-8A-33-A2-83	<input type="checkbox"/> Enabled	35
6	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled		1/6 vid		EC-D6-8A-33-A2-84	<input type="checkbox"/> Enabled	35
7	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled		1/7 vid		EC-D6-8A-33-A2-85	<input type="checkbox"/> Enabled	35
8	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled		1/8 vid		EC-D6-8A-33-A2-86	<input type="checkbox"/> Enabled	35
9	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled		1/9 vid		EC-D6-8A-33-A2-87	<input type="checkbox"/> Enabled	35
10	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled		1/10 vid		EC-D6-8A-33-A2-88	<input type="checkbox"/> Enabled	35
11	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled		1/11 vid		EC-D6-8A-33-A2-89	<input type="checkbox"/> Enabled	35
12	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled		1/12 vid		EC-D6-8A-33-A2-8A	<input type="checkbox"/> Enabled	35

◆ **PPPoE IA Status** – Enables the PPPoE IA on an interface. (Default: Disabled) Note that PPPoE IA must also be enabled globally on the switch for this command to take effect.

◆ **Trust Status** – Sets an interface to trusted mode to indicate that it is connected to a PPPoE server. (Default: Disabled)

■ Set any interfaces connecting the switch to a PPPoE Server as trusted. Interfaces that connect the switch to users (PPPoE clients) should be set as untrusted.

■ At least one trusted interface must be configured on the switch for the PPPoE IA to function.

◆ **Vendor Tag Strip** – Enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server. (Default: Disabled) This parameter only applies to trusted interfaces. It is used to strip off vendorspecific tags (which carry subscriber and line identification information) in PPPoE Discovery packets received from an upstream PPPoE server before forwarding them to a user.

◆ **Circuit ID** – String identifying the circuit identifier (or interface) on this switch to which the user is connected. (Range: 1-10 ASCII characters; Default: Unit/ Port:VLAN-ID, or 0/Trunk-ID:VLAN-ID)

■ The PPPoE server extracts the Line-ID tag from PPPoE discovery stage messages, and uses the Circuit-ID field of that tag as a NAS-Port-ID attribute in AAA access and accounting requests.

■ The switch intercepts PPPoE discovery frames from the client and inserts a unique line identifier using the PPPoE Vendor-Specific tag (0x0105) to PPPoE Active Discovery Initiation (PADI) and Request (PADR) packets. The switch then forwards these packets to the PPPoE server. The tag contains the Line-ID of the customer line over which the discovery packet was received, entering the switch (or access node) where the intermediate agent resides.

■ Outgoing PAD Offer (PADO) and Session-confirmation (PADS) packets sent from the PPPoE Server include the Circuit-ID tag inserted by the switch, and should be stripped out of PADO and PADS packets which are to be passed directly to end-node clients.

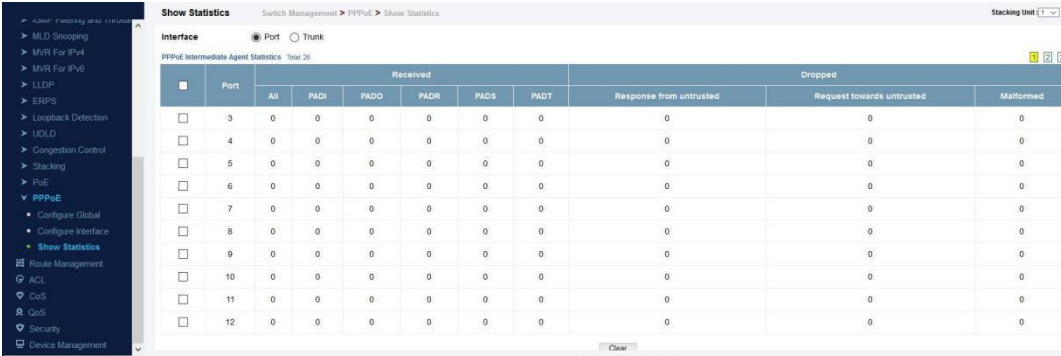
◆ **Operational Circuit ID** – The configured circuit identifier.

◆ **Remote ID** – String identifying the remote identifier (or interface) on this switch to which the user is connected. (Range: 1-63 ASCII characters; Default: Port MACaddress)

◆ **Operational Remote ID** – The configured circuit identifier.

Show Statistics

Switch Management > PPPoE > Show Statistics page is used to display counters.



Interface	Port	Received						Dropped		
		All	PADI	PADO	PADR	PADS	PADT	Response from untrusted	Request towards untrusted	Malformed
<input type="checkbox"/>	3	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	4	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	5	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	6	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	7	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	8	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	9	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	10	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	11	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	12	0	0	0	0	0	0	0	0	0

Route Management

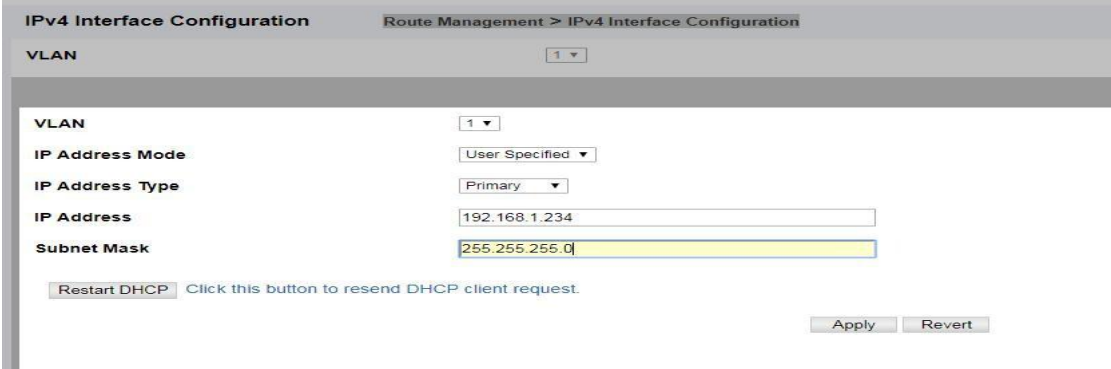
IPv4 Interface Configuration

This section describes how to configure an IPv4 interface for management access over the network. Route Management > IPv4 Interface Configuration page is used to configure an IPv4 address for the switch. An IPv4 address is obtained via DHCP by default for VLAN 1. To configure a static address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment. You can direct the device to obtain an address from a BOOTP or DHCP server, or manually configure a static IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – ID of the configured VLAN (1-4093). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.
- ◆ **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (User Specified), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP/BOOTP responses can include the IP address, subnet mask, and default gateway. (Default: DHCP)
- ◆ **IP Address Type** – Specifies a primary or secondary IP address. An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. For initial configuration, set this parameter to Primary. (Options: Primary, Secondary; Default: Primary) Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router or switch in a network segment uses a secondary address, all other routers/switches in that segment must also use a secondary address from the same network or subnet address space.
- ◆ **IP Address** – Address of the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: None)
- ◆ **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: None)
- ◆ **Restart DHCP** – Requests a new IP address from the DHCP server.



The screenshot shows the 'IPv4 Interface Configuration' page. At the top, there is a breadcrumb trail: 'Route Management > IPv4 Interface Configuration'. Below this, there is a 'VLAN' dropdown menu set to '1'. The main configuration area includes:

- VLAN:** 1
- IP Address Mode:** User Specified
- IP Address Type:** Primary
- IP Address:** 192.168.1.234
- Subnet Mask:** 255.255.255.0

 There is a 'Restart DHCP' button with the text 'Click this button to resend DHCP client request.' At the bottom right, there are 'Apply' and 'Revert' buttons.

IPv6 Interface Configuration

This section describes how to configure an IPv6 interface for management access over the network.

Configure Global

Route Management > IPv6 Interface Configuration > Configure Global page is used to configure an IPv6 default gateway for the switch.

PARAMETERS

These parameters are displayed:

- ◆ **Default Gateway** – Sets the IPv6 address of the default next hop router.
- 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.



The screenshot shows the 'Configure Global' page. At the top, there is a breadcrumb trail: 'Route Management > IPv6 Interface Configuration > Configure Global'. Below this, there is a 'Default Gateway' text input field containing the value '1024::1234'. At the bottom right, there are 'Apply' and 'Revert' buttons.

Configure Interface

Route Management > IPv6 Interface Configuration > Configure Interface page is used to configure general IPv6 settings for the selected VLAN, including auto-configuration of a global unicast address, explicit configuration of a link local interface address, the MTU size, and neighbor discovery protocol settings for duplicate address detection and the neighbor solicitation interval.

COMMAND USAGE

- ◆ The switch must always be configured with a link-local address. The switch's address auto-configuration function will automatically create a link-local address, as well as an IPv6 global address if router advertisements are detected on the local interface.

◆ The option to explicitly enable IPv6 will also create a link-local address, but will not generate a global IPv6 address if auto-configuration is not enabled. In this case, you must manually configure an address.

◆ IPv6 Neighbor Discovery Protocol supersedes IPv4 Address Resolution Protocol in IPv6 networks. IPv6 nodes on the same network segment use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors. The key parameters used to facilitate this process are the number of attempts made to verify whether or not a duplicate address exists on the same network segment, and the interval between neighbor solicitations used to verify reachability information.

PARAMETERS

These parameters are displayed:

VLAN Mode

◆ **VLAN** – ID of a configured VLAN which is to be used for management access. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)

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

■ If the router advertisements have the “other stateful configuration” flag set, the switch will attempt to acquire other non-address configuration information (such as a default gateway).

■ If auto-configuration is not selected, then an address must be manually configured using the Add Interface page described below.

◆ **Enable IPv6 Explicitly** – Enables IPv6 on an interface. Note that when an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed. (Default: Disabled) Disabling this parameter does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

◆ **MTU** – Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. (Range: 1280-65535 bytes; Default: 1500 bytes)

■ The maximum value set in this field cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.

■ IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.

■ All devices on the same physical medium must use the same MTU in order to operate correctly.

■ IPv6 must be enabled on an interface before the MTU can be set. If an IPv6 address has not been assigned to the switch, “N/A” is displayed in the MTU field.

◆ **ND DAD Attempts** – The number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. (Range: 0-600, Default: 3)

■ Configuring a value of 0 disables duplicate address detection.

■ Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.

■ Duplicate address detection is stopped on any interface that has been suspended.

While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.

■ An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface’s link-local address, the other IPv6 addresses remain in a “tentative” state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.

■ If a duplicate address is detected, it is set to “duplicate” state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in “duplicate” state.

■ If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

◆ **ND NS Interval** – The interval between transmitting IPv6 neighbor solicitation messages on an interface. (Range: 1000-3600000 milliseconds; Default: 1000 milliseconds is used for neighbor discovery operations, 0 milliseconds is advertised in router advertisements. This attribute specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

◆ **ND Reachable-Time** – The amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. (Range: 0-3600000 milliseconds; Default: 30000 milliseconds)

◆ **Interface** – Shows port or trunk configuration page.

◆ **RA Guard** – Blocks incoming Router Advertisement and Router Redirect packets. (Default: Disabled)

IPv6 Router Advertisements (RA) convey information that enables nodes to auto-configure on the network. This information may include the default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, note that unintended misconfigurations, or possibly malicious attacks on the network, may lead to bogus RAs being sent, which in turn can cause operational problems for hosts on the network. RA Guard can be used to block RAs and Router Redirect (RR) messages on the specified interface. Determine which interfaces are connected to known routers, and enable RA Guard on all other untrusted interfaces.

Configure Interface Route Management > IPv6 Interface Configuration > Configure Interface

Mode VLAN RA Guard

VLAN

Enable IPv6 Explicitly Enabled

MTU (1280-65535) bytes

ND DAD Attempts (0-600)

ND NS Interval (1000-3600000) ms

ND Reachable-Time (0-3600000) ms

IPv6 Address

Route Management > IPv6 Interface Configuration > IPv6 Address page is used to configure an IPv6 interface for management access over the network.

COMMAND USAGE

- ◆ All IPv6 addresses must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ The switch must always be configured with a link-local address. Therefore any configuration process that enables IPv6 functionality, or assigns a global unicast address to the switch, including address autoconfiguration or explicitly enabling IPv6, will also automatically generate a link-local unicast address. The prefix length for a link-local address is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier (i.e., the physical MAC address). Alternatively, you can manually configure the link-local address by entering the full address with the network prefix in the range of FE80~FEBF.
- ◆ To connect to a larger network with multiple subnets, you must configure a global unicast address. There are several alternatives to configuring this address type:
 - The global unicast address can be automatically configured by taking the network prefix from router advertisements observed on the local interface, and using the modified EUI-64 form of the interface identifier to automatically create the host portion of the address.
 - It can be manually configured by specifying the entire network prefix and prefix length, and using the EUI-64 form of the interface identifier to automatically create the low-order 64 bits in the host portion of the address.
 - You can also manually configure the global unicast address by entering the full address and prefix length.
- ◆ You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.
- ◆ If a duplicate link-local address is detected on the local segment, this interface is disabled and a warning message displayed on the console. If a duplicate global unicast address is detected on the network, the address is disabled on this interface and a warning message

displayed on the console.

◆ When an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed.

PARAMETERS

These parameters are displayed:

◆ **VLAN** – ID of a configured VLAN which is to be used for management access. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)

◆ **Address Type** – Defines the address type configured for this interface.

■ **Global** – Configures an IPv6 global unicast address with a full IPv6 address including the network prefix and host address bits, followed by a forward slash, and a decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

■ **EUI-64** (Extended Universal Identifier) – Configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits.

■ When using EUI-64 format for the low-order 64 bits in the host portion of the address, the value entered in the IPv6 Address field includes the network portion of the address, and the prefix length indicates how many contiguous bits (starting at the left) of the address comprise the prefix (i.e., the network portion of the address). Note that the value specified in the IPv6 Address field may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the bits used in the network portion of the address will take precedence over the interface identifier.

■ IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device's MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address. For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., organizationally unique identifier, or company identifier) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

■ This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

■ **Link Local** – Configures an IPv6 link-local address.

■ The address prefix must be in the range of FE80~FEBF.

■ You can configure only one link-local address per interface.

■ The specified address replaces a link-local address that was automatically generated for the interface.

◆ **IPv6 Address** – IPv6 address assigned to this interface.

IPv6 Address Route Management > IPv6 Interface Configuration > IPv6 Address

VLAN

VLAN

Address Type

IPv6 Address

IPv6 Address Route Management > IPv6 Interface Configuration > IPv6 Address

VLAN

IPv6 Address List Total: 2

	IPv6 Address Type	IPv6 Address	Configuration Mode
<input type="checkbox"/>	Global	2001::2001/64	Manual
<input type="checkbox"/>	Link Local	fe80::200:3fff:fe00:2%1/64	Auto

Show IPv6 Neighbor Cache

Route Management > IPv6 Interface Configuration > Show IPv6 Neighbor Cache page is used to display the IPv6 addresses detected for neighbor devices.

PARAMETERS

These parameters are displayed:

Field	Description
IPv6 Address	IPv6 address of neighbor
Age	The time since the address was verified as reachable (in seconds). A static entry is indicated by the value "Permanent."
Link-layer Addr	Physical layer MAC address.
State	The following states are used for dynamic entries:
	◆ INCMP (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message.
	◆ REACH (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets.
	◆ STALE - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent.
◆ DELAY - More than the ReachableTime interval has elapsed since	

	<p>the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will send a neighbor solicitation message and change the state to PROBE.</p>
	<p>PROBE - A reachability confirmation is actively sought by</p> <ul style="list-style-type: none"> ◆ resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received.
	The following states are used for static entries:
	<ul style="list-style-type: none"> ◆ INCOMP (Incomplete)-The interface for this entry is down.
	<ul style="list-style-type: none"> ◆ REACH (Reachable) - The interface for this entry is up. ◆ Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.
VLAN	VLAN interface from which the address was reached.

Route Management > IPv6 Interface Configuration > Show IPv6 Neighbor Cache

Current Neighbor Cache Table Total: 16

IPv6 Address	Age	Link-layer Address	State	VLAN
2001::1b6:faa4:5c77:800e	19	54-E1-AD-FA-7A-7D	Stale	1
2001::2911:031:909f:203b	16	8C-16-45-15-56-8F	Stale	1
2001::7045:4f37:ebbc:90d0	19	6C-4B-90-15-5C-89	Stale	1
2001::943a:427b:9640:d2e3	14	94-C6-91-21-CF-9A	Stale	1
2001::9944:c05:6493:6082	14	6C-4B-90-15-F7-62	Stale	1
2001::ad5:bccf:359d:7f2b	19	54-E1-AD-FA-67-EA	Stale	1
fe80::594b:3a82:9c92:a221	14	6C-4B-90-15-F6-DF	Stale	1
fe80::60fa:1c7f:cea1:2385	14	94-C6-91-21-CF-9A	Stale	1
fe80::a134:1bd2:3a49:d33c	14	8C-16-45-15-66-8F	Stale	1
fe80::a401:1af2:3749:9f14	14	00-1B-21-BB-2B-7C	Stale	1

Show Statistics

Route Management > IPv6 Interface Configuration > Show Statistics page is used to display statistics about IPv6 traffic passing through this switch.

COMMAND USAGE

This switch provides statistics for the following traffic types:

- ◆ **IPv6** – The Internet Protocol for Version 6 addresses provides a mechanism for transmitting blocks of data (often called packets or frames) from a source to a destination, where these network devices (that is, hosts) are identified by fixed length addresses. The Internet Protocol also provides for fragmentation and reassembly of long packets, if necessary, for transmission through “small packet” networks.

- ◆ **ICMPv6** – Internet Control Message Protocol for Version 6 addresses is a network layer protocol that transmits message packets to report errors in processing IPv6 packets. ICMP is therefore an integral part of the Internet Protocol. ICMP messages may be used to report various situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. ICMP is also used by routers to feed back information about more suitable routes (that is, the next hop router) to use for a specific

destination.

◆ **UDP** – User Datagram Protocol provides a datagram mode of packet switched communications. It uses IP as the underlying transport mechanism, providing access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

PARAMETERS

These parameters are displayed:

Field	Description
IPv6 Statistics	
<i>IPv6 Received</i>	
Total	The total number of input datagrams received by the interface, including those received in error.
Header Errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, IPv6 options, etc.
Too Big Errors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
No Routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
Address Errors	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Unknown Protocols	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
Truncated Packets	The number of input datagrams discarded because datagram frame didn't carry enough data.
Discards	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
Delivers	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the

	datagrams.
Reassembly Request Datagrams	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
Reassembly Succeeded	The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
Reassembly Failed	The number of failures detected by the IPv6 re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
IPv6 Transmitted	
Forwards Datagrams	The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.”
Requests	The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in <code>ipv6IfStatsOutForwDatagrams</code> .
Discards	The number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in <code>ipv6IfStatsOutForwDatagrams</code> if any such packets met this (discretionary) discard criterion.
No Routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
Generated Fragments	The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
Fragment Succeeded	The number of IPv6 datagrams that have been successfully fragmented at this output interface.
Fragment Failed	The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.

ICMPv6 Statistics	
ICMPv6 received	
Input	The total number of ICMP messages received by the interface which includes all those counted by ipv6IcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
Errors	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP check sums, bad length, etc.).
Destination Unreachable Messages	The number of ICMP Destination Unreachable messages received by the interface.
Packet Too Big Messages	The number of ICMP Packet Too Big messages received by the interface.
Time Exceeded Messages	The number of ICMP Time Exceeded messages received by the interface.
Parameter Problem Messages	The number of ICMP Parameter Problem messages received by the interface.
Echo Request Messages	The number of ICMP Echo (request) messages received by the interface.
Echo Reply Messages	The number of ICMP Echo Reply messages received by the interface.
Router Solicit Messages	The number of ICMP Router Solicit messages received by the interface.
Router Advertisement Messages	The number of ICMP Router Advertisement messages received by the interface.
Neighbor Solicit Messages	The number of ICMP Neighbor Solicit messages received by the interface.
Neighbor Advertisement Messages	The number of ICMP Neighbor Advertisement messages received by the interface.
Redirect Messages	The number of Redirect messages received by the interface.
Group Membership Query Messages	The number of ICMPv6 Group Membership Query messages received by the interface.
Group Membership Response Messages	The number of ICMPv6 Group Membership Response messages received by the interface.
Group Membership Reduction Messages	The number of ICMPv6 Group Membership Reduction messages received by the interface.
Multicast Listener Discovery Version 2 Reports	The number of MLDv2 reports received by the interface.
ICMPv6 Transmitted	

Output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
Destination Unreachable Messages	The number of ICMP Destination Unreachable messages sent by the interface.
Packet Too Big Messages	The number of ICMP Packet Too Big messages sent by the interface.
Time Exceeded Messages	The number of ICMP Time Exceeded messages sent by the interface.
Parameter Problem Message	The number of ICMP Parameter Problem messages sent by the interface.
Echo Request Messages	The number of ICMP Echo (request) messages sent by the interface.
Echo Reply Messages	The number of ICMP Echo Reply messages sent by the interface.
Router Solicit Messages	The number of ICMP Router Solicitation messages sent by the interface.
Router Advertisement Messages	The number of ICMP Router Advertisement messages sent by the interface.
Neighbor Solicit Messages	The number of ICMP Neighbor Solicit messages sent by the interface.
Neighbor Advertisement Messages	The number of ICMP Router Advertisement messages sent by the interface.
Redirect Messages	The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
Group Membership Query Messages	The number of ICMPv6 Group Membership Query messages sent by the interface.
Group Membership Response Messages	The number of ICMPv6 Group Membership Response messages sent.
Group Membership Reduction Messages	The number of ICMPv6 Group Membership Reduction messages sent.
Multicast Listener Discovery Version 2 Reports	The number of MLDv2 reports sent by the interface.
Input	The total number of UDP datagrams delivered to UDP users.
No Port Errors	The total number of received UDP datagrams for which there was no application at the destination port.
Other Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Output	The total number of UDP datagrams sent from this entity.

Show Statistics Route Management > IPv6 Interface Configuration > Show Statistics

Type IPv6 ICMPv6 UDP

IPv6 Statistics			
Total Received	191	Received Reassembly Succeeded	0
Received Header Errors	0	Received Reassembly Failed	0
Received Too Big Errors	0	Transmitted Forwards Datagrams	0
Received No Routes	60	Transmitted Requests	122
Received Address Errors	0	Transmitted Discards	0
Received Unknown Protocols	0	Transmitted No Routes	24
Received Truncated Packets	0	Transmitted Generated Fragments	0
Received Discards	0	Transmitted Fragment Succeeded	0
Received Delivers	100	Transmitted Fragment Failed	0
Received Reassembly Request Datagrams	0		

Show MTU

Route Management > IPv6 Interface Configuration > Show MTU page is used to display the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

PARAMETERS

These parameters are displayed:

Field	Description
MTU	Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path.
Since	Time since an ICMP packet-too-big message was received from this destination.
Destination Address	Address which sent an ICMP packet-too-big message.

Show MTU Route Management > IPv6 Interface Configuration > Show MTU

MTU Table Total: 0

MTU	Since	Destination Address
1400	00:04:21	5000:1::3
1280	00:04:50	FE80::203:A0FF:FED6:141D

ARP

If IP routing is enabled, the router uses its routing tables to make routing decisions, and uses Address Resolution Protocol (ARP) to forward traffic from one hop to the next. ARP is used to map an IP address to a physical layer (i.e., MAC) address. When an IP frame is received by this router (or any standards-based router), it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the router writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the next hop. IP traffic passes along the path to its final destination in this way, with each routing device mapping the destination IP address to the MAC address of the next hop toward the recipient, until the packet is delivered to the final destination.

If there is no entry for an IP address in the ARP cache, the router will broadcast an ARP

request packet to all devices on the network. The ARP request contains the following fields similar to that shown in this example:

destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC address field and send the message back to the source hardware address. When the source device receives a reply, it writes the destination IP address and corresponding MAC address into its cache, and forwards the IP traffic on to the next hop. As long as this entry has not timed out, the router will be able forward traffic directly to the next hop for this destination without having to broadcast another ARP request. Also, if the switch receives a request for its own IP address, it will send back a response, and also cache the MAC of the source device's IP address.

Configure General

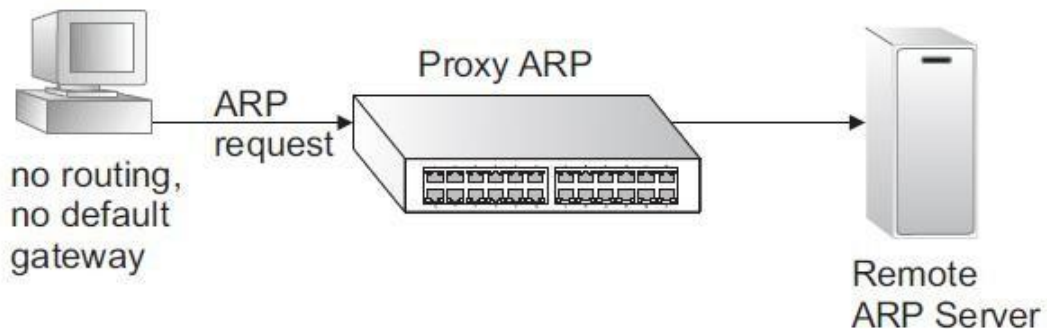
Route Management > ARP > Configure General page is used to specify the timeout for ARP cache entries, or to enable Proxy ARP for specific VLAN interfaces.

COMMAND USAGE

Proxy ARP

When a node in the attached sub-network does not have routing or a default gateway configured, Proxy ARP can be used to forward ARP requests to a remote sub-network. When the router receives an ARP request for a remote network and Proxy ARP is enabled, it determines if it has the best route to the remote network, and then answers the ARP request by sending its own MAC address to the requesting node. That node then sends traffic to the router, which in turn uses its own routing table to forward the traffic to the remote destination.

Proxy ARP



PARAMETERS

These parameters are displayed:

◆ **Timeout** – Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes) The ARP aging timeout can be set for any configured VLAN.

The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table. When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.

◆ **Proxy ARP** – Enables or disables Proxy ARP for specified VLAN interfaces, allowing a non-routing device to determine the MAC address of a host on another subnet or network. (Default: Disabled)

End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices. Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

WEB INTERFACE

To configure the timeout for the ARP cache or to enable Proxy ARP for a VLAN (i.e., IP subnetwork):

1. Click Route Management > ARP > Configure General.
2. Set the timeout to a suitable value for the ARP cache, or enable Proxy ARP for subnetworks that do not have routing or a default gateway.
3. Click Apply.

Configure General		Route Management > ARP > Configure General	
Timeout (300-86400)	<input type="text" value="1200"/>	sec	
Proxy ARP			
VLAN	<input type="text" value="1"/>		
Status	<input type="checkbox"/>	Enabled	
		<input type="button" value="Apply"/>	<input type="button" value="Revert"/>

Static ARP

For devices that do not respond to ARP requests or do not respond in a timely manner, traffic will be dropped because the IP address cannot be mapped to a physical address. If this occurs, use the Route Management > ARP > Static Arp page to manually map an IP address to the corresponding physical address in the ARP cache.

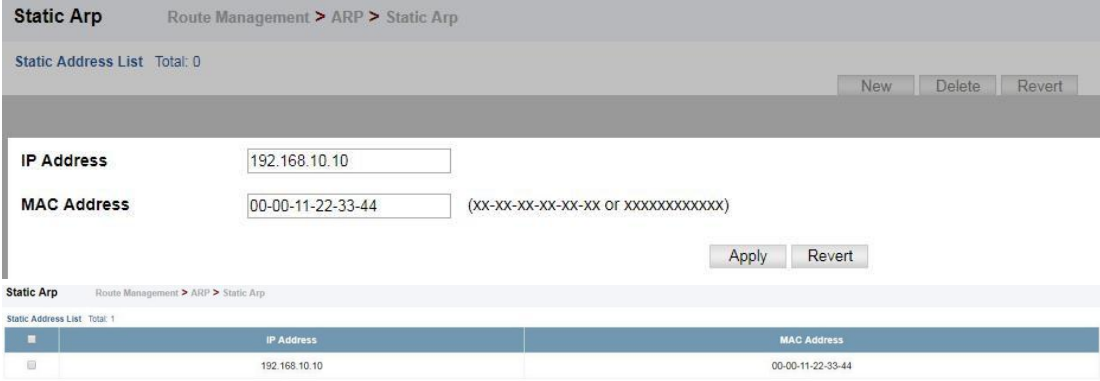
COMMAND USAGE

- ◆ The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (that is, Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- ◆ You can define up to 128 static entries in the ARP cache.
- ◆ A static entry may need to be used if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.
- ◆ Static entries will not be aged out or deleted when power is reset. You can only remove a static entry via the configuration interface.
- ◆ Static entries are only displayed on the Show page for VLANs that are up. In other words, static entries are only displayed when configured for the IP subnet of an existing VLAN, and that VLAN is linked up.

Parameters

These parameters are displayed:

- ◆ **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)
- ◆ **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xxxx-xx-xx-xx)



Static Arp Route Management > ARP > Static Arp

Static Address List Total: 0 New Delete Revert

IP Address

MAC Address (XX-XX-XX-XX-XX-XX OF XXXXXXXXXXXXX)

Apply Revert

Static Arp Route Management > ARP > Static Arp

Static Address List Total: 1

	IP Address	MAC Address
<input type="checkbox"/>	192.168.10.10	00-00-11-22-33-44

New Delete Revert

Show Information

Route Management > ARP > Show Information page is used to display dynamic or local entries in the ARP cache and statistics for ARP messages crossing all interfaces on this router. The ARP cache contains static entries, and entries for local interfaces, including subnet, host, and broadcast addresses. However, most entries will be dynamically learned through replies to broadcast messages.

Show Information Route Management > ARP > Show Information

ARP Address
 Statistics

ARP Address List Total: 4

IP Address	MAC Address	Type	Interface
192.168.1.1	E0-C6-3C-CE-C2-08	dynamic	VLAN 1
192.168.1.64	6C-4B-90-15-5C-A9	dynamic	VLAN 1
192.168.1.98	00-00-03-00-00-02	other	VLAN 1
192.168.1.102	54-E1-AD-FA-7A-7D	dynamic	VLAN 1

Show Information Route Management > ARP > Show Information

ARP Address
 Statistics

ARP Statistics

Received Request	3805	Sent Request	0
Received Reply	7	Sent Reply	13

Routing Table

Route Management > Routing Table page is used to display all routes that can be accessed via local network interfaces, through static routes, or through a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic (except when the distance parameter of a dynamic route is set to a value that makes its priority exceed that of a static route). Also note that the route for a local interface is not enabled (i.e., listed in the routing table) unless there is at least one active link connected to that interface.

COMMAND USAGE

◆ The Forwarding Information Base (FIB) contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB. The FIB is distinct from the routing table (or, Routing Information Base – RIB), which holds all routing information received from routing peers. The FIB contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a FIB entry are a network prefix, a router (i.e., VLAN) interface, and next hop information.

◆ The Routing Table (and the “show ip route” command described in the CLI Reference Guide) only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up. Note that routes currently not accessible for forwarding, may still be displayed by using the “show ip route database” command.

PARAMETERS

These parameters are displayed:

- ◆ **VLAN** – VLAN identifier (i.e., configured as a valid IP subnet).
- ◆ **Destination IP Address** – IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.

- ◆ **Net Mask / Prefix Length** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- ◆ **Next Hop** – The IP address of the next hop (or gateway) in this route.
- ◆ **Metric** – Cost for this interface.
- ◆ **Protocol** – The protocol which generated this route information. (Options: Local, Static, RIP, OSPF, Others)

Routing Table						Stacking Unit: 1
Route Management > Routing Table						
Routing Table						
Static Routes						
Configure ECMP Number						
Routing Table List Total: 3						
Interface	Destination IP Address	Net Mask / Prefix Length	Next Hop	Metric	Protocol	
lo	127.0.0.0	255.0.0.0	--	0	Local	
VLAN 1	192.168.1.0	255.255.255.0	--	0	Local	
lo	::1	128	--	0	Local	

you can also manually enter static routes in the routing table. Static routes may be required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

COMMAND USAGE

- ◆ Up to 256 static routes can be configured.
- ◆ Up to eight equal-cost multi-paths (ECMP) can be configured for static routing.
- ◆ If an administrative distance is defined for a static route, and the same destination can be reached through a dynamic route at a lower administration distance, then the dynamic route will be used.
- ◆ If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.
- ◆ Static routes are included in RIP and OSPF updates periodically sent by the router if this feature is enabled.

PARAMETERS

These parameters are displayed:

- ◆ **Destination IP Address** – IP address of the destination network, subnetwork, or host.
- ◆ **Net Mask / Prefix Length** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- ◆ **Next Hop** – IP address of the next router hop used for this route.
- ◆ **Distance** – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF, 120 for RIP, 20 for eBGP, and 200 for iBGP. (Range: 1-255, Default: 1)

Routing Table
Route Management > Routing Table

Routing Table
Static Routes
Configure ECMP Number

Destination IP Address	<input type="text" value="192.168.10.0"/>
Net Mask / Prefix Length	<input type="text" value="255.255.255.0"/>
Next Hop	<input type="text" value="192.168.10.1"/>
Distance (1-255)	<input style="background-color: #ffffcc;" type="text" value="5"/> (Optional)

The following feature is optional:

Route Management > Routing Table (Configure ECMP Number) page is used to configure the maximum number of equal-cost paths that can transmit traffic to the same destination. The Equal-cost Multipath routing algorithm is a technique that supports load sharing over multiple equal-cost paths for data passing to the same destination. Whenever multiple paths with equal path cost to the same destination are found in the routing table, the ECMP algorithm first checks if the cost is lower than that of any other entries in the routing table. If the cost is the lowest in the table, the switch will use up to eight of the paths with equal lowest cost to balance the traffic forwarded to the destination. ECMP uses either equal-cost multipaths manually configured in the static routing table, or equal-cost multipaths dynamically generated by the Open Shortest Path Algorithm (OSPF). In other words, it uses either static or OSPF entries, not both. Normal unicast routing simply selects the path to the destination that has the lowest cost. Multipath routing still selects the path with the lowest cost, but can forward traffic over multiple paths if they all have the same lowest cost. ECMP is enabled by default on the switch. If there is only one lowest cost path toward the destination, this path will be used to forward all traffic. If there is more than one lowest-cost path configured in the static routing table, or dynamically generated by OSPFv2, then up to 8 paths with the same lowest cost can be used to forward traffic to the destination.

COMMAND USAGE

- ◆ ECMP only selects paths of the same protocol type. It cannot be applied to both static paths and dynamic paths at the same time for the same destination. If both static and dynamic paths have the same lowest cost, the static paths have precedence over dynamic paths.
- ◆ Each path toward the same destination with equal-cost takes up one entry in the routing table to record routing information. In other words, a route with 8 paths will take up 8 entries.
- ◆ The routing table can only have up to 8 equal-cost multipaths for static routing and 8 for dynamic routing for a common destination. However, the system supports up to 256 total ECMP entries in ASIC for fast switching, with any additional entries handled by software routing.
- ◆ When there are multiple paths toward the same destination with equal-cost, the system chooses one of these paths to forward each packet toward the destination by applying a

load-splitting algorithm. A hash value is calculated based upon the source and destination IP fields of each packet as an indirect index to one of the multiple paths. Because the hash algorithm is calculated based upon the packet header information which can identify specific traffic flows, this technique minimizes the number of times a path is changed for individual flows. In general, path changes for individual flows will only occur when a path is added or removed from the multipath group.

PARAMETERS

These parameters are displayed:

◆ **ECMP Number** – Sets the maximum number of equal-cost paths to the same destination that can be installed in the routing table. (Range: 1-8; Default: 8)

ACL

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP, or next header type), or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

Configuring Access Control Lists –

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

ACL Management

ACL page is used to create an ACL.

PARAMETERS

These parameters are displayed:

◆ **ACL Name** – Name of the ACL. (Maximum length: 32 characters)

◆ **Type** – The following filter modes are supported:

■ **IP Standard**: IPv4 ACL mode filters packets based on the source IPv4 address.

■ **IP Extended**: IPv4 ACL mode filters packets based on the source or destination IPv4 address, as well as the protocol type and protocol port number. If the “TCP” protocol is specified, then you can also filter packets based on the TCP control code.

■ **IPv6 Standard**: IPv6 ACL mode filters packets based on the source IPv6 address.

■ **IPv6 Extended**: IPv6 ACL mode filters packets based on the source or destination IP address, as well as DSCP, and the next header type.

■ **MAC** – MAC ACL mode filters packets based on the source or destination MAC address

and the Ethernet frame type (RFC 1060).

■ **ARP** – ARP ACL specifies static IP-to-MAC address bindings used for ARP inspection (see "ARP Inspection").



To show a list of ACLs:

1. Click ACL.



ACL Management	
ACL > ACL Management	
ACL List Total: 1	
ACL Name	Type
acl_test	IP Standard

ACL Rule Management

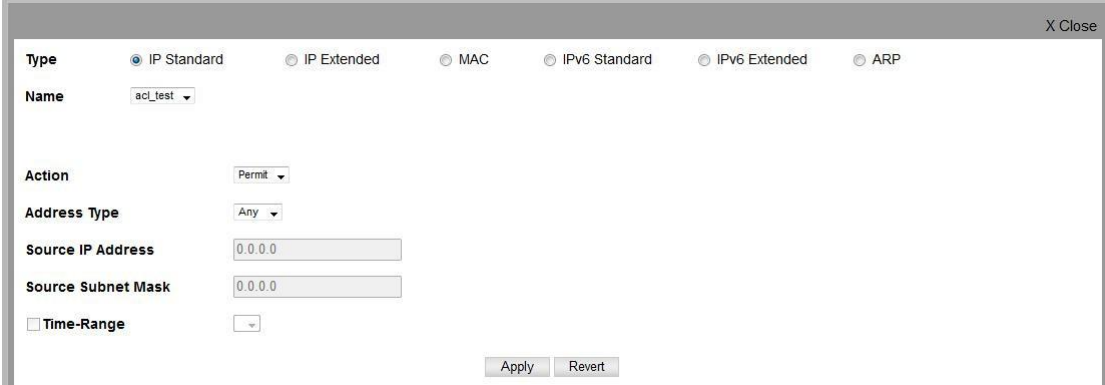
Configuring a Standard Ipv4 ACL

ACL > ACL Rule Management > Ip Standard page is used to configure a Standard IPv4 ACL.

PARAMETERS

These parameters are displayed:

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



Configuring an Extended Ipv4 ACL

ACL > ACL Rule Management > Ip Extended page is used to configure an Extended IPv4 ACL.

PARAMETERS

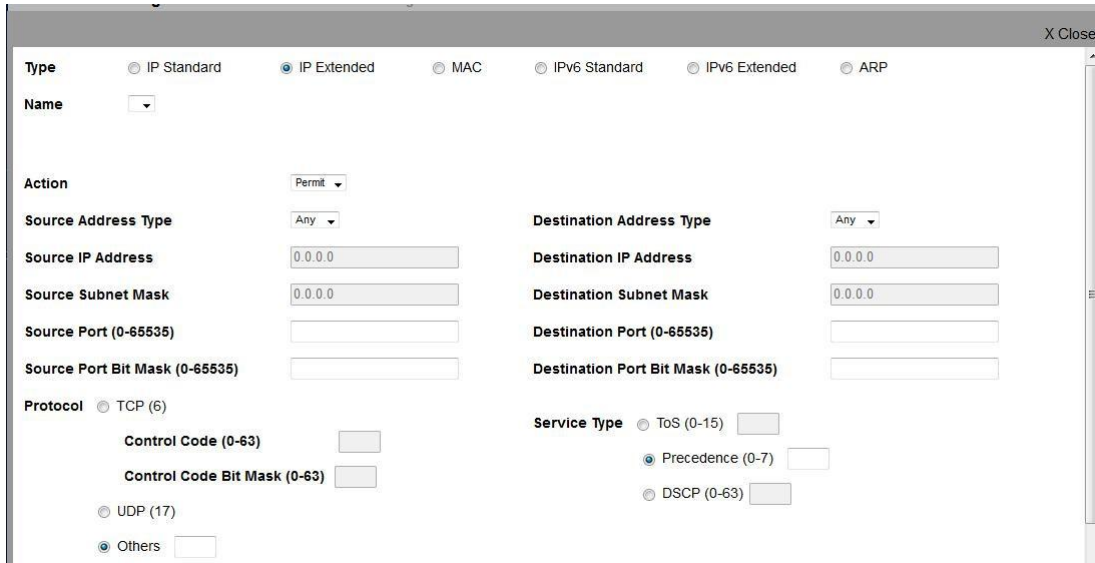
These parameters are displayed:

- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Source/Destination Address Type** – Specifies the source or destination IP address type. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- ◆ **Source/Destination IP Address** – Source or destination IP address.
- ◆ **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask .)
- ◆ **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- ◆ **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- ◆ **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: Others)
- ◆ **Service Type** – Packet priority settings based on the following criteria:
 - **Precedence** – IP precedence level. (Range: 0-7)
 - **DSCP** – DSCP priority level. (Range: 0-63)
 - ◆ **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
 - ◆ **Control Code Bit Mask** – Decimal number representing the code bits to match. (Range: 0-63) The control bit mask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
 - 1 (fin) – Finish
 - 2 (syn) – Synchronize
 - 4 (rst) – Reset

- 8 (psh) – Push
- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

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

- SYN flag valid, use control-code 2, control bit mask 2
- Both SYN and ACK valid, use control-code 18, control bit mask 18
- SYN valid and ACK invalid, use control-code 2, control bit mask 18
- ◆ **Time Range** – Name of a time range.



The screenshot shows a web management interface for configuring an ACL rule. The interface is titled "X Close" in the top right corner. It features several sections:

- Type:** Radio buttons for IP Standard, IP Extended (selected), MAC, IPv6 Standard, IPv6 Extended, and ARP.
- Name:** A dropdown menu.
- Action:** A dropdown menu set to "Permit".
- Source Address Type:** A dropdown menu set to "Any".
- Destination Address Type:** A dropdown menu set to "Any".
- Source IP Address:** A text input field containing "0.0.0.0".
- Destination IP Address:** A text input field containing "0.0.0.0".
- Source Subnet Mask:** A text input field containing "0.0.0.0".
- Destination Subnet Mask:** A text input field containing "0.0.0.0".
- Source Port (0-65535):** A text input field.
- Destination Port (0-65535):** A text input field.
- Source Port Bit Mask (0-65535):** A text input field.
- Destination Port Bit Mask (0-65535):** A text input field.
- Protocol:** Radio buttons for TCP (6), UDP (17), and Others (selected).
- Control Code (0-63):** A text input field.
- Control Code Bit Mask (0-63):** A text input field.
- Service Type:** Radio buttons for ToS (0-15), Precedence (0-7) (selected), and DSCP (0-63).

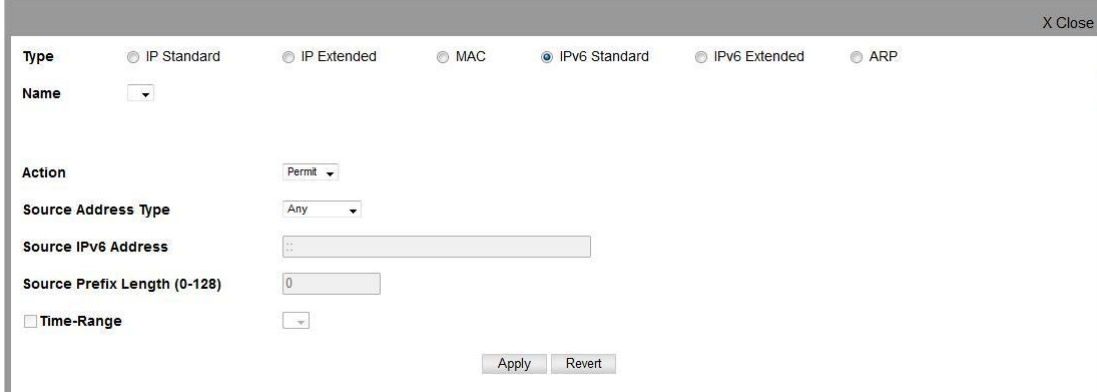
Configuring a Standard IPv6 ACL

ACL > ACL Rule Management > IPv6 Standard page is used to configure a Standard IPv6 ACL.

PARAMETERS

These parameters are displayed in the web interface:

- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Source Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IPv6-Prefix” to specify a range of addresses. (Options: Any, Host, IPv6-Prefix; Default: Any)
- ◆ **Source IPv6 Address** – An IPv6 source address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ **Source Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address). (Range: 0-128 bits)
- ◆ **Time Range** – Name of a time range.



Configuring an Extended Ipv6 ACL

ACL > ACL Rule Management > IPv6 Extended page is used to configure an Extended IPv6 ACL.

PARAMETERS

These parameters are displayed in the web interface:

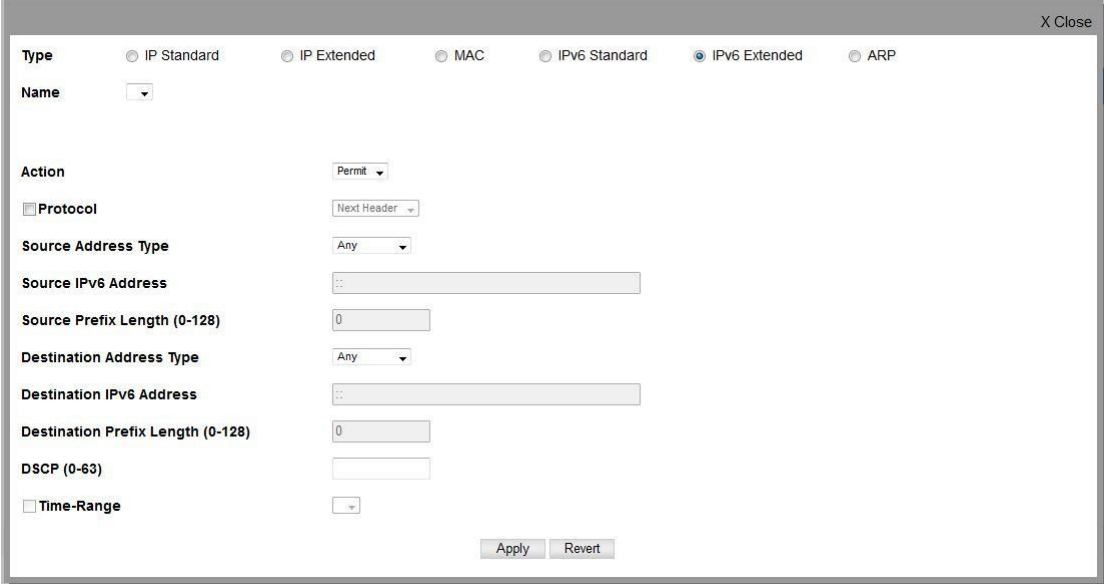
- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Source/Destination Address Type** – Specifies the source or destination IP address type. Use “Any” to include all possible addresses, or “IPv6-Prefix” to specify a range of addresses. (Options: Any, IPv6-Prefix; Default: Any)
- ◆ **Source/Destination IPv6 Address** – An IPv6 address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- ◆ **Source/Destination Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128 bits for the source address; 0-8 bits for the destination address)
- ◆ **DSCP** – DSCP traffic class. (Range: 0-63)
- ◆ **Next Header** – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, and includes these commonly used headers:

- 0 : Hop-by-Hop Options (RFC 2460)
- 6 : TCP Upper-layer Header (RFC 1700)
- 17 : UDP Upper-layer Header (RFC 1700)
- 43 : Routing (RFC 2460)
- 44 : Fragment (RFC 2460)
- 50 : Encapsulating Security Payload (RFC 2406)

51 : Authentication (RFC 2402)

60 : Destination Options (RFC 2460)



Configuring a Mac ACL

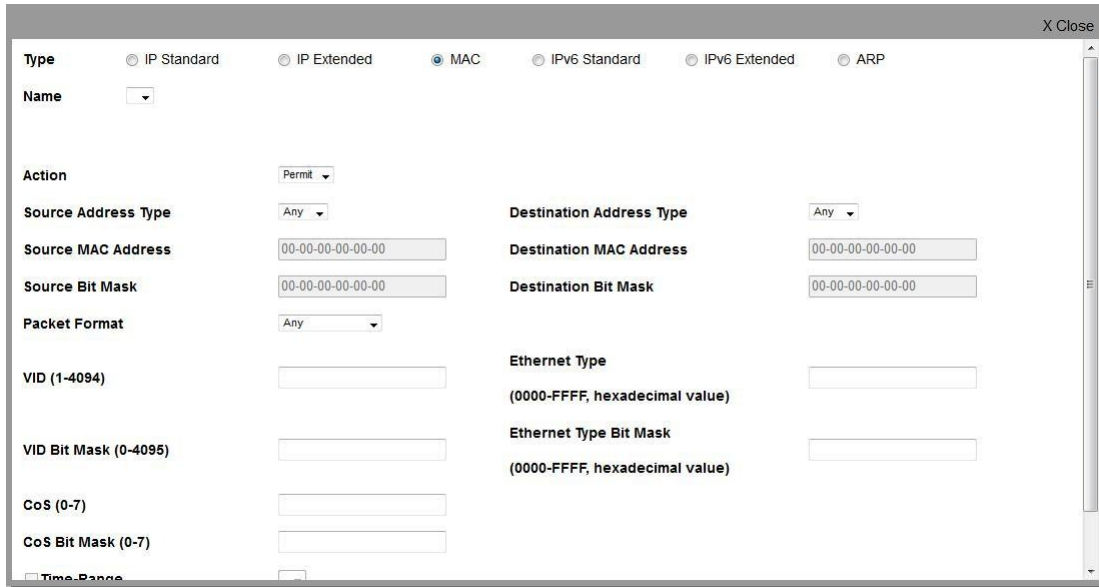
ACL > ACL Rule Management > MAC page is used to configure a MAC ACL based on hardware addresses, packet format, and Ethernet type.

PARAMETERS

These parameters are displayed:

- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Source/Destination Address Type** – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Bit Mask fields. (Options: Any, Host, MAC; Default: Any)
- ◆ **Source/Destination MAC Address** – Source or destination MAC address.
- ◆ **Source/Destination Bit Mask** – Hexadecimal mask for source or destination MAC address.
- ◆ **Packet Format** – This attribute includes the following packet types:
 - **Any** – Any Ethernet packet type.
 - **Untagged-eth2** – Untagged Ethernet II packets.
 - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
 - **Tagged-eth2** – Tagged Ethernet II packets.
 - **Tagged-802.3** – Tagged Ethernet 802.3 packets.
- ◆ **VID** – VLAN ID. (Range: 1-4094)
- ◆ **VID Bit Mask** – VLAN bit mask. (Range: 0-4095)
- ◆ **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-ffff hex.) A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- ◆ **Ethernet Type Bit Mask** – Protocol bit mask. (Range: 600-ffff hex)

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



Configuring an ARP ACL

ACL > ACL Rule Management > ARP page is used to configure ACLs based on ARP message addresses. ARP Inspection can then use these ACLs to filter suspicious traffic.

PARAMETERS

These parameters are displayed:

- ◆ **Type** – Selects the type of ACLs to show in the Name list.
- ◆ **Name** – Shows the names of ACLs matching the selected type.
- ◆ **Action** – An ACL can contain any combination of permit or deny rules.
- ◆ **Packet Type** – Indicates an ARP request, ARP response, or either type.
(Range: IP, Request, Response; Default: IP)
- ◆ **Source/Destination IP Address Type** – Specifies the source or destination IPv4 address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Mask fields.
(Options: Any, Host, IP; Default: Any)
- ◆ **Source/Destination IP Address** – Source or destination IP address.
- ◆ **Source/Destination IP Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask .)
- ◆ **Source/Destination MAC Address Type** – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Mask fields. (Options: Any, Host, MAC; Default: Any)
- ◆ **Source/Destination MAC Address** – Source or destination MAC address.
- ◆ **Source/Destination MAC Bit Mask** – Hexadecimal mask for source or destination MAC address.
- ◆ **Log** – Logs a packet when it matches the access control entry.

X Close

Type IP Standard IP Extended MAC IPv6 Standard IPv6 Extended ARP

Name

<p>Action <input type="text" value="Permit"/></p> <p>Source IP Address Type <input type="text" value="Any"/></p> <p>Source IP Address <input type="text" value="0.0.0.0"/></p> <p>Source IP Subnet Mask <input type="text" value="0.0.0.0"/></p> <p>Source MAC Address Type <input type="text" value="Any"/></p> <p>Source MAC Address <input type="text" value="00-00-00-00-00-00"/></p> <p>Source MAC Bit Mask <input type="text" value="00-00-00-00-00-00"/></p> <p><input type="checkbox"/> Log</p>	<p>Packet Type <input type="text" value="IP"/></p> <p>Destination IP Address Type <input type="text" value="Any"/></p> <p>Destination IP Address <input type="text" value="0.0.0.0"/></p> <p>Destination IP Subnet Mask <input type="text" value="0.0.0.0"/></p> <p>Destination MAC Address Type <input type="text" value="Any"/></p> <p>Destination MAC Address <input type="text" value="00-00-00-00-00-00"/></p> <p>Destination MAC Bit Mask <input type="text" value="00-00-00-00-00-00"/></p>
---	--

Show TCAM

ACL > Show TCAM page is used to show utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

COMMAND USAGE

Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, QinQ, MAC-based VLANs, or traps. For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

PARAMETERS

These parameters are displayed:

- ◆ **Total Policy Control Entries** – The number policy control entries in use.
- ◆ **Free Policy Control Entries** – The number of policy control entries available for use.
- ◆ **Entries Used by System** – The number of policy control entries used by the operating system.
- ◆ **Entries Used by User** – The number of policy control entries used by configuration settings, such as access control lists.
- ◆ **TCAM Utilization** – The overall percentage of TCAM in use.

Show TCAM ACL > Show TCAM

Pool Capability Code:

AM - MAC ACL, A4 - IPv4 ACL, A6S - IPv6 Standard ACL,
A6E - IPv6 extended ACL, DM - MAC diffServ, D4 - IPv4 diffServ,
D6S - IPv6 standard diffServ, D6E - IPv6 extended diffServ,
AEM - Egress MAC ACL, AE4 - Egress IPv4 ACL,
AE6S - Egress IPv6 standard ACL, AE6E - Egress IPv6 extended ACL,
DEM - Egress MAC diffServ, DE4 - Egress IPv4 diffServ,
DE6S - Egress IPv6 standard diffServ,
DE6E - Egress IPv6 extended diffServ, W - Web authentication,
I - IP source guard, I6 - IPv6 source guard, C - CPU interface,
L - Link local, Reserved - Reserved,
ALL - All supported function.

TCAM List Total: 11

Unit	Device	Pool	Total	Used	Free	Capability
1	0	0	128	0	128	A6S A6E D6S D6E
1	0	1	256	0	256	A4 D4

Configure Interface

ACL > Configure Interface page is used to bind the ports that need to filter traffic to the appropriate ACLs. You can assign one IP access list and one MAC access list to any port.

PARAMETERS

These parameters are displayed:

- ◆ **Type** – Selects the type of ACLs to bind to a port.
- ◆ **Port** – Port identifier.
- ◆ **ACL** – ACL used for ingress or egress packets.
- ◆ **Time Range** – Name of a time range.
- ◆ **Counter** – Enables counter for ACL statistics.

Configure Interface ACL > Configure Interface Stacking Unit: 1

Type IP MAC IPv6

Port

Ingress

ACL

Time-Range

Counter

Egress

ACL

Time-Range

Counter

Show Hardware Counter

ACL > Show Hardware Counters page is used to show statistics for ACL hardware counters.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Type** – Selects the type of ACL.

- ◆ **Direction** – Displays statistics for ingress or egress traffic.
- ◆ **ACL Name** – The ACL bound this port.
- ◆ **Action** – Shows if action is to permit or deny specified packets.
- ◆ **Rules** – Shows the rules for the ACL bound to this port.
- ◆ **Hit** – Shows the number of packets matching this ACL.
- ◆ **Clear Counter** – Clears the hit counter for the specified ACL.

Show Hardware Counter Stacking Unit: 1
 ACL > Show Hardware Counter

Port: 1
 Type: IP Standard
 Direction: Ingress

Query

ACL Name: acl_test

Total: 1

Action	Source IP Address	Time-Range	Hit	Clear Counter
Permit	Any			

CoS

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

Default Priority

CoS > Default Priority page is used to specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

COMMAND USAGE

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

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Displays a list of ports or trunks.
- ◆ **CoS** – The priority that is assigned to untagged frames received on the specified interface.

(Range: 0-7; Default: 0)

Default Priority
CoS > Default Priority
Stacking Unit: 1

Interface Port Trunk

Port to CoS Mapping Table Total: 28 1 2 3

Port	CoS (0-7)
1	0 <input style="width: 50px;" type="text"/>
2	0 <input style="width: 50px;" type="text"/>
3	0 <input style="width: 50px;" type="text"/>
4	0 <input style="width: 50px;" type="text"/>
5	0 <input style="width: 50px;" type="text"/>

Queue

CoS > Queue page is used to set the queue mode for the egress queues on any interface. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, or Weighted Round-Robin (WRR) queuing which specifies a scheduling weight for each queue. It can also be configured to use a combination of strict and weighted queuing.

COMMAND USAGE

- ◆ Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- ◆ WRR queuing specifies a relative weight for each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.
- ◆ If Strict and WRR mode is selected, a combination of strict service is used for the high priority queues and weighted service for the remaining queues. The queues assigned to use strict priority should be specified using the Strict Mode field parameter.
- ◆ A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value. Service time is shared at the egress ports by defining scheduling weights for WRR, or one of the queuing modes that use a combination of strict and weighted queuing.
- ◆ The specified queue mode applies to all interfaces.
- ◆ Protocols used to synchronize distributed switches use packets of 1588 bytes to control the synchronization process. This switch therefore assigns packets of this size to the highest priority queue to ensure quick passage.

PARAMETERS

These parameters are displayed:

◆ Queue Mode

- **Strict** – Services the egress queues in sequential order, transmitting all traffic in the higher

priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

■ **WRR** – Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights, and servicing each queue in a round-robin fashion. (This is the default setting.)

■ **Strict and WRR** – Uses strict priority on the high-priority queues and WRR on the remaining queues.

◆ **Queue ID** – The ID of the priority queue. (Range: 0-7)

◆ **Strict Mode** – If “Strict and WRR” mode is selected, then a combination of strict service is used for the high priority queues and weighted service for the remaining queues. Use this parameter to specify the queues assigned to use strict priority. (Default: Disabled)

◆ **Weight** – Sets a weight for each queue which is used by the WRR scheduler. (Range: 1-255; Default: Weights 1, 2, 4, 6, 8, 10, 12 and 14 are assigned to queues 0 - 7 respectively)

Queue CoS > Queue Stacking Unit: 1

Port:

Queue Mode:

Queue Setting Table Total: 8

Queue ID	Weight (1-15)
0	<input type="text" value="1"/>
1	<input type="text" value="2"/>
2	<input type="text" value="4"/>
3	<input type="text" value="6"/>
4	<input type="text" value="8"/>
5	<input type="text" value="10"/>
6	<input type="text" value="12"/>
7	<input type="text" value="14"/>

Trust Mode

The switch allows a choice between using DSCP or CoS priority processing methods. CoS > Trust Mode page is used to select the required processing method.

COMMAND USAGE

◆ If the QoS mapping mode is set to DSCP, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.

◆ If the QoS mapping mode is set to DSCP, and a non-IP packet is received, the packet's CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority is used for priority processing.

◆ If the QoS mapping mode is set to CoS, and the ingress packet type is IPv4, then priority processing will be based on the CoS and CFI values in the ingress packet.

For an untagged packet, the default port priority is used for priority processing.

PARAMETERS

These parameters are displayed:

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

◆ **Trust Mode**

■ **CoS** – Maps layer 3/4 priorities using Class of Service values. (This is the default setting.)

■ **DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point values.

Trust Mode
CoS > Trust Mode
Stacking Unit : 1

Trust Mode List Total: 28
1 2 3

Port	Trust Mode
1	CoS
2	CoS
3	CoS
4	CoS
5	CoS
6	CoS
7	CoS
8	CoS
9	CoS
10	CoS

DSCP to DSCP

CoS > DSCP to DSCP page is used to map DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing. The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

COMMAND USAGE

- ◆ Enter per-hop behavior and drop precedence for any of the DSCP values 0 - 63.
- ◆ This map is only used when the priority mapping mode is set to DSCP, and the ingress packet type is IPv4. Any attempt to configure the DSCP mutation map will not be accepted by the switch, unless the trust mode has been set to DSCP.
- ◆ Two QoS domains can have different DSCP definitions, so the DSCP-to-PHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

PARAMETERS

These parameters are displayed:

◆ **Port** – Specifies a port.

◆ **DSCP** – DSCP value in ingress packets. (Range: 0-63)

- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- ◆ **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

	0	1	2	3	4	5	6	7	8	9
ingress-dscp1										
ingress-dscp10										
0	0,0	0,1	0,0	0,3	0,0	0,1	0,0	0,3	1,0	1,1
1	1,0	1,3	1,0	1,1	1,0	1,3	2,0	2,1	2,0	2,3
2	2,0	2,1	2,0	2,3	3,0	3,1	3,0	3,3	3,0	3,1
3	3,0	3,3	4,0	4,1	4,0	4,3	4,0	4,1	4,0	4,3
4	5,0	5,1	5,0	5,3	5,0	5,1	6,0	5,3	6,0	6,1
5	6,0	6,3	6,0	6,1	6,0	6,3	7,0	7,1	7,0	7,3
6	7,0	7,1	7,0	7,3						

X Close

Port

DSCP (0-63)

PHB (0-7)

Drop Precedence

To show the DSCP to internal PHB/drop precedence map:

DSCP to DSCP CoS > DSCP to DSCP Stacking Unit:

Port

DSCP to DSCP Mapping List Total: 64 1 2 3 4 5 6 7

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

CoS to DSCP

CoS > CoS to DSCP page is used to maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing.

COMMAND USAGE

- ◆ The default mapping of CoS to PHB values is shown in following table.
- ◆ Enter up to eight CoS/CFI paired values, per-hop behavior and drop precedence.
- ◆ If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.
- ◆ The internal DSCP consists of three bits for per-hop behavior (PHB) which determines the queue to which a packet is sent; and two bits for drop precedence (namely color) which is used to control traffic congestion.
- ◆ The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Specifies a port.
- ◆ **CoS** – CoS value in ingress packets. (Range: 0-7)
- ◆ **CFI** – Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)
- ◆ **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- ◆ **Drop Precedence** – Drop precedence used in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

CFI CoS	0	1
0	(0,0)	(0,0)
1	(1,0)	(1,0)
2	(2,0)	(2,0)
3	(3,0)	(3,0)
4	(4,0)	(4,0)
5	(5,0)	(5,0)
6	(6,0)	(6,0)
7	(7,0)	(7,0)

X Close

Port

CoS (0-7)

CFI (0-1)

PHB (0-7)

Drop

Precedence

To show the CoS/CFI to internal PHB/drop precedence map:

CoS to DSCP Stacking Unit:

Port

CoS to DSCP Mapping List Total: 16

	CoS	CFI	PHB	Drop Precedence
<input type="checkbox"/>	0	0	0	0: Green
<input type="checkbox"/>	0	1	0	0: Green
<input type="checkbox"/>	1	0	1	0: Green
<input type="checkbox"/>	1	1	1	0: Green
<input type="checkbox"/>	2	0	2	0: Green
<input type="checkbox"/>	2	1	2	0: Green
<input type="checkbox"/>	3	0	3	0: Green
<input type="checkbox"/>	3	1	3	0: Green
<input type="checkbox"/>	4	0	4	0: Green
<input type="checkbox"/>	4	1	4	0: Green

DSCP to CoS

CoS > DSCP to CoS page is used to map internal per-hop behavior and drop precedence value pairs to CoS values used in tagged egress packets on a Layer 2 interface.

CLI REFERENCES

COMMAND USAGE

- ◆ Enter any per-hop behavior and drop precedence pair within the internal priority map, and then enter the corresponding CoS/CFI pair.
- ◆ If the packet is forwarded with an 8021.Q tag, the priority value in the egress packet is modified based on the default values shown in the following table, or on the values modified by this function.

PARAMETERS

These parameters are displayed in the web interface:

- ◆ Port – Specifies a port.
- ◆ PHB – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- ◆ Drop Precedence – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)
- ◆ CoS – Class-of-Service value. (Range: 0-7)
- ◆ CFI – Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)

Drop Precedence	0 (green)	1 (red)	3 (yellow)
Per-hop Behavior			
0	(0,0)	(0,0)	(0,0)
1	(1,0)	(1,0)	(1,0)
2	(2,0)	(2,0)	(2,0)
3	(3,0)	(3,0)	(3,0)
4	(4,0)	(4,0)	(4,0)
5	(5,0)	(5,0)	(5,0)
6	(6,0)	(6,0)	(6,0)
7	(7,0)	(7,0)	(7,0)

X Close

Port

PHB (0-7)

Drop Precedence

CoS (0-7)

CFI (0-1)

DSCP to CoS CoS > DSCP to CoS Stacking Unit : 1

Port: 1

DSCP to CoS Mapping List Total: 24

<input type="checkbox"/>	PHB	Drop Precedence	CoS	CFI
<input type="checkbox"/>	0	0	0	0
<input type="checkbox"/>	0	1	0	0
<input type="checkbox"/>	0	3	0	0
<input type="checkbox"/>	1	0	1	0
<input type="checkbox"/>	1	1	1	0
<input type="checkbox"/>	1	3	1	0
<input type="checkbox"/>	2	0	2	0
<input type="checkbox"/>	2	1	2	0
<input type="checkbox"/>	2	3	2	0
<input type="checkbox"/>	3	0	3	0

IP Precedence to DSCP

CoS > IP Precedence to DSCP page is used to map IP precedence values in incoming packets to per-hop behavior and drop precedence values for priority processing.

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 default IP Precedence values map one-to-one to the Class of Service values (that is, Precedence value 0 maps to PHB value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types.

Priority Level	Traffic Type
7	Network Control
6	Internetwork Control
5	Critical
4	Flash Override
3	Flash
2	Immediate
1	Priority
0	Routine

- ◆ Enter per-hop behavior and drop precedence for any of the IP Precedence values 0 - 7.
- ◆ If the priority mapping mode is set the IP Precedence and the ingress packet type is IPv4, then the IP Precedence-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing.

PARAMETERS

These parameters are displayed in the web interface:

- ◆ Port – Specifies a port.
- ◆ IP Precedence – IP Precedence value in ingress packets. (Range: 0-7)
- ◆ PHB – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- ◆ Drop Precedence – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

IP Precedence Value	0	1	2	3	4	5	6	7
Per-hop Behavior	0	1	2	3	4	5	6	7
Drop Precedence	0	0	0	0	0	0	0	0

X Close

Port

IP Precedence

(0-7)

PHB (0-7)

Drop Precedence

IP Precedence to DSCP Stacking Unit:

Port

IP Precedence to DSCP Mapping List Total: 8

IP Precedence	PHB	Drop Precedence
0	0	0: Green
1	1	0: Green
2	2	0: Green
3	3	0: Green
4	4	0: Green
5	5	0: Green
6	6	0: Green
7	7	0: Green

IP Port to DSCP

CoS > IP Port to DSCP page is used to map network applications designated by a TCP/UDP destination port number in the frame header to per-hop behavior and drop precedence

values for internal priority processing.

COMMAND USAGE

◆ This mapping table is only used if the protocol type of the arriving packet is TCP or UDP. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

◆ No default mapping is defined for ingress TCP/UDP port types.

PARAMETERS

These parameters are displayed in the web interface:

- ◆ Port – Specifies a port.
- ◆ IP Protocol
- TCP – Transport Control Protocol
- UDP – User Datagram Protocol
- ◆ Destination Port Number – 16-bit TCP/UDP destination port number. (Range: 0-65535)
- ◆ PHB – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- ◆ Drop Precedence – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

X Close

Port 1

IP Protocol TCP

Destination Port
(0-65535)

PHB (0-7)

Drop Precedence 0: Green

Apply
Revert

IP Port to DSCP Stacking Unit: 1

CoS > IP Port to DSCP

Port 1

IP Port to DSCP Mapping List Total: 1

	IP Protocol	Destination Port	PHB	Drop Precedence
☐	TCP	21	1	0

Configure
Delete
Revert

PHB to Queue

CoS > PHB to Queue page is used to specify the hardware output queues to use based on the internal per-hop behavior value. (For more information on exact manner in which the ingress priority tags are mapped to egress queues for internal processing, see "Mapping CoS Priorities to Internal DSCP Values").

The switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict priority, Weighted Round-Robin

(WRR), or a combination of strict and weighted queuing. Up to eight separate traffic priorities are defined in IEEE 802.1p. Default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in following table. The following table indicates the default mapping of internal per-hop behavior to the hardware queues. The actual mapping may differ if the CoS priorities to internal DSCP values have been modified .

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

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

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

COMMAND USAGE

◆ Egress packets are placed into the hardware queues according to the mapping defined by this command.

◆ The default internal PHB to output queue mapping is shown below.

Per-hop Behavior 0	1	2	3	4	5	6	7
Hardware Queues 2	0	1	3	4	5	6	7

◆ The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed:

◆ **Port** – Specifies a port.

◆ **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7, where 7 is the highest priority)

◆ **Queue** – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

X Close

Port 1 ▾

PHB (0-7)

Queue (0-7)

Apply Revert

PHB to Queue
CoS > PHB to Queue
Stacking Unit : 1 ▾

Port 1 ▾

PHB to Queue Mapping List Total: 8

	PHB	Queue
<input type="checkbox"/>	0	2
<input type="checkbox"/>	1	0
<input type="checkbox"/>	2	1
<input type="checkbox"/>	3	3
<input type="checkbox"/>	4	4
<input type="checkbox"/>	5	5
<input type="checkbox"/>	6	6
<input type="checkbox"/>	7	7

Configure Default Revert

QoS

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called perhop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

Class

A class map is used for matching packets to a specified class. QoS > Class page is used to

configure a class map.

COMMAND USAGE

◆ The class map is used with a policy map to create a service policy for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.

◆ Up to 32 class maps can be configured.

PARAMETERS

These parameters are displayed:

Add

◆ **Class Name** – Name of the class map. (Range: 1-32 characters)

◆ **Type** – The criteria specified by the match command.

■ **Match All** – Match all conditions within a class map.

■ **Match Any** – Match any condition within a class map.

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

◆ **Class Name** – Name of the class map.

◆ **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.

◆ **ACL** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs.

◆ **IP DSCP** – A DSCP value. (Range: 0-63)

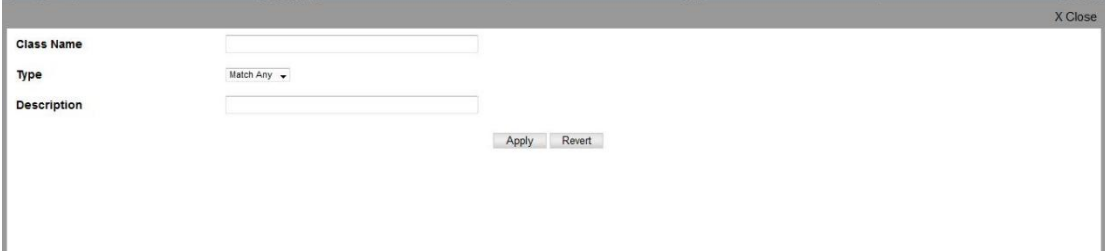
◆ **IP Precedence** – An IP Precedence value. (Range: 0-7)

◆ **IPv6 DSCP** – A DSCP value contained in an IPv6 packet. (Range: 0-63)

◆ **VLAN ID** – A VLAN. (Range: 1-4093)

◆ **CoS** – A CoS value. (Range: 0-7)

◆ **Source Port** – A source port. (Range: 1-28)



Class [QoS > Class](#)

Class List Total: 1

	Class Name	Type	Description
<input type="checkbox"/>	class_test	Match Any	

Class Rule

To edit the rules for a class map:



Policy

QoS > Policy page is used to create a policy map that can be attached to multiple interfaces. A policy map is used to group one or more class map statements, modify service tagging, and enforce bandwidth policing. A policy map can then be bound by a service policy to one or more interfaces.

Configuring QoS policies requires several steps. A class map must first be configured which indicates how to match the inbound packets according to an access list, a DSCP or IP Precedence value, or a member of specific VLAN. A policy map is then configured which indicates the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic. A policy map may contain one or more classes based on previously defined class maps. The class of service or per-hop behavior (i.e., the priority used for internal queue processing) can be assigned to matching packets. In addition, the flow rate of inbound traffic can be monitored and the response to conforming and non-conforming traffic based by one of three distinct policing methods as described below.

Police Flow Meter – Defines the committed information rate (maximum throughput), committed burst size (burst rate), and the action to take for conforming and non-conforming traffic. Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the “burst” field (BC), and the average rate tokens are removed from the bucket is specified by the “rate” option (CIR). Action may be taken for traffic conforming to the maximum throughput, or exceeding the maximum throughput.

srTCM Police Meter – Defines an enforcer for classified traffic based on a single rate three color meter scheme defined in RFC 2697. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and excess burst size (BE). Action may be taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the excess burst size.

◆ The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP servicevalue, or drop a packet, the switch will

also mark the two color bits used to set the drop precedence of a packet. A packet is marked green if it doesn't exceed the committed information rate and committed burst size, yellow if it does exceed the committed

information rate and committed burst size, but not the excess burst size, and red otherwise.

◆ The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

◆ The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE. The token buckets C and E are initially full, that is, the token count $Tc(0) = BC$ and the token count $Te(0) = BE$. Thereafter, the token counts Tc and Te are updated CIR times per second as follows:

- If Tc is less than BC, Tc is incremented by one, else
- if Te is less than BE, Te is incremented by one, else
- neither Tc nor Te is incremented.

When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in Color-Blind mode:

- If $Tc(t) - B \geq 0$, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- if $Te(t) - B \geq 0$, the packets is yellow and Te is decremented by B down to the minimum value of 0,
- else the packet is red and neither Tc nor Te is decremented. When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in Color-Aware mode:

- If the packet has been precolored as green and $Tc(t) - B \geq 0$, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- If the packet has been precolored as yellow or green and if $Te(t) - B \geq 0$, the packets is yellow and Te is decremented by B down to the minimum value of 0, else
- the packet is red and neither Tc nor Te is decremented. The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

trTCM Police Meter – Defines an enforcer for classified traffic based on a two rate three color meter scheme defined in RFC 2698. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate), and peak burst size (BP). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the peak burst size.

◆ The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP servicevalue, or drop a packet, the switch will

also mark the two color bits used to set the drop precedence of a packet. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR. The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

◆ The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

◆ The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC. The token buckets P and C are initially (at time 0) full, that is, the token count $T_p(0) = BP$ and the token count $T_c(0) = BC$. Thereafter, the token count T_p is incremented by one PIR times per second up to BP and the token count T_c is incremented by one CIR times per second up to BC. When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in Color-Blind mode:

- If $T_p(t) - B < 0$, the packet is red, else
- if $T_c(t) - B < 0$, the packet is yellow and T_p is decremented by B, else
- the packet is green and both T_p and T_c are decremented by B. When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in Color-Aware mode:

- If the packet has been precolored as red or if $T_p(t) - B < 0$, the packet is red, else
- if the packet has been precolored as yellow or if $T_c(t) - B < 0$, the packet is yellow and T_p is decremented by B, else
- the packet is green and both T_p and T_c are decremented by B.

◆ The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

COMMAND USAGE

◆ A policy map can contain 512 class statements that can be applied to the same interface . Up to 32 policy maps can be configured for ingress ports.

◆ After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy to take effect.

PARAMETERS

These parameters are displayed:

Add

◆ **Policy Name** – Name of policy map. (Range: 1-32 characters)

◆ **Description** – A brief description of a policy map. (Range: 1-256 characters)

Add Rule

◆ **Policy Name** – Name of policy map.

◆ **Class Name** – Name of a class map that defines a traffic classification upon which a policy can act.

◆ **Action** – This attribute is used to set an internal QoS value in hardware for matching

packets. The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion with the srTCM and trTCM metering functions.

■ **Set CoS** – Configures the service provided to ingress traffic by setting an internal CoS value for a matching packet (as specified in rule settings for a class map). (Range: 0-7).

■ **Set PHB** – Configures the service provided to ingress traffic by setting the internal per-hop behavior for a matching packet (as specified in rule settings for a class map). (Range: 0-7).

◆ **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.

◆ **Meter Mode** – Selects one of the following policing methods.

■ **Flow (Police Flow)** – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and the action to take for conforming and non-conforming traffic. Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the “burst” field, and the average rate tokens are removed from the bucket is by specified by the “rate” option.

■ **Committed Information Rate (CIR)** – Rate in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower) The rate cannot exceed the configured interface speed.

■ **Committed Burst Size (BC)** – Burst in bytes. (Range: 64-16000000 at a granularity of 4k bytes) The burst size cannot exceed 16 Mbytes.

■ **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.

■ **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

■ **Violate** – Specifies whether the traffic that exceeds the maximum rate (CIR) will be dropped or the DSCP service level will be reduced.

■ **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)

■ **Drop** – Drops out of conformance traffic.

■ **srTCM (Police Meter)** – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate) and excess burst size (BE), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the excess burst size, or exceeding the excess burst size. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet. The color modes include “Color-Blind” which assumes that the packet stream is uncolored, and “Color-Aware” which assumes that the incoming packets are pre-colored. The functional differences between these modes is described at the beginning of this section under “srTCM Police Meter.”

■ **Committed Information Rate (CIR)** – Rate in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower) The rate cannot exceed the configured interface speed.

■ **Committed Burst Size (BC)** – Burst in bytes. (Range: 64-16000000 at a granularity of 4k bytes) The burst size cannot exceed 16 Mbytes.

■ **Excess Burst Size (BE)** – Burst in excess of committed burst size. (Range: 0-16000000 at a

granularity of 4k bytes) The burst size cannot exceed 16 Mbytes.

■ **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.

■ **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

■ **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the excess burst size (BE) will be dropped or the DSCP service level will be reduced.

■ **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)

■ **Drop** – Drops out of conformance traffic.

■ **Violate** – Specifies whether the traffic that exceeds the excess burst size (BE) will be dropped or the DSCP service level will be reduced.

■ **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)

■ **Drop** – Drops out of conformance traffic.

■ **trTCM (Police Meter)** – Defines the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate) and peak burst size (BP), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the peak information rate, or exceeding the peak information rate. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet. The color modes include “Color-Blind” which assumes that the packet stream is uncolored, and “Color-Aware” which assumes that the incoming packets are pre-colored. The functional differences between these modes is described at the beginning of this section under “trTCM Police Meter.”

■ **Committed Information Rate (CIR)** – Rate in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower) The rate cannot exceed the configured interface speed.

■ **Committed Burst Size (BC)** – Burst in bytes. (Range: 64-16000000 at a granularity of 4k bytes) The burst size cannot exceed 16 Mbytes.

■ **Peak Information Rate (PIR)** – Rate in kilobits per second. (Range: 0-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower) The rate cannot exceed the configured interface speed.

■ **Peak Burst Size (BP)** – Burst size in bytes. (Range: 0-16000000 at a granularity of 4k bytes) The burst size cannot exceed 16 Mbytes.

■ **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.

■ **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

■ **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.

■ **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).

■ **Drop** – Drops out of conformance traffic.

■ **Violate** – Specifies whether the traffic that exceeds the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.

■ **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).

■ **Drop** – Drops out of conformance traffic.

X Close

Policy Name

Description

Policy QoS > Policy

Policy List Total: 1

	Policy Name	Description
<input type="checkbox"/>	policy_test	policy_test

Policy Rule

To edit the rules for a policy map:

X Close

Policy Name policy_test

Rule:

Class Name class_test

Action Set CoS (0-7)

Meter

Meter Mode Flow

Committed Information Rate (0-10000000) kbps

Committed Burst Size (4000-16000000) bytes

Excess Burst Size (4000-16000000) bytes

Peak Information Rate (0-10000000) kbps

Peak Burst Size (4000-16000000) bytes

Conform Set IP DSCP (0-63)

Exceed Set IP DSCP (0-63)

Violate Set IP DSCP (0-63)

To show the rules for a policy map:

Policy Rule QoS > Policy Rule

Policy Name policy_test

Rule List Total: 1

	Class Name	Action	Meter							Conform	Exceed	Violate
			Meter Mode	Committed Information Rate (kbps)	Committed Burst Size (bytes)	Excess Burst Size (bytes)	Peak Information Rate (kbps)	Peak Burst Size (bytes)				
<input type="checkbox"/>	class_test	Set CoS 4	Flow	10000	4000	N/A	N/A	N/A	Transmit	N/A	Drop	

Configure Interface

QoS > Configure Interface page is used to bind a policy map to a port.

COMMAND USAGE

First define a class map, define a policy map, and bind the service policy to the required interface.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Specifies a port.
- ◆ **Ingress** – Applies the selected rule to ingress traffic.
- ◆ **Egress** – Applies the selected rule to egress traffic.

Configure Interface
QoS > Configure Interface
Stacking Unit: 1

Port Service Policy List Total: 28
1 2 3

Port	Ingress	Egress
1	<input checked="" type="checkbox"/> policy_test	<input checked="" type="checkbox"/> policy_test
2	<input checked="" type="checkbox"/> policy_test	<input checked="" type="checkbox"/> policy_test
3	<input type="checkbox"/> policy_test	<input type="checkbox"/> policy_test
4	<input type="checkbox"/> policy_test	<input type="checkbox"/> policy_test
5	<input type="checkbox"/> policy_test	<input type="checkbox"/> policy_test
6	<input type="checkbox"/> policy_test	<input type="checkbox"/> policy_test
7	<input type="checkbox"/> policy_test	<input type="checkbox"/> policy_test
8	<input type="checkbox"/> policy_test	<input type="checkbox"/> policy_test
9	<input type="checkbox"/> policy_test	<input type="checkbox"/> policy_test
10	<input type="checkbox"/> policy_test	<input type="checkbox"/> policy_test

Security

AAA

The authentication, authorization, and accounting (AAA) feature provides the main framework for configuring access control on the switch. The three security functions can be summarized as follows:

- ◆ **Authentication** — Identifies users that request access to the network.
- ◆ **Authorization** — Determines if users can access specific services.
- ◆ **Accounting** — Provides reports, auditing, and billing for services that users have accessed on the network. The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a

request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops. The switch supports the following AAA features:

- ◆ Accounting for IEEE 802.1X authenticated users that access the network through the switch.
- ◆ Accounting for users that access management interfaces on the switch through the console and Telnet.
- ◆ Accounting for commands that users enter at specific CLI privilege levels.
- ◆ Authorization of users that access management interfaces on the switch through the console and Telnet.

System Authentication

Security > AAA > System Authentication page to specify local or remote authentication. Local authentication restricts management access based on user names and passwords manually configured on the switch. Remote authentication uses a remote access authentication server based on RADIUS or TACACS+ protocols to verify management access.

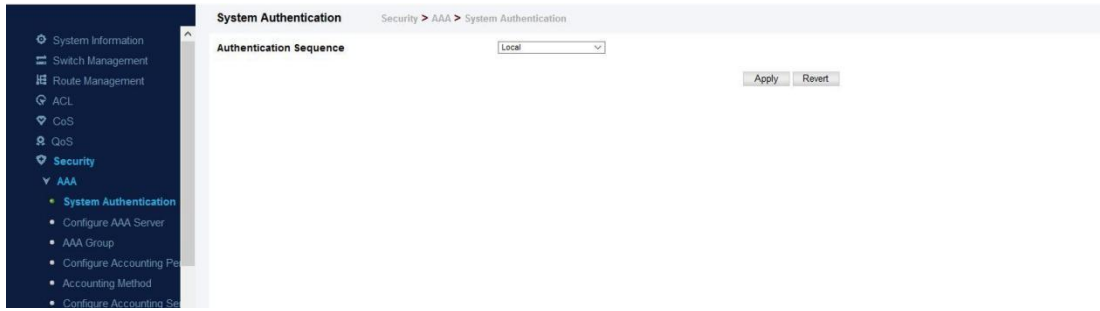
Command Usage

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

Parameters

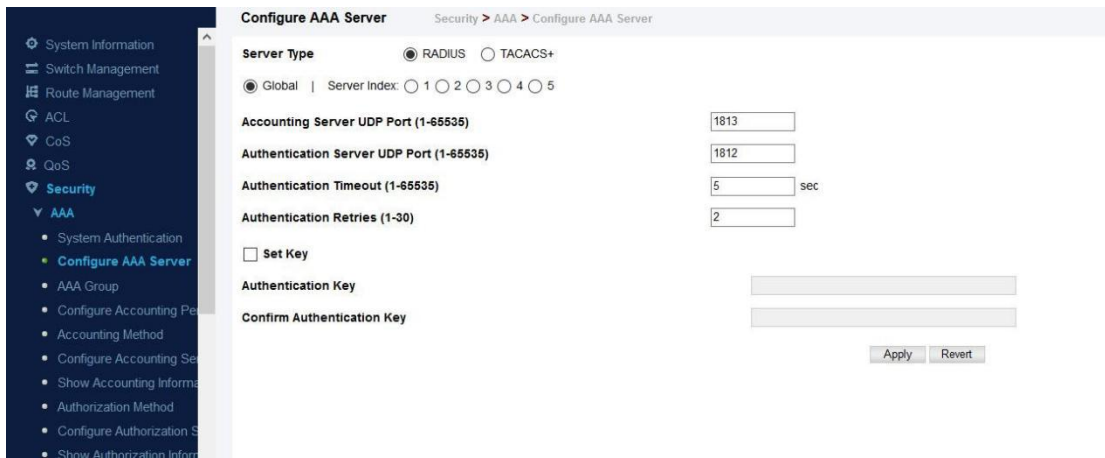
These parameters are displayed:

- ◆ **Authentication Sequence** – Select the authentication, or authentication sequence required:
 - **Local** – User authentication is performed only locally by the switch.
 - **RADIUS** – User authentication is performed using a RADIUS server only.
 - **TACACS** – User authentication is performed using a TACACS+ server only.
 - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.



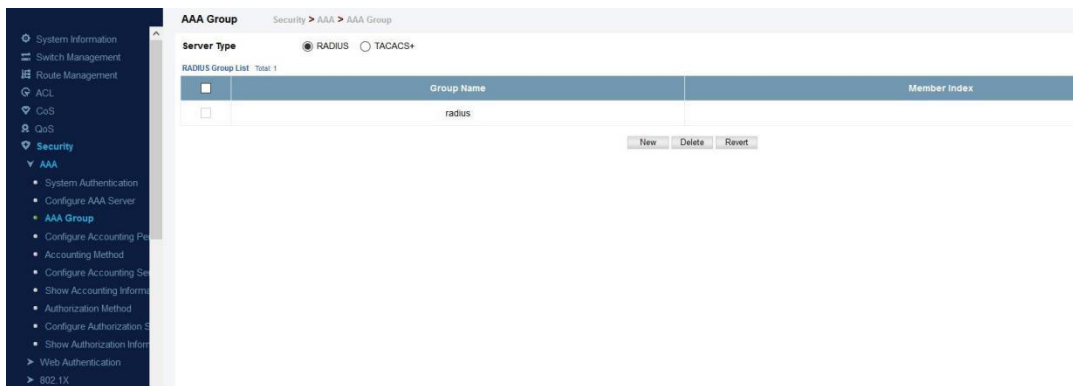
Configure AAA Server

To configure the parameters for RADIUS or TACACS+ authentication:



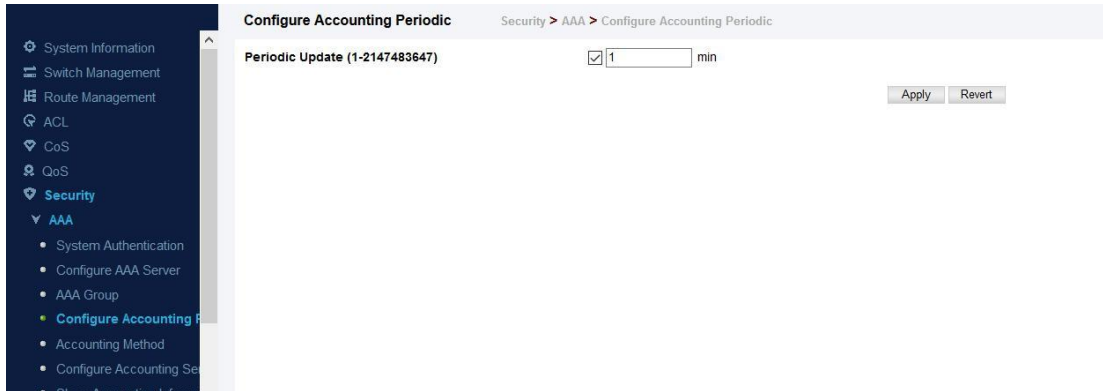
AAA Group

To configure the RADIUS or TACACS+ server groups to use for accounting and authorization:



Configure Accounting Periodic

To configure global settings for AAA accounting:



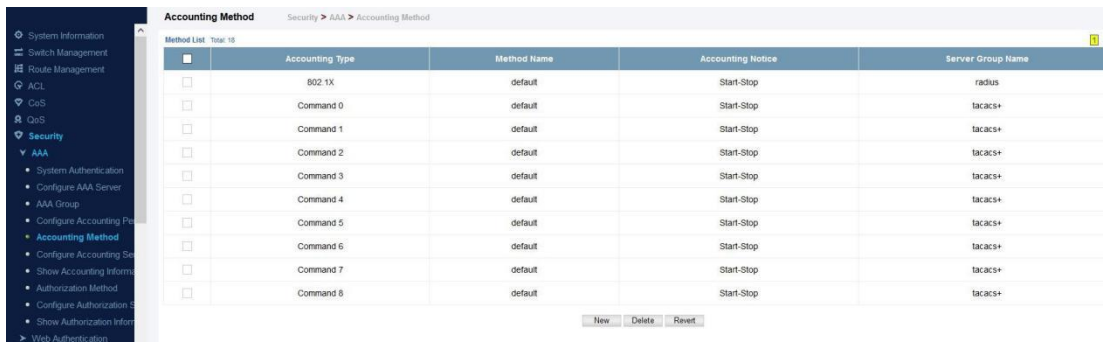
Configure Accounting Periodic Security > AAA > Configure Accounting Periodic

Periodic Update (1-2147483647) 1 min

Apply Revert

Accounting Method

To configure the accounting method applied to various service types and the assigned server group:



Accounting Method Security > AAA > Accounting Method

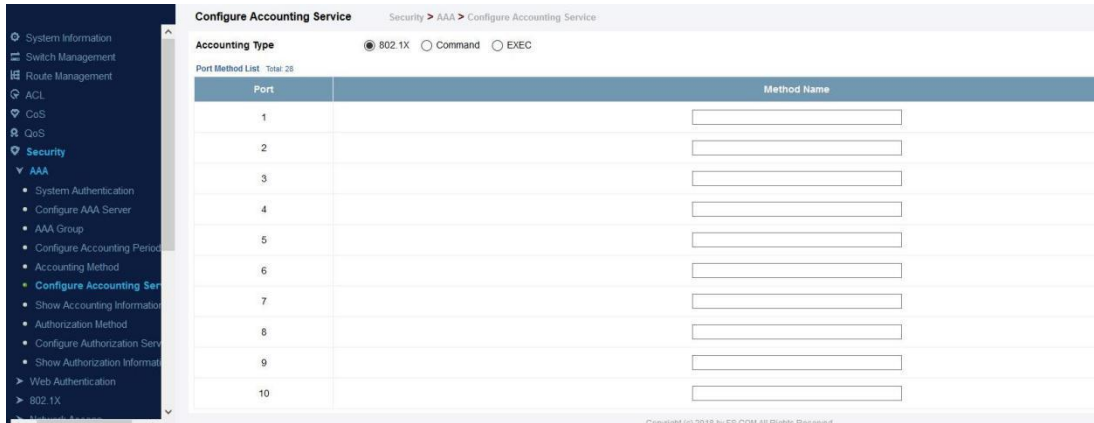
Method List Total: 15

<input type="checkbox"/>	Accounting Type	Method Name	Accounting Notice	Server Group Name
<input type="checkbox"/>	802.1X	default	Start-Stop	radius
<input type="checkbox"/>	Command 0	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 1	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 2	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 3	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 4	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 5	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 6	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 7	default	Start-Stop	tacacs+
<input type="checkbox"/>	Command 8	default	Start-Stop	tacacs+

New Delete Revert

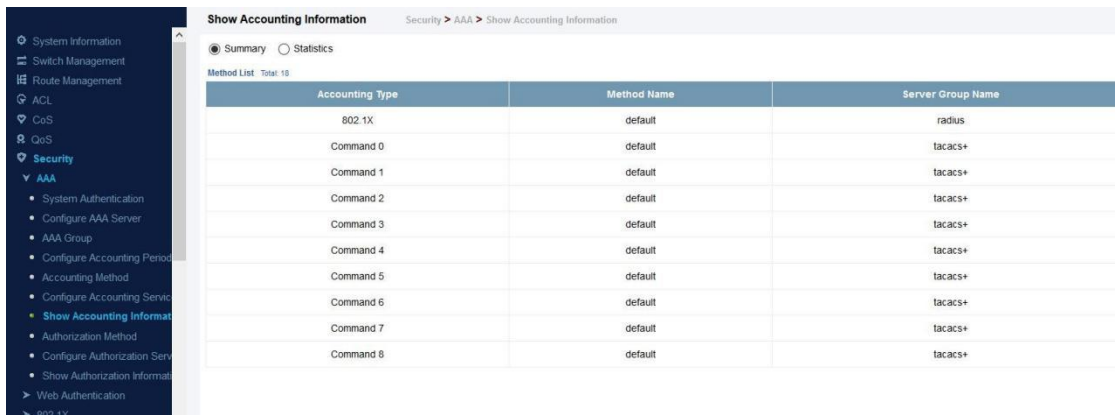
Configure Accounting Service

To configure the accounting method applied to specific interfaces, console commands entered at specific privilege levels, and local console, Telnet, or SSH connections:



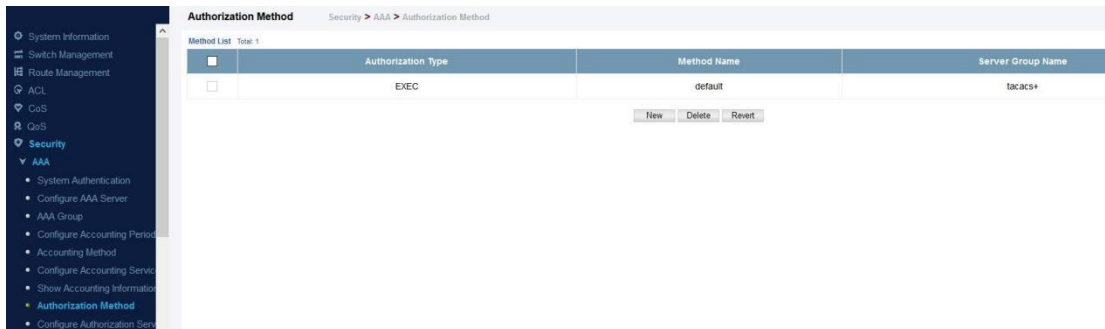
Show Accounting Information

To display a summary of the configured accounting methods and assigned server groups for specified service types:



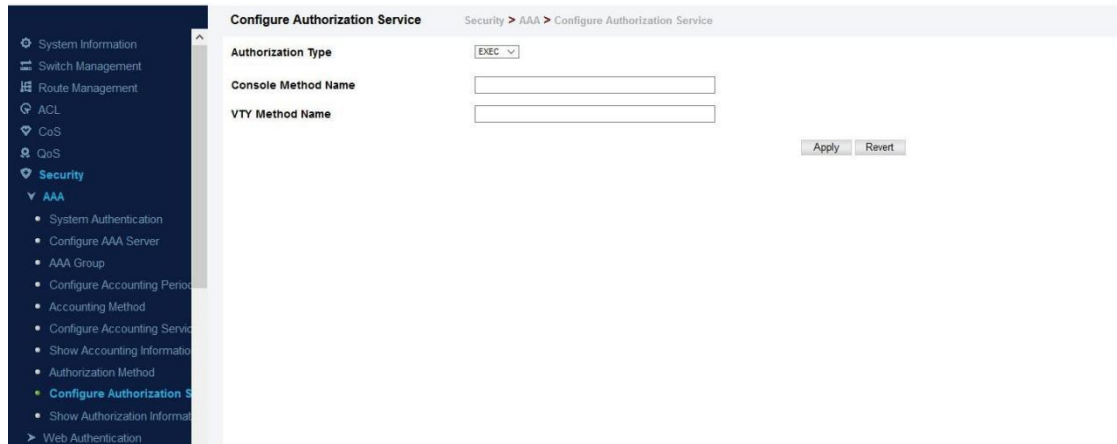
Authorization Method

To configure the authorization method applied to the Exec service type and the assigned server group:



Configure Authorization service

To configure the authorization method applied to local console, Telnet, or SSH connections:



Show Authorization Information

To display the configured authorization method and assigned server groups for the Exec service type:

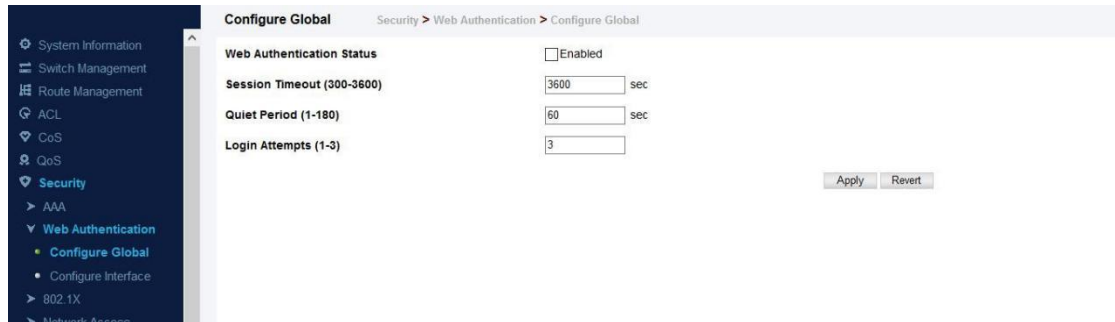


Web Authentication

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.

Configure Global

Security > Web Authentication > Configure Global page is used to edit the global parameters for web authentication.



◆ **Web Authentication Status** – Enables web authentication for the switch. (Default: Disabled)

Note that this feature must also be enabled for any port where required under the Configure Interface menu.

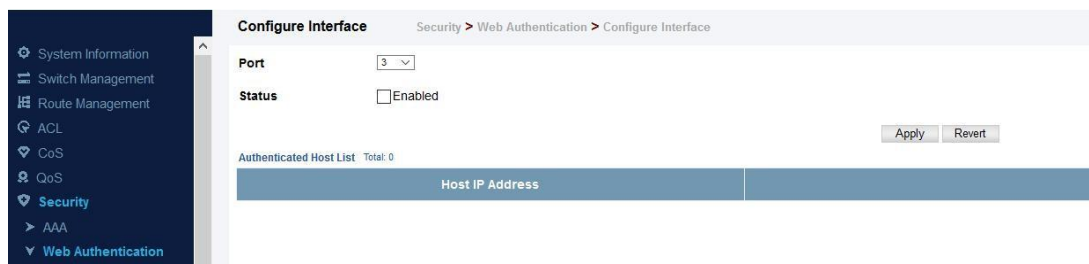
◆ **Session Timeout** – Configures how long an authenticated session stays active before it must re-authenticate itself. (Range: 300-3600 seconds; Default: 3600seconds)

◆ **Quiet Period** – Configures how long a host must wait to attempt authentication again after it has exceeded the maximum allowable failed login attempts. (Range: 1-180 seconds; Default: 60 seconds)

◆ **Login Attempts** – Configures the amount of times a supplicant may attempt and fail authentication before it must wait the configured quiet period. (Range: 1-3 attempts; Default: 3 attempts)

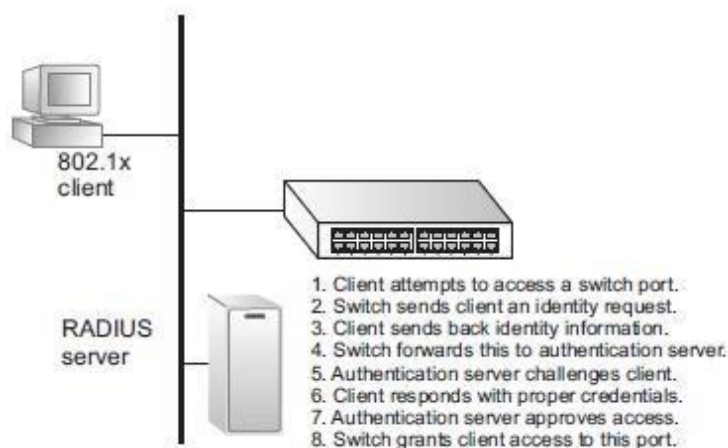
Configure Interface

Security > Web Authentication > Configure Interface page is used to configure the interface.



802.1X

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data. The IEEE 802.1X (dot1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network. This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The encryption method used to pass authentication messages can be MD5 (Message-Digest 5), TLS (Transport Layer Security), PEAP (Protected Extensible Authentication Protocol), or TTLS (Tunneled Transport Layer Security). The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, non-EAP traffic on the port is blocked or assigned to a guest VLAN based on the “intrusion-action” setting. In “multi-host” mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.



Configure Global

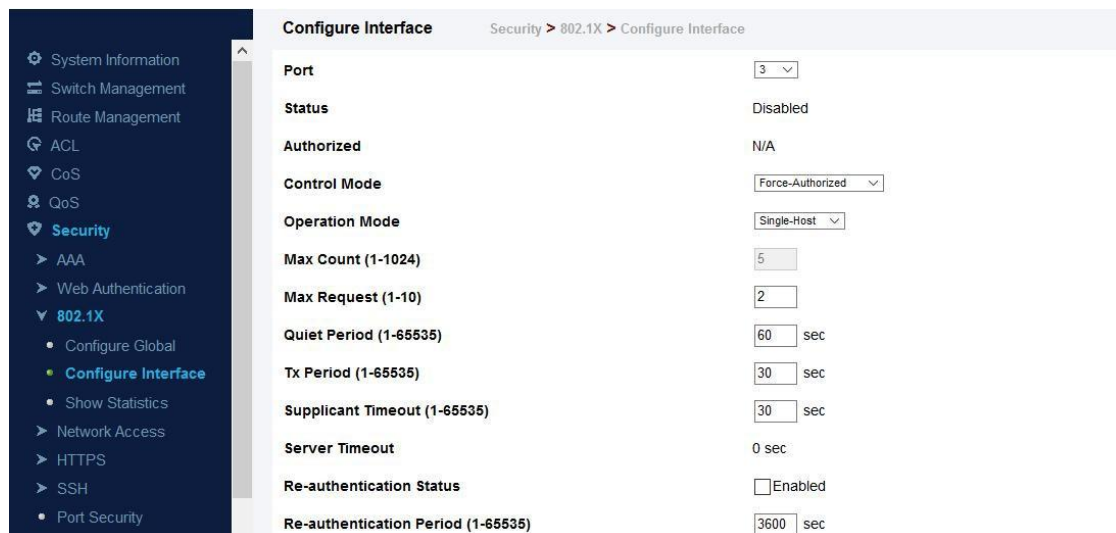
Security > 802.1x > Configure Global page is used to configure the global parameter of 802.1x.



- ◆ **System Authentication Control** – Sets the global setting for 802.1X. (Default: Disabled)
- ◆ **EAPOL Pass Through** – Passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. (Default: Disabled)

Configure Interface

Security > 802.1x > Configure Interface page is used to configure the parameters of a port.



Show Statistics

Security > 802.1x > Show Statistics page is used to display the statistics of 802.1x.



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

Network Access

Some devices connected to switch ports may not be able to support 802.1X authentication due to hardware or software limitations. This is often true for devices such as network printers, IP phones, and some wireless access points. The switch enables network access from these devices to be controlled by authenticating device MAC addresses with a central RADIUS server.

Configure Global

Security > Web Authentication > Configure Global page is used to configure the global parameters.



Configure Global	
Web Authentication Status	<input type="checkbox"/> Enabled
Session Timeout (300-3600)	<input type="text" value="3600"/> sec
Quiet Period (1-180)	<input type="text" value="60"/> sec
Login Attempts (1-3)	<input type="text" value="3"/>

◆ **Web Authentication Status** – Enables web authentication for the switch. (Default: Disabled) Note that this feature must also be enabled for any port where required under the Configure Interface menu.

◆ **Session Timeout** – Configures how long an authenticated session stays active before it must re-authenticate itself. (Range: 300-3600 seconds; Default: 3600seconds)

◆ **Quiet Period** – Configures how long a host must wait to attempt authentication again after it has exceeded the maximum allowable failed login attempts. (Range: 1-180 seconds; Default: 60 seconds)

◆ **Login Attempts** – Configures the amount of times a supplicant may attempt and fail authentication before it must wait the configured quiet period. (Range: 1-3 attempts; Default:

3 attempts)

Configure Interface

Security > Web Authentication > Configure Interface page is used to configure the parameters of interface.



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.

Configure Global

The Security > HTTPS > Configure Global page is used to enable or disable HTTPS and specify the UDP port used for this service.

COMMAND USAGE

◆ Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port.

◆ If you enable HTTPS, you must indicate this in the URL that you specify in your browser: `https://device[:port_number]`

◆ When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server's digital certificate.
- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.
- ◆ The client and server establish a secure encrypted connection. A padlock icon should appear in the status bar for Internet Explorer 6.x or above, or Mozilla Firefox 3.6.2/4/5.
- ◆ The following web browsers and operating systems currently support HTTPS:

Web Browser	Operating System
Internet Explorer 6.x or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows Vista, Windows 7

Mozilla Firefox 3.6.2/4/5

Windows 2000, Windows XP, Linux

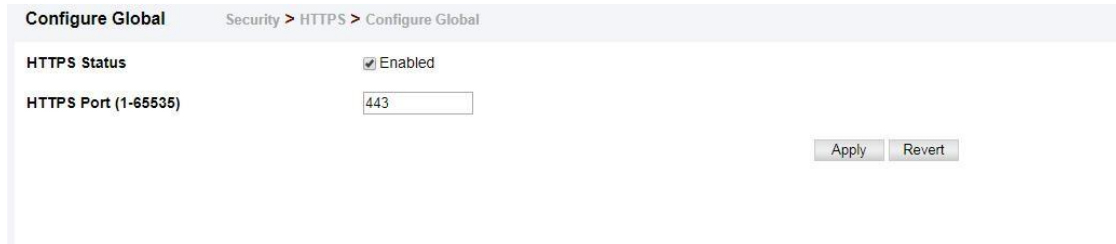
PARAMETERS

These parameters are displayed:

◆ **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch.

(Default: Enabled)

◆ **HTTPS Port** – Specifies the UDP port number used for HTTPS connection to the switch's web interface. (Default: Port 443)



Configure Global Security > HTTPS > Configure Global

HTTPS Status Enabled

HTTPS Port (1-65535)

Apply Revert

Copy Certificate

The Security > HTTPS > Copy Certificate page is used to replace the default secure-site certificate.

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that the web browser displays will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority. When you have obtained these, place them on your TFTP server and transfer them to the switch to replace the default (unrecognized) certificate with an authorized one.

PARAMETERS

These parameters are displayed:

◆ **TFTP Server IP Address** – IP address of TFTP server which contains the certificate file.

◆ **Certificate Source File Name** – Name of certificate file stored on the TFTP server.

◆ **Private Key Source File Name** – Name of private key file stored on the TFTP server.

◆ **Private Password** – Password stored in the private key file. This password is used to verify authorization for certificate use, and is verified when downloading the certificate to the switch.

◆ **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not download the certificate if these two fields do not match.

Copy Certificate Security > HTTPS > Copy Certificate

TFTP Server IP Address
 Certificate Source File Name
 Private Key Source File Name
 Private Password
 Confirm Password

Click this button to delete current certificate.

SSH

The Berkeley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks. Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkeley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

Configure Global

The Security > SSH > Configure Global page is used to enable the SSH server and configure basic settings for authentication.

PARAMETERS

These parameters are displayed:

- ◆ **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)
- ◆ **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- ◆ **Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1-120 seconds; Default: 120 seconds)
- ◆ **Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)
- ◆ **Server-Key Size** – Specifies the SSH server key size. (Range: 512-896 bits; Default: 768)
 - The server key is a private key that is never shared outside the switch.
 - The host key is shared with the SSH client, and is fixed at 1024 bits.

Configure Global Security > SSH > Configure Global

SSH Server Status Enabled

Version 2.0

Authentication Timeout (1-120) sec

Authentication Retries (1-5)

Server-Key Size (512-896)

Show Host Key

The Security > SSH > Show Host Key page is used to generate a host public/private key pair used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch.

PARAMETERS

These parameters are displayed:

◆ **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both; Default: Both) The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

◆ **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory) to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair. (Default: Disabled)

Show Host Key Security > SSH > Show Host Key

Public-Key of Host-Key

RSA

DSA

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

Show User Key

The Security > SSH > Show User Key page is used to upload a user's public key to the switch. This public key must be stored on the switch for the user to be able to log in using the public key authentication mechanism. If the user's public key does not exist on the switch, SSH will revert to the interactive password authentication mechanism to complete authentication.

PARAMETERS

These parameters are displayed:

◆ **User Name** – This drop-down box selects the user who’s public key you wish to manage.

Note that you must first create users on the User Accounts page.

◆ **User Key Type** – The type of public key to upload.

■ **RSA**: The switch accepts a RSA version 1 encrypted public key.

■ **DSA**: The switch accepts a DSA version 2 encrypted public key. The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption. The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

◆ **TFTP Server IP Address** – The IP address of the TFTP server that contains the public key file you wish to import.

◆ **Source File Name** – The public key file to upload.

Security > SSH > Show User Key

Show User Key

User Name

Public-Key of User-Key

RSA

DSA

User Name

User-Key Type

TFTP Server IP Address

Source File Name

Port Security

The Security > Port Security page is used to configure the maximum number of device MAC addresses that can be learned by a switch port, stored in the address table, and authorized to access the network. When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the address table will be authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

COMMAND USAGE

◆ The default maximum number of MAC addresses allowed on a secure port is zero (that is, disabled). To use port security, you must configure the maximum number of addresses allowed on a port.

◆ To configure the maximum number of address entries which can be learned on a port,

specify the maximum number of dynamic addresses allowed. The switch will learn up to the maximum number of allowed address pairs <source MAC address, VLAN> for frames received on the port. When the port has reached the maximum number of MAC addresses, the port will stop learning new addresses. The MAC addresses already in the address table will be retained and will not be aged out. Note that you can manually add additional secure addresses to a port using the Static Address Table .

- ◆ When the port security state is changed from enabled to disabled, all dynamically learned entries are cleared from the address table.
- ◆ If port security is enabled, and the maximum number of allowed addresses are set to a non-zero value, any device not in the address table that attempts to use the port will be prevented from accessing the switch.
- ◆ If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Interface > Port > General page.
- ◆ A secure port has the following restrictions:
 - It cannot be used as a member of a static or dynamic trunk.
 - It should not be connected to a network interconnection device.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port number.
- ◆ **Security Status** – Enables or disables port security on an interface. (Default: Disabled)
- ◆ **Port Status** – The operational status:
 - Secure/Down – Port security is disabled.
 - Secure/Up – Port security is enabled.
 - Shutdown – Port is shut down due to a response to a port security violation.
- ◆ **Action** – Indicates the action to be taken when a port security violation is detected:
 - **None**: No action should be taken. (This is the default.)
 - **Trap**: Send an SNMP trap message.
 - **Shutdown**: Disable the port.
 - **Trap and Shutdown**: Send an SNMP trap message and disable the port.
- ◆ **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled) The maximum address count is effective when port security is enabled or disabled.
- ◆ **Current MAC Count** – The number of MAC addresses currently associated with this interface.
- ◆ **MAC Filter** – Shows if MAC address filtering has been set under Security > Network Access (Configure MAC Filter) as described.
- ◆ **MAC Filter ID** – The identifier for a MAC address filter.
- ◆ **Last Intrusion MAC** – The last unauthorized MAC address detected.
- ◆ **Last Time Detected Intrusion MAC** – The last time an unauthorized MAC address was detected.

Port Security									
Security > Port Security									
Stacking Unit: 1									
Port Security List Total: 26									
Port	Security Status	Port Status	Action	Max MAC Count (0-1024)	Current MAC Count	MAC Filter	MAC Filter ID	Last Intrusion MAC	Last Time Detected Intrusion MAC
1	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
2	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
3	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
4	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
5	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
6	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
7	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
8	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
9	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
10	<input checked="" type="checkbox"/> Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA

Apply Revert

DAI

DAI is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain “man-in-the-middle” attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped. ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database. This database is built by DHCP snooping if it is enabled on globally on the switch and on the required VLANs. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured addresses.

Configure General

The Security > DAI > Configure General page is used to enable ARP inspection globally for the switch, to validate address information in each packet, and configure logging.

COMMAND USAGE

ARP Inspection Validation

- ◆ By default, ARP Inspection Validation is disabled.
- ◆ Specifying at least one of the following validations enables ARP Inspection Validation globally. Any combination of the following checks can be active concurrently.
 - Destination MAC – Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
 - IP – Checks the ARP body for invalid and unexpected IP addresses. These addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.
 - Source MAC – Checks the source MAC address in the Ethernet header against the sender

MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.


ARP Inspection Logging

- ◆ By default, logging is active for ARP Inspection, and cannot be disabled.
- ◆ The administrator can configure the log facility rate.
- ◆ When the switch drops a packet, it places an entry in the log buffer, then generates a system message on a rate-controlled basis. After the system message is generated, the entry is cleared from the log buffer.
- ◆ Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- ◆ If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- ◆ If the log buffer is full, the oldest entry will be replaced with the newest entry.

PARAMETERS

These parameters are displayed:

- ◆ **ARP Inspection Status** – Enables ARP Inspection globally. (Default: Disabled)
- ◆ **ARP Inspection Validation** – Enables extended ARP Inspection Validation if any of the following options are enabled. (Default: Disabled)
 - **Dst-MAC** – Validates the destination MAC address in the Ethernet header against the target MAC address in the body of ARP responses.
 - **IP** – Checks the ARP body for invalid and unexpected IP addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.
 - **Src-MAC** – Validates the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.
- ◆ **Log Message Number** – The maximum number of entries saved in a log message. (Range: 0-256; Default: 5)
- ◆ **Log Interval** – The interval at which log messages are sent. (Range: 0-86400 seconds; Default: 1 second)



The screenshot shows the 'Configure General' page for ARP Inspection. The breadcrumb trail is 'Security > DAI > Configure General'. The configuration options are as follows:

Parameter	Value
ARP Inspection Status	<input checked="" type="checkbox"/> Enabled
ARP Inspection Validation	<input type="checkbox"/> Dst-MAC <input type="checkbox"/> IP <input type="checkbox"/> Allow Zeros <input type="checkbox"/> Src-MAC
Log Message Number (0-256)	<input type="text" value="20"/>
Log Interval (0-86400)	<input type="text" value="10"/> sec

Buttons: Apply, Revert

Configure VLAN

The Security > DAI > Configure VLAN page is used to enable ARP inspection for any VLAN and to specify the ARP ACL to use.

COMMAND USAGE

ARP Inspection VLAN Filters (ACLs)

- ◆ By default, no ARP Inspection ACLs are configured and the feature is disabled.
- ◆ ARP Inspection ACLs are configured within the ARP ACL configuration page.
- ◆ ARP Inspection ACLs can be applied to any configured VLAN.
- ◆ ARP Inspection uses the DHCP snooping bindings database for the list of valid IP-to-MAC address bindings. ARP ACLs take precedence over entries in the DHCP snooping bindings database. The switch first compares ARP packets to any specified ARP ACLs.
- ◆ If *Static* is specified, ARP packets are only validated against the selected ACL – packets are filtered according to any matching rules, packets not matching any rules are dropped, and the DHCP snooping bindings database check is bypassed.
- ◆ If *Static* is not specified, ARP packets are first validated against the selected ACL; if no ACL rules match the packets, then the DHCP snooping bindings database determines their validity.

PARAMETERS

These parameters are displayed:

- ◆ **ARP Inspection VLAN ID** – Selects any configured VLAN. (Default: 1)
- ◆ **ARP Inspection VLAN Status** – Enables ARP Inspection for the selected VLAN. (Default: Disabled)
- ◆ **ARP Inspection ACL Name**
 - **ARP ACL** – Allows selection of any configured ARP ACLs. (Default: None)
 - **Static** – When an ARP ACL is selected, and static mode also selected, the switch only performs ARP Inspection and bypasses validation against the DHCP Snooping Bindings database. When an ARP ACL is selected, but static mode is not selected, the switch first performs ARP Inspection and then validation against the DHCP Snooping Bindings database. (Default: Disabled)

Configure VLAN Security > DAI > Configure VLAN

ARP Inspection VLAN List Total: 10

VLAN	DAI Status	ACL Name	ACL Status
1	<input checked="" type="checkbox"/> Enabled	<input type="text" value=""/>	<input type="checkbox"/> Static
2	<input checked="" type="checkbox"/> Enabled	<input type="text" value=""/>	<input type="checkbox"/> Static
3	<input checked="" type="checkbox"/> Enabled	<input type="text" value=""/>	<input type="checkbox"/> Static
4	<input checked="" type="checkbox"/> Enabled	<input type="text" value=""/>	<input type="checkbox"/> Static
5	<input checked="" type="checkbox"/> Enabled	<input type="text" value=""/>	<input type="checkbox"/> Static
6	<input checked="" type="checkbox"/> Enabled	<input type="text" value=""/>	<input type="checkbox"/> Static
7	<input checked="" type="checkbox"/> Enabled	<input type="text" value=""/>	<input type="checkbox"/> Static
8	<input checked="" type="checkbox"/> Enabled	<input type="text" value=""/>	<input type="checkbox"/> Static
9	<input checked="" type="checkbox"/> Enabled	<input type="text" value=""/>	<input type="checkbox"/> Static
10	<input checked="" type="checkbox"/> Enabled	<input type="text" value=""/>	<input type="checkbox"/> Static

Configure Interface

The Security > DAI > Configure Interface page is used to specify the ports that require ARP inspection, and to adjust the packet inspection rate.

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Port or trunk identifier.
- ◆ **Trust Status** – Configures the port as trusted or untrusted. (Default: Untrusted) By default,

all untrusted ports are subject to ARP packet rate limiting, and all trusted ports are exempt from ARP packet rate limiting. Packets arriving on trusted interfaces bypass all ARP Inspection and ARP Inspection Validation checks and will always be forwarded, while those arriving on untrusted interfaces are subject to all configured ARP inspection tests.

◆ **Packet Rate Limit** – Sets the maximum number of ARP packets that can be processed by CPU per second on trusted or untrusted ports. (Range: 0-2048; Default: 15) Setting the rate limit to “0” means that there is no restriction on the number of ARP packets that can be processed by the CPU. The switch will drop all ARP packets received on a port which exceeds the configured ARP-packets-per-second rate limit.



The screenshot shows the 'Configure Interface' page for Security > DAI > Configure Interface. It displays a table for configuring ARP Packet Rate Limit (0-2048 pps) for ports 1 through 10. All ports are currently set to 'Enabled' with a rate limit of 15 pps.

Port	Trust Status	Packet Rate Limit (0-2048 pps)
1	Enabled	15
2	Enabled	15
3	Enabled	15
4	Enabled	15
5	Enabled	15
6	Enabled	15
7	Enabled	15
8	Enabled	15
9	Enabled	15
10	Enabled	15

Show Statistics

The Security > DAI > Show Statistics page is used to display statistics about the number of ARP packets processed, or dropped for various reasons.

PARAMETERS

These parameters are displayed:

Parameter	Description
Received ARP packets before ARP inspection rate limit	Count of ARP packets received but not exceeding the ARP Inspection rate limit.
Dropped ARP packets in the process of ARP inspection rate limit	Count of ARP packets exceeding (and dropped by) ARP rate limiting.
ARP packets dropped by additional validation (IP)	Count of ARP packets that failed the IP address test.
ARP packets dropped by additional validation (Dst-MAC)	Count of packets that failed the destination MAC address test.
Total ARP packets processed by ARP inspection	Count of all ARP packets processed by the ARP Inspection engine.
ARP packets dropped by additional validation (Src-MAC)	Count of packets that failed the source MAC address test.
ARP packets dropped by ARP	Count of ARP packets that failed validation against ARP

ACLs	ACL rules.
ARP packets dropped by DHCP snooping	Count of packets that failed validation against the DHCP Snooping Binding database.

Show Statistics Security > DAI > Show Statistics

Received ARP packets before ARP inspection rate limit	0
Dropped ARP packets in processing ARP inspection rate limit	0
Total ARP packets processed by ARP inspection	0
ARP packets dropped by additional validation (Src-MAC)	0
ARP packets dropped by additional validation (Dst-MAC)	0
ARP packets dropped by additional validation (IP)	0
ARP packets dropped by ARP ACLs	0
ARP packets dropped by DHCP snooping	0

Show Log

The Security > DAI > Show Log page is used to show information about entries stored in the log, including the associated VLAN, port, and address components.

PARAMETERS

These parameters are displayed:

Parameter	Description
VLAN ID	The VLAN where this packet was seen.
Port	The port where this packet was seen.
Src. IP Address	The source IP address in the packet.
Dst. IP Address	The destination IP address in the packet.
Src. MAC Address	The source MAC address in the packet.
Dst. MAC Address	The destination MAC address in the packet.

Show Log Security > DAI > Show Log

ARP Inspection Log List Total: 0

VLAN ID	Port	Src. IP Address	Dst. IP Address	Src. MAC Address	Dst. MAC Address
---------	------	-----------------	-----------------	------------------	------------------

IP Filter

IP Filter Management

The Security > IP Filter > IP Filter Management page is used to create a list of up to 15 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.

COMMAND USAGE

- ◆ The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- ◆ If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- ◆ IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- ◆ When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- ◆ You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- ◆ You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

PARAMETERS

These parameters are displayed:

◆ Mode

■ **Web** – Configures IP address(es) for the web group.

■ **SNMP** – Configures IP address(es) for the SNMP group.

■ **Telnet** – Configures IP address(es) for the Telnet group.

◆ **Start IP Address** – A single IP address, or the starting address of a range.

◆ **End IP Address** – The end address of a range.



DoS Protection

The Security > DoS Protection page is used to protect against denial-of-service (DoS) attacks. A DoS attack is an attempt to block the services provided by a computer or network resource. This kind of attack tries to prevent an Internet site or service from functioning efficiently or at all. In general, DoS attacks are implemented by either forcing the target to reset, to consume most of its resources so that it can no longer provide its intended service, or to obstruct the communication media between the intended users and the target so that they can no longer communicate adequately. This section describes how to protect against DoS attacks.

PARAMETERS

These parameters are displayed:

◆ **Echo/Chargen Attack** – Attacks in which the echo service repeats anything sent to it, and the chargen (character generator) service generates a continuous stream of data. When

used together, they create an infinite loop and result in a denial-of-service. (Default: Disabled)

◆ **Echo/Chargen Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)

◆ **Smurf Attack** – Attacks in which a perpetrator generates a large amount of spoofed ICMP Echo Request traffic to the broadcast destination IP address (255.255.255.255), all of which uses a spoofed source address of the intended victim. The victim should crash due to the many interrupts required to send ICMP Echo response packets. (Default: Enabled)

◆ **TCP Flooding Attack** – Attacks in which a perpetrator sends a succession of TCP SYN requests (with or without a spoofed-Source IP) to a target and never returns ACK packets. These half-open connections will bind resources on the target, and no new connections can be made, resulting in a denial of service. (Default: Disabled)

◆ **TCP Flooding Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)

◆ **TCP Null Scan** – A TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. (Default: Enabled)

◆ **TCP-SYN/FIN Scan** – A TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. (Default: Enabled)

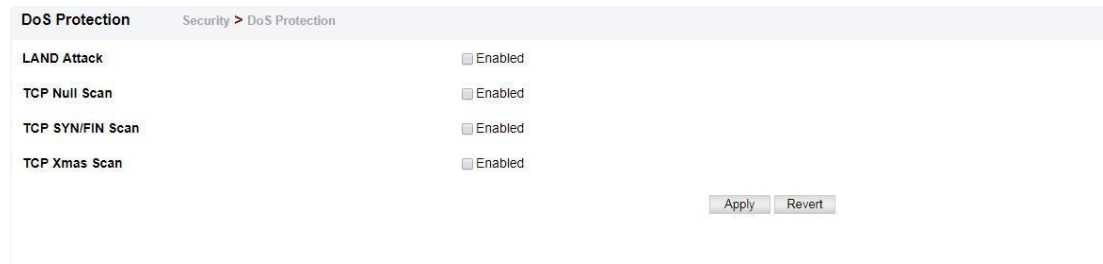
◆ **TCP Xmas Scan** – A so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target replies with a TCP RST packet.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

◆ **UDP Flooding Attack** – Attacks in which a perpetrator sends a large number of UDP packets (with or without a spoofed-Source IP) to random ports on a remote host. The target will determine that application is listening at that port, and reply with an ICMP Destination Unreachable packet. It will be forced to send many ICMP packets, eventually leading it to be unreachable by other clients. (Default: Disabled)

◆ **UDP Flooding Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)

◆ **WinNuke Attack** – Attacks in which affected the Microsoft Windows 3.1x/95/NT operating systems. In this type of attack, the perpetrator sends the string of OOB out-of-band (OOB) packets contained a TCP URG flag to the target computer on TCP port 139 (NetBIOS), casing it to lock up and display a “Blue Screen of Death.” This did not cause any damage to, or change data on, the computer’s hard disk, but any unsaved data would be lost. Microsoft made patches to prevent the WinNuke attack, but the OOB packets. (Default: Disabled)

◆ **WinNuke Attack Rate** – Maximum allowed rate. (Range: 64-2000 kbits/second; Default: 1000 kbits/second)



IPv4 DHCP Snooping

The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping (or using the static bindings configured with IP Source Guard). DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

Configure Global

Security > IPv4 DHCP Snooping > Configure Global page is used to enable DHCP Snooping globally on the switch, or to configure MAC Address Verification.

PARAMETERS

These parameters are displayed:

- ◆ **DHCP Snooping Status** – Enables DHCP snooping globally. (Default: Disabled)
- ◆ **DHCP Snooping MAC-Address Verification** – Enables or disables MAC address verification. If the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped. (Default: Enabled)
- ◆ **DHCP Snooping Rate Limit** – Sets the maximum number of DHCP packets that can be trapped by the switch for DHCP snooping. (Range: 1-2048 packets/ second)
- ◆ **DHCP Snooping Information Option Status** – Enables or disables DHCP Option 82 information relay. (Default: Disabled)
- ◆ **DHCP Snooping Information Option Sub-option Format** – Enables or disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information.
- ◆ **DHCP Snooping Information Option Remote ID** – Specifies the MAC address, IP address, or arbitrary identifier of the requesting device (i.e., the switch in this context).
- **MAC Address** – Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (i.e., the MAC address of the switch's CPU). This attribute can be encoded in Hexadecimal or ASCII.
- **IP Address** – Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (i.e., the IP address of the management interface). This attribute can be encoded in Hexadecimal or ASCII.
- **string** - An arbitrary string inserted into the remote identifier field. (Range: 1-32

characters)

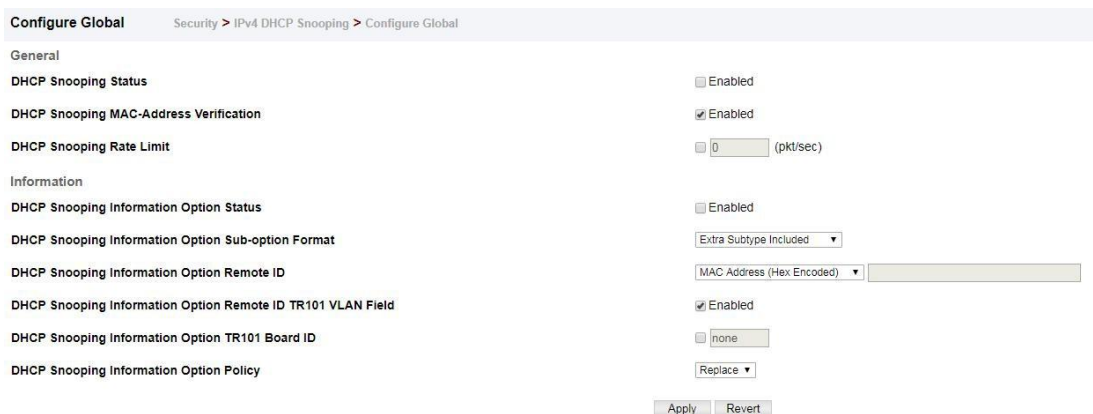
◆ **DHCP Snooping Information Option Remote ID TR101 VLAN Field** – Adds “:VLAN” in TR101 field for untagged packets. The format for TR101 option 82 is: “<IP>eth <SID>/<PORT>[:<VLAN>]”. Note that the SID (Switch ID) is always 0. By default the PVID is added to the end of the TR101 field for untagged packets. For tagged packets, the VLAN ID is always added.

◆ **DHCP Snooping Information Option Policy** – Specifies how to handle DHCP client request packets which already contain Option 82 information.

■ **Drop** – Drops the client’s request packet instead of relaying it.

■ **Keep** – Retains the Option 82 information in the client request, and forwards the packets to trusted ports.

■ **Replace** – Replaces the Option 82 information circuit-id and remote-id fields in the client’s request with information about the relay agent itself, inserts the relay agent’s address (when DHCP snooping is enabled), and forwards the packets to trusted ports. (This is the default policy.)



The screenshot shows the 'Configure Global' page for IPv4 DHCP Snooping. The breadcrumb trail is 'Security > IPv4 DHCP Snooping > Configure Global'. The page is divided into two sections: 'General' and 'Information'.
General Section:
 - DHCP Snooping Status: Disabled, Enabled
 - DHCP Snooping MAC-Address Verification: Enabled
 - DHCP Snooping Rate Limit: 0 (pkt/sec)
Information Section:
 - DHCP Snooping Information Option Status: Disabled, Enabled
 - DHCP Snooping Information Option Sub-option Format: Extra Subtype Included (dropdown)
 - DHCP Snooping Information Option Remote ID: MAC Address (Hex Encoded) (dropdown) [text input field]
 - DHCP Snooping Information Option Remote ID TR101 VLAN Field: Enabled
 - DHCP Snooping Information Option TR101 Board ID: none
 - DHCP Snooping Information Option Policy: Replace (dropdown)
 At the bottom right, there are 'Apply' and 'Revert' buttons.

Configure VLAN

Security > IPv4 DHCP Snooping > Configure VLAN page is used to enable or disable DHCP snooping on specific VLANs.

COMMAND USAGE

◆ When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.

◆ When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.

◆ When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

PARAMETERS

These parameters are displayed:

◆ **VLAN** – ID of a configured VLAN. (Range: 1-4093)

◆ **DHCP Snooping Status** – Enables or disables DHCP snooping for the selected VLAN. When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN. (Default:

Disabled)



Configure Interface

Security > IPv4 DHCP Snooping > Configure Interface page is used to configure switch ports as trusted or un-trusted.

COMMAND USAGE

- ◆ A trusted interface is an interface that is configured to receive only messages from within the network. An un-trusted interface is an interface that is configured to receive messages from outside the network or fire wall.
- ◆ When DHCP snooping is enabled both globally and on a VLAN, DHCP filtering will be performed on any un-trusted ports within the VLAN.
- ◆ When an un-trusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- ◆ Set all ports connected to DHCP servers within the local network or fire wall to trusted state. Set all other ports outside the local network or fire wall to untrusted state.

PARAMETERS

These parameters are displayed:

- ◆ **Trust Status** – Enables or disables a port as trusted. (Default: Disabled)
- ◆ **Circuit ID** – Specifies DHCP Option 82 circuit ID suboption information.
- **Mode** – Specifies the default string “VLAN-Unit-Port” or an arbitrary string. (Default: VLAN-Unit-Port)
- **Value** – An arbitrary string inserted into the circuit identifier field. (Range: 1-32 characters)

Show Information

Security > IPv4 DHCP Snooping > Show Information page is used to display entries in the binding table.

PARAMETERS

These parameters are displayed:

- ◆ **MAC Address** – Physical address associated with the entry.
- ◆ **IP Address** – IP address corresponding to the client.
- ◆ **Lease Time** – The time for which this IP address is leased to the client.
- ◆ **Type** – Entry types include:
 - **DHCP-Snooping** – Dynamically snooped.
 - **Static-DHCPSPNP** – Statically configured.
- ◆ **VLAN** – VLAN to which this entry is bound.

- ◆ **Interface** – Port or trunk to which this entry is bound.
- ◆ **Store** – Writes all dynamically learned snooping entries to flash memory. This function can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.
- ◆ **Clear** – Removes all dynamically learned snooping entries from flash memory.

Show Information Security > IPv6 DHCP Snooping > Show Information

DHCP Snooping Binding List Total: 0

MAC Address	IP Address	Lease Time (seconds)	Type	VLAN	Interface
-------------	------------	----------------------	------	------	-----------

IPv6 DHCP Snooping

The addresses assigned to DHCPv6 clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCPv6 Snooping (or using the static bindings configured with IPv6 Source Guard). DHCPv6 snooping allows a switch to protect a network from rogue DHCPv6 servers or other devices which send port-related information to a DHCPv6 server. This information can be useful in tracking an IP address back to a physical port.

COMMAND USAGE

DHCP Snooping Process

- ◆ Network traffic may be disrupted when malicious DHCPv6 messages are received from an outside source. DHCPv6 snooping is used to filter DHCPv6 messages received on a unsecure interface from outside the network or fire wall. When DHCPv6 snooping is enabled globally and enabled on a VLAN interface, DHCPv6 messages received on an untrusted interface from a device not listed in the DHCPv6 snooping table will be dropped.
- ◆ When enabled, DHCPv6 messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCPv6 snooping.
- ◆ Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IPv6 address, lease time, binding type, VLAN identifier, and port identifier.
- ◆ When DHCPv6 snooping is enabled, the rate limit for the number of DHCPv6 messages that can be processed by the switch is 100 packets per second. Any DHCPv6 packets in excess of this limit are dropped.

Configure Global

Security > IPv6 DHCP Snooping > Configure Global page is used to enable DHCPv6 Snooping globally on the switch, or to configure MAC Address Verification.

PARAMETERS

These parameters are displayed:

- ◆ **DHCPv6 Snooping Status** – Enables DHCPv6 snooping globally. (Default: Disabled)
- ◆ **DHCPv6 Snooping Option Remote ID** – Enables the insertion of remote-id option 37 information into DHCPv6 client messages. Remote-id option information such as the port

attached to the client, DUID, and VLAN ID is used by the DHCPv6 server to assign pre-assigned configuration data specific to the DHCPv6 client. (Default: Disabled)

- DHCPv6 provides a relay mechanism for sending information about the switch and its DHCPv6 clients to the DHCPv6 server. Known as DHCPv6 Option 37, it allows compatible DHCPv6 servers to use the information when assigning IP addresses, or to set other services or policies for clients.

- When DHCPv6 Snooping Information Option 37 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCPv6 request packets forwarded by the switch and in reply packets sent back from the DHCPv6 server.

- When the DHCPv6 Snooping Option 37 is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCPv6 client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.

- DHCPv6 snooping must be enabled for the DHCPv6 Option 37 information to be inserted into packets. When enabled, the switch will either drop, keep or remove option 37 information in incoming DHCPv6 packets. Packets are processed as follows:

- If an incoming packet is a DHCPv6 request packet with option 37 information, it will modify the option 37 information according to the settings specified.

- If an incoming packet is a DHCPv6 request packet without option 37 information, enabling the DHCPv6 snooping information option will add option 37 information to the packet.

- If an incoming packet is a DHCPv6 reply packet with option 37 information, enabling the DHCPv6 snooping information option will remove option 37 information from the packet.

- When this switch inserts Option 37 information in DHCPv6 client request packets, the switch's MAC address (hexadecimal) is used for the remote ID.

- ◆ **DHCPv6 Snooping Option Policy** – Sets the remote-id option policy for DHCPv6 client packets that include Option 37 information. When the switch receives DHCPv6 packets from clients that already include DHCP Option 37 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCPv6 packets, keep the existing information, or replace it with the switch's relay agent information.

- **Drop** – Drops the client's request packet instead of relaying it (This is the default policy).

- **Keep** – Retains the Option 82 information in the client request, and forwards the packets to trusted ports.

- **Replace** – Replaces the Option 37 remote-ID in the client's request with the relay agent's remote-ID (when DHCPv6 snooping is enabled), and forwards the packets to trusted ports.

Configure Global Security > IPv6 DHCP Snooping > Configure Global

DHCPv6 Snooping Status	<input type="checkbox"/> Enabled
DHCPv6 Snooping Option Remote ID	<input type="checkbox"/> Enabled
DHCPv6 Snooping Option Policy	Drop ▼

VLAN Management

Security > IPv6 DHCP Snooping > VLAN Management page is used to enable or disable DHCPv6 snooping on specific VLANs.

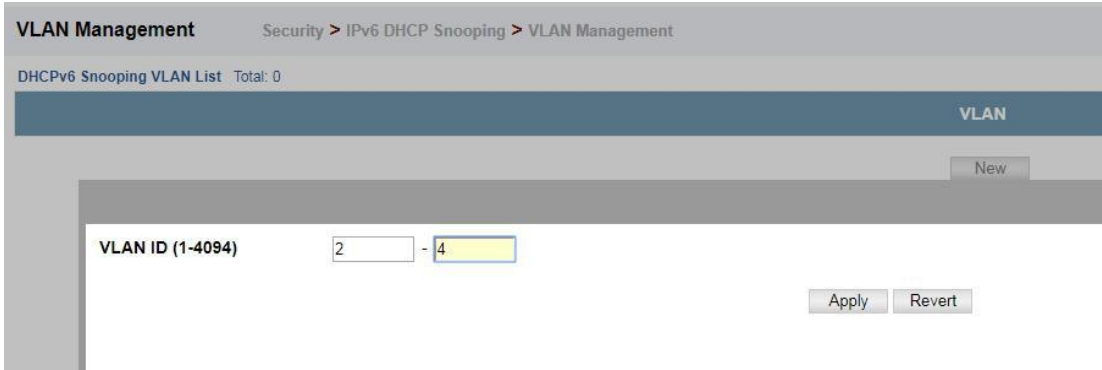
COMMAND USAGE

- ◆ When DHCPv6 snooping enabled globally and enabled on a VLAN, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN.
- ◆ When the DHCPv6 snooping is globally disabled, DHCPv6 snooping can still be configured for specific VLANs, but the changes will not take effect until DHCPv6 snooping is globally re-enabled.
- ◆ When DHCPv6 snooping is enabled globally, and then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

PARAMETERS

These parameters are displayed:

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



The screenshot shows the 'VLAN Management' page. At the top, the breadcrumb navigation is 'Security > IPv6 DHCP Snooping > VLAN Management'. Below this, it indicates 'DHCPv6 Snooping VLAN List Total: 0'. A table with the header 'VLAN' is visible, with a 'New' button to its right. The table contains one entry with 'VLAN ID (1-4094)' and two input fields containing the values '2' and '4', separated by a hyphen. Below the input fields are 'Apply' and 'Revert' buttons.

Configure Interface

Security > IPv6 DHCP Snooping > Configure Interface page is used to configure switch interfaces as trusted or untrusted, and set the maximum number of entries which can be stored in the binding database for an interface.

COMMAND USAGE

- ◆ A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.
- ◆ Set all interfaces connected to DHCPv6 servers within the local network or fire wall to trusted, and all other interfaces outside the local network or fire wall to untrusted.
- ◆ When DHCPv6 snooping is enabled globally and enabled on a VLAN, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface.
- ◆ When an untrusted port is changed to a trusted port, all the dynamic DHCPv6 snooping bindings associated with this port are removed.
- ◆ Additional considerations when the switch itself is a DHCPv6 client – The port(s) through which it submits a client request to the DHCPv6 server must be configured as trusted.

PARAMETERS

These parameters are displayed:

- ◆ **Interface** – Port or trunk identifier.
- ◆ **Trust Status** – Enables or disables an interface as trusted. (Default: Disabled)
- ◆ **Max Binding** – Sets the maximum number of entries which can be stored in the binding database for an interface. (Range: 1-5; Default: 5)
- ◆ **Current Binding** – Shows the maximum number of entries which can be stored in the binding database for an interface.

Configure Interface Security > IPv6 DHCP Snooping > Configure Interface

DHCPv6 Snooping Interface List Total: 50

Interface	Trust Status	Max Binding (1 - 5)	Current Binding
Eth 1/1	<input checked="" type="checkbox"/> Enabled	5	0
Eth 1/2	<input checked="" type="checkbox"/> Enabled	5	0
Eth 1/3	<input checked="" type="checkbox"/> Enabled	5	0

Show Information

Security > IPv6 DHCP Snooping > Show Information page is used to display entries in the binding table.

PARAMETERS

These parameters are displayed:

- ◆ **Link-layer Address** – IPv6 link-layer address associated with the entry.
- ◆ **IPv6 Address** – IPv6 address corresponding to the client.
- ◆ **Lifetime** – The time (number of seconds) for which this IPv6 address is leased to the client.
- ◆ **VLAN** – VLAN to which this entry is bound.
- ◆ **Interface** – Port or trunk to which this entry is bound.
- ◆ **Type** – Entry types include:
 - **NA** – Non-temporary address.
 - **TA** – Temporary address.
- ◆ **Clear** – Removes all dynamically learned snooping entries from RAM.

Show Information Security > IPv6 DHCP Snooping > Show Information

● Binding ● Statistics

DHCPv6 Snooping Binding List Total: 0

Link-layer Address	IPv6 Address	Lifetime	VLAN	Interface	Type
--------------------	--------------	----------	------	-----------	------

IPv4 Source Guard

IPv4 Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table when enabled. IP source guard can be used to prevent traffic attacks caused when a host tries to use the IPv4 address of a neighbor to access the network. This section describes how to configure IPv4 Source Guard.

General

Security > IP Source Guard > Port Configuration page is used to set the filtering type based on source IP address, or source IP address and MAC address pairs. IP Source Guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.

COMMAND USAGE

◆ Setting source guard mode to SIP (Source IP) or SIP-MAC (Source IP and MAC) enables this function on the selected port. Use the SIP option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the SIP-MAC option to check these same parameters, plus the source MAC address. If no matching entry is found, the packet is dropped.

◆ When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table.

◆ If IP source guard is enabled, an inbound packet's IP address (SIP option) or both its IP address and corresponding MAC address (SIP-MAC option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.

◆ Filtering rules are implemented as follows:

■ If DHCP snooping is disabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the SIP-MAC option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.

■ If DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the SIP-MAC option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.

■ If IP source guard is enabled on an interface for which IP source bindings have not yet been configured (neither by static configuration in the IP source guard binding table nor dynamically learned from DHCP snooping), the switch will drop all IP traffic on that port, except for DHCP packets.

PARAMETERS

These parameters are displayed:

◆ **Filter Type** – Configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. (Default: None)

■ **None** – Disables IP source guard filtering on the port.

■ **SIP** – Enables traffic filtering based on IP addresses stored in the binding table.

■ **SIP-MAC** – Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.

◆ **Max Binding Entry** – The maximum number of entries that can be bound to an interface. (Range: 1-5; Default: 5) This parameter sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping and static entries set by IP source guard.

General Security > IPv4 Source Guard > General Stacking Unit: 1

Port Configuration List Total: 50

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

Apply Revert

ACL Table

Security > IPv4 Source Guard > ACL Table page is used to bind a valid static IP source guard entry to a port in ACL mode.

COMMAND USAGE

◆ Static bindings are processed as follows:

- A valid static IP source guard entry will be added to the binding table in ACL mode if one of the following conditions is true:
 - If there is no entry with the same VLAN ID and MAC address, a new entry is added to the binding table using the type “static IP source guard binding.”
 - If there is an entry with the same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
 - If there is an entry with the same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

PARAMETERS

These parameters are displayed:

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

ACL Table Security > IPv4 Source Guard > ACL Table Stacking Unit: 1

Static Binding List Total: 0

MAC Address	IP Address	VLAN	Interface
New			

Port:

VLAN:

MAC Address: (00:00:00:00:00:00 or xxxxxxxxxxxx)

IP Address:

X Close

Apply Revert

MAC Table

Security > IPv4 Source Guard > MAC Table page is used to bind a valid static IP source guard

entry to a port in MAC mode.

COMMAND USAGE

◆ Static bindings are processed as follows:

■ A valid static IP source guard entry will be added to the binding table in MAC mode if one of the following conditions are true:

■ If there is no binding entry with the same IP address and MAC address, a new entry will be added to the binding table using the type of static IP source guard binding entry.

■ If there is a binding entry with same IP address and MAC address, then the new entry shall replace the old one.

PARAMETERS

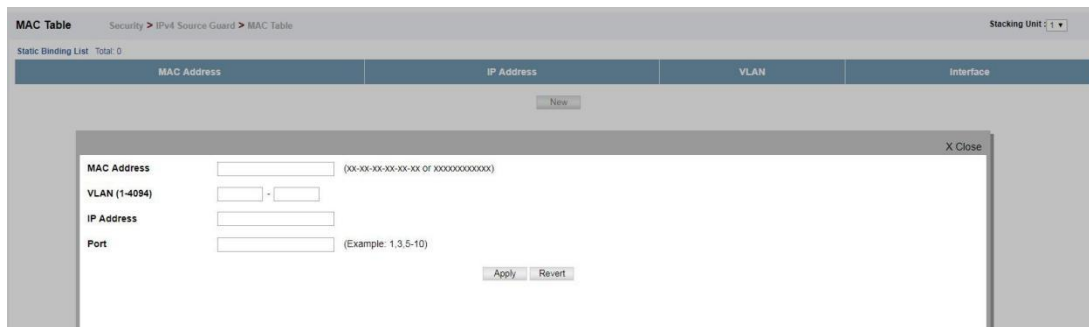
These parameters are displayed:

◆ **MAC Address** – A valid unicast MAC address.

◆ **VLAN** – ID of a configured VLAN or a range of VLANs. (Range: 1-4094)

◆ **IP Address** – A valid unicast IP address, including classful types A, B or C.

◆ **Port** – The port to which a static entry is bound. Specify a physical port number or list of port numbers. Separate nonconsecutive port numbers with a comma and no spaces; or use a hyphen to designate a range of port numbers.(Range: 1-26/28/52)



Dynamic Binding

Security > IPv4 Source Guard > Dynamic Binding page is used to display the source-guard binding table for a selected interface.

PARAMETERS

These parameters are displayed:

Query by

◆ **Port** – A port on this switch.

◆ **VLAN** – ID of a configured VLAN (Range: 1-4093)

◆ **MAC Address** – A valid unicast MAC address.

◆ **IP Address** – A valid unicast IP address, including classful types A, B or C.

Dynamic Binding List

◆ **VLAN** – VLAN to which this entry is bound.

◆ **MAC Address** – Physical address associated with the entry.

◆ **Interface** – Port to which this entry is bound.

◆ **IP Address** – IP address corresponding to the client.

◆ **Lease Time** – The time for which this IP address is leased to the client.

Dynamic Binding Security > IPv4 Source Guard > Dynamic Binding Stacking Unit: 1

Query by:

Port

VLAN

MAC Address

IP Address

Dynamic Binding List Total: 0

VLAN	MAC Address	Interface	IP Address	Type
------	-------------	-----------	------------	------

IPv6 Source Guard

IPv6 Source Guard is a security feature that filters IPv6 traffic on non-routed, Layer 2 network interfaces based on manually configured entries in the IPv6 Source Guard table, or dynamic entries in the Neighbor Discovery Snooping table or DHCPv6 Snooping table when either snooping protocol is enabled (refer to the DHCPv6 Snooping commands in the CLI Reference Guide). IPv6 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv6 address of a neighbor to access the network. This section describes how to configure IPv6 Source Guard.

Port Configuration

Security > IPv6 Source Guard > Port Configuration page is used to filter inbound traffic based on the source IPv6 address stored in the binding table. IPv6 Source Guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IPv6 address of a neighbor.

COMMAND USAGE

- ◆ Setting source guard mode to SIP (Source IP) enables this function on the selected port. Use the SIP option to check the VLAN ID, IPv6 global unicast source IP address, and port number against all entries in the binding table.
- ◆ After IPv6 source guard is enabled on an interface, the switch initially blocks all IPv6 traffic received on that interface, except for ND packets allowed by ND snooping and DHCPv6 packets allowed by DHCPv6 snooping. A port access control list (ACL) is applied to the interface. Traffic is then filtered based upon dynamic entries learned via ND snooping or DHCPv6 snooping, or static addresses configured in the source guard binding table. The port allows only IPv6 traffic with a matching entry in the binding table and denies all other IPv6 traffic.
- ◆ Table entries include a MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Binding, Dynamic-DHCPv6-Binding), VLAN identifier, and port identifier.
- ◆ Static addresses entered in the source guard binding table (using the Static Binding page) are automatically configured with an infinite lease time. Dynamic entries learned via DHCPv6 snooping are configured by the DHCPv6 server itself.
- ◆ If IPv6 source guard is enabled, an inbound packet's source IPv6 address will be checked

against the binding table. If no matching entry is found, the packet will be dropped.

◆ Filtering rules are implemented as follows:

■ If ND snooping and DHCPv6 snooping are disabled, IPv6 source guard will check the VLAN ID, source IPv6 address, and port number. If a matching entry is found in the binding table and the entry type is static IPv6 source guard binding, the packet will be forwarded.

■ If ND snooping or DHCP snooping is enabled, IPv6 source guard will check the VLAN ID, source IP address, and port number. If a matching entry is found in the binding table and the entry type is static IPv6 source guard binding, dynamic ND snooping binding, or dynamic DHCPv6 snooping binding, the packet will be forwarded.

■ If IPv6 source guard is enabled on an interface for which IPv6 source bindings (dynamically learned via ND snooping or DHCPv6 snooping, or manually configured) are not yet configured, the switch will drop all IPv6 traffic on that port, except for ND packets and DHCPv6 packets allowed by DHCPv6 snooping.

■ Only IPv6 global unicast addresses are accepted for static bindings.

PARAMETERS

◆ **Port** – Port identifier.

◆ **Filter Type** – Configures the switch to filter inbound traffic based on the following options. (Default: Disabled)

■ **Disabled** – Disables IPv6 source guard filtering on the port.

■ **SIP** – Enables traffic filtering based on IPv6 global unicast source IPv6 addresses stored in the binding table.

◆ **Max Binding Entry** – The maximum number of entries that can be bound to an interface. (Range: 1-5; Default: 5)

■ This parameter sets the maximum number of IPv6 global unicast source IPv6 address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by ND snooping, DHCPv6 snooping .

■ IPv6 source guard maximum bindings must be set to a value higher than DHCPv6 snooping maximum bindings and ND snooping maximum bindings.

■ If IPv6 source guard, ND snooping, and DHCPv6 snooping are enabled on a port, the dynamic bindings used by ND snooping, DHCPv6 snooping, and IPv6 source guard static bindings cannot exceed the maximum allowed bindings set by this parameter. In other words, no new entries will be added to the IPv6 source guard binding table.

■ If IPv6 source guard is enabled on a port, and the maximum number of allowed bindings is changed to a lower value, precedence is given to deleting entries learned through DHCPv6 snooping, ND snooping, and then manually configured IPv6 source guard static bindings, until the number of entries in the binding table reaches the newly configured maximum number of allowed bindings.

Port Configuration Security > IPv6 Source Guard > Port Configuration

Port Configuration List Total: 50

Port	Filter Type	Max Binding Entry (1-5)
1	Disabled ▾	5 <input type="text"/>
2	Disabled ▾	5 <input type="text"/>
3	Disabled ▾	5 <input type="text"/>
4	Disabled ▾	5 <input type="text"/>
5	Disabled ▾	5 <input type="text"/>
6	Disabled ▾	5 <input type="text"/>
7	Disabled ▾	5 <input type="text"/>
8	Disabled ▾	5 <input type="text"/>
9	Disabled ▾	5 <input type="text"/>
10	Disabled ▾	5 <input type="text"/>

Static Binding

Use the Security > IPv6 Source Guard > Static Binding page to bind a static address to a port. Table entries include a MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Binding, Dynamic-DHCPv6-Binding), VLAN identifier, and port identifier.

COMMAND USAGE

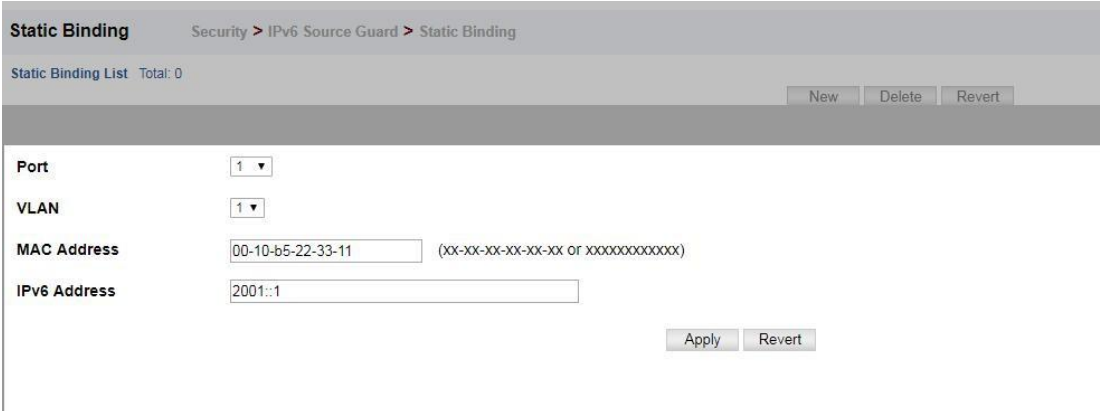
- ◆ Traffic filtering is based only on the source IPv6 address, VLAN ID, and port number.
- ◆ Static addresses entered in the source guard binding table are automatically configured with an infinite lease time.
- ◆ When source guard is enabled, traffic is filtered based upon dynamic entries learned via ND snooping, DHCPv6 snooping, or static addresses configured in the source guard binding table.
- ◆ An entry with same MAC address and a different VLAN ID cannot be added to the binding table.
- ◆ Static bindings are processed as follows:
 - If there is no entry with same MAC address and IPv6 address, a new entry is added to binding table using static IPv6 source guard binding.
 - If there is an entry with same MAC address and IPv6 address, and the type of entry is static IPv6 source guard binding, then the new entry will replace the old one.
 - If there is an entry with same MAC address and IPv6 address, and the type of the entry is either a dynamic ND snooping binding or DHCPv6 snooping binding, then the new entry will replace the old one and the entry type will be changed to static IPv6 source guard binding.
 - Only unicast addresses are accepted for static bindings.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – The port to which a static entry is bound.
- ◆ **VLAN** – ID of a configured VLAN (Range: 1-4094)
- ◆ **MAC Address** – A valid unicast MAC address.
- ◆ **IPv6 Address** – A valid global unicast IPv6 address. This address must be entered according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit

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



Static Binding Security > IPv6 Source Guard > Static Binding

Static Binding List Total: 0

New Delete Revert

Port: 1

VLAN: 1

MAC Address: 00-10-b5-22-33-11 (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)

IPv6 Address: 2001::1

Apply Revert

Dynamic Binding

Security > IPv6 Source Guard > Dynamic Binding page is used to display the source-guard binding table for a selected interface.

PARAMETERS

These parameters are displayed:

Query by

- ◆ **Port** – A port on this switch.
- ◆ **VLAN** – ID of a configured VLAN (Range: 1-4094)
- ◆ **MAC Address** – A valid unicast MAC address.
- ◆ **IPv6 Address** – A valid global unicast IPv6 address.

Dynamic Binding List

- ◆ **VLAN** – VLAN to which this entry is bound.
- ◆ **MAC Address** – Physical address associated with the entry.
- ◆ **Interface** – Port to which this entry is bound.
- ◆ **IPv6 Address** – IPv6 address corresponding to the client.
- ◆ **Type** – Shows the entry type:
 - **DHCP** – Dynamic DHCPv6 binding, stateful address.
 - **ND** – Dynamic Neighbor Discovery binding, stateless address.



Dynamic Binding Security > IPv6 Source Guard > Dynamic Binding Stacking Unit: 1

Query by:

Port: 1

VLAN: 1

MAC Address: (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)

IPv6 Address:

Query

Dynamic Binding List Total: 0

VLAN	MAC Address	Interface	IPv6 Address	Type
------	-------------	-----------	--------------	------

Application Filter

Use the Security > Application Filter page to forward CDP or PVST packets.

COMMAND USAGE

If this feature is not enabled, the switch will handle CDP or PVST packets as normal packets. In other words, they are forwarded to other ports in the same VLAN that are also configured to forward the specified packet type.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier (Range: 1-26/28/52)
- ◆ **CDP** – Cisco Discovery Protocol
- ◆ **PVST** – Per-VLAN Spanning Tree

Application Filter Security > Application Filter

Application Filter List Total: 50

Port	CDP	PVST
1	Default ▾	Default ▾
2	Default ▾	Default ▾
3	Default ▾	Default ▾
4	Default ▾	Default ▾
5	Default ▾	Default ▾
6	Default ▾	Default ▾
7	Default ▾	Default ▾
8	Default ▾	Default ▾
9	Default ▾	Default ▾
10	Default ▾	Default ▾

Apply Revert

CPU Guard

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

PARAMETERS

The following parameters are displayed:

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

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

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

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

CPU Guard Security > CPU Guard	
CPU Guard Status	<input checked="" type="checkbox"/> Enabled
High Watermark (20-100)	<input type="text" value="90"/> %
Low Watermark (20-100)	<input type="text" value="70"/> %
Maximum Threshold (50-500)	<input type="text" value="500"/> packets/sec
Minimum Threshold (50-500)	<input type="text" value="50"/> packets/sec
Trap Status	<input type="checkbox"/> Enabled
Current Threshold	500 packets/sec

Device Management

SNMP

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems. Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network. The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using network management software. Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication. Access to the switch from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. The SNMPv3 security structure consists of security models,

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

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

Configure Global

Device Management > SNMP > Configure Global page is used to enable SNMPv3 service for all management clients (i.e., versions 1, 2c, 3), and to enable trap messages.

PARAMETERS

These parameters are displayed:

- ◆ **Agent Status** – Enables SNMP on the switch. (Default: Enabled)
- ◆ **Authentication Traps10** – Issues a notification message to specified IP trap managers

whenever an invalid community string is submitted during the SNMP access authentication process. (Default: Enabled)

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

Configure Global		Device Management > SNMP > Configure Global	
Agent Status	<input checked="" type="checkbox"/>	Enabled	
Authentication Traps	<input checked="" type="checkbox"/>	Enabled	
		<input type="button" value="Apply"/>	<input type="button" value="Revert"/>

Community

Device Management > SNMP > Community page is used to configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. For security reasons, you should consider removing the default strings.

PARAMETERS

These parameters are displayed:

◆ **Community String** – A community string that acts like a password and permits access to the SNMP protocol. Range: 1-32 characters, case sensitive Default strings: “public” (Read-Only), “private” (Read/Write)

◆ **Access Mode** – Specifies the access rights for the community string:

■ **Read-Only** – Authorized management stations are only able to retrieve MIB objects.

■ **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

Community			Device Management > SNMP > Community	
SNMP Community String List Total: 2				
	Community String	Access Mode		
<input type="checkbox"/>	public	Read-Only		
<input type="checkbox"/>	private	Read/Write		
			<input type="button" value="New"/>	<input type="button" value="Delete"/>
			<input type="button" value="Revert"/>	

Set Engine ID

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

CLI REFERENCES

◆ "snmp-server engine-id"

COMMAND USAGE

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

cleared. You will need to reconfigure all existing users.

PARAMETERS

These parameters are displayed:

◆ **Engine ID** – A new engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value “123456789” is equivalent to “1234567890”.

◆ **Engine Boots** – The number of times that the engine has (re-)initialized since the SNMP EngineID was last configured.

Set Engine ID	
Device Management > SNMP > Set Engine ID	
Engine ID	<input type="text" value="8000c7be030000010300010000"/>
Engine Boots	<input type="text" value="55"/>
<input type="button" value="Default"/> <input type="button" value="Save"/>	

Remote Engine

Device Management > SNMP > Remote Engine page is used to configure a engine ID for a remote management station. To allow management access from an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host.

COMMAND USAGE

◆ SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent’s SNMP engine ID before you can send proxy requests or informs to it.

PARAMETERS

These parameters are displayed:

◆ **Remote Engine ID** – The engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value “123456789” is equivalent to “1234567890”.

◆ **Remote IP Host** – The IP address of a remote management station which is using the specified engine ID.

Remote Engine Device Management > SNMP > Remote Engine

SNMPv3 Remote Engine List Total: 0

Remote Engine ID	Remote IP Host
New	

Remote Engine ID

Remote IP Host

[Apply](#) [Revert](#)

View

Device Management > SNMP > View page is used to configure SNMPv3 views which are used to restrict user access to specified portions of the MIB tree. The predefined view "defaultview" includes access to the entire MIB tree.

CLI REFERENCES

◆ "snmp-server view"

PARAMETERS

These parameters are displayed:

Add View

- ◆ **View Name** – The name of the SNMP view. (Range: 1-64 characters)
- ◆ **OID Subtree** – Specifies the initial object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. Use the Add OID Subtree page to configure additional object identifiers.
- ◆ **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Add OID Subtree

- ◆ **View Name** – Lists the SNMP views configured in the Add View page.
- ◆ **OID Subtree** – Adds an additional object identifier of a branch within the MIB tree to the selected View. Wild cards can be used to mask a specific portion of the OID string.
- ◆ **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

View Device Management > SNMP > View

SNMPv3 View List Total: 1

	View Name
<input type="checkbox"/>	defaultview

[New](#) [Delete](#) [Revert](#)

View Name

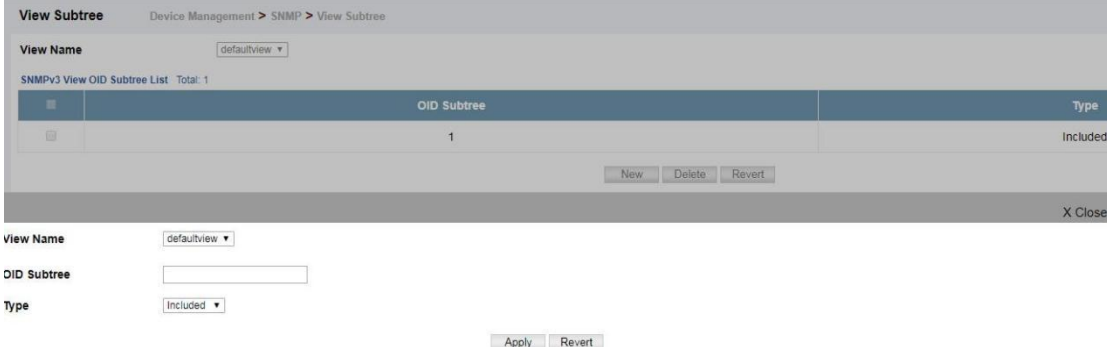
OID Subtree

Type

[Apply](#) [Revert](#)

View Subtree

Device Management > SNMP > View Subtree page is used to add an object identifier to an existing SNMP view of the switch's MIB.



View Subtree Device Management > SNMP > View Subtree

View Name

SNMPv3 View OID Subtree List Total: 1

	OID Subtree	Type
<input type="checkbox"/>	1	Included

X Close

View Name

OID Subtree

Type

Group

Device Management > SNMP > Group page is used to add an SNMPv3 group which can be used to set the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

PARAMETERS

These parameters are displayed:

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

Group Device Management > SNMP > Group

SNMPv3 Group List Total: 4

	Group Name	Model	Level	Read View	Write View	Notify View
<input type="checkbox"/>	public	v1	noAuthNoPriv	defaultview	No writeview specified	No notifyview specified
<input type="checkbox"/>	public	v2c	noAuthNoPriv	defaultview	No writeview specified	No notifyview specified
<input type="checkbox"/>	private	v1	noAuthNoPriv	defaultview	defaultview	No notifyview specified
<input type="checkbox"/>	private	v2c	noAuthNoPriv	defaultview	defaultview	No notifyview specified

New Delete Revert

X Close

Group Name

Security Model

Security Level

Read View

Write View

Notify View

Apply Revert

SNMPv3 Local User

Device Management > SNMP > SNMPv3 Local User page is used to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

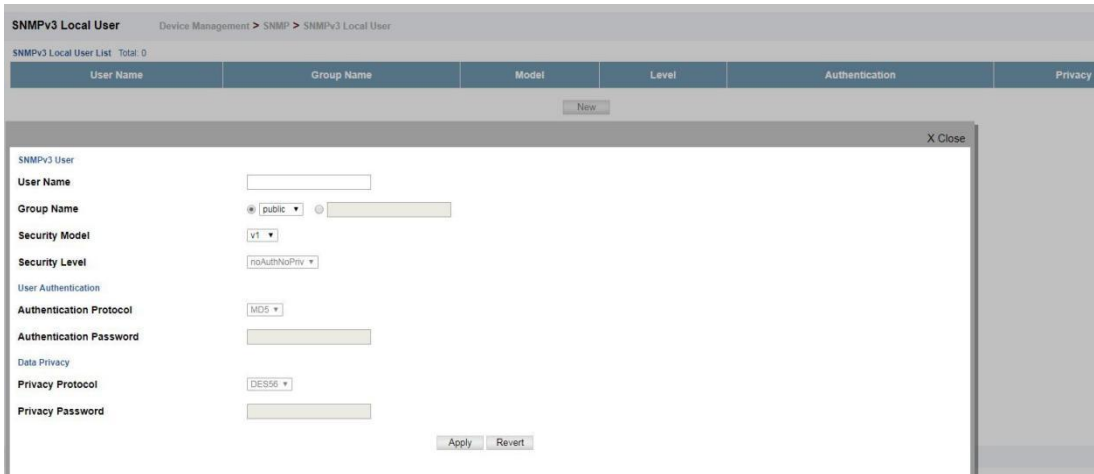
CLI REFERENCES

◆ "snmp-server user"

PARAMETERS

These parameters are displayed:

- ◆ **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- ◆ **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- ◆ **Security Model** – The user security model; SNMP v1, v2c or v3.
- ◆ **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
 - **AuthPriv** – SNMP communications use both authentication and encryption.
- ◆ **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- ◆ **Authentication Password** – A minimum of eight plain text characters is required.
- ◆ **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- ◆ **Privacy Password** – A minimum of eight plain text characters is required.



Change SNMPv3 Local User

Device Management > SNMP > Change SNMPv3 Local User Group page is used to modify group of specify local user.



SNMPv3 Remote User

Device Management > SNMP > SNMPv3 Remote User page is used to identify the source of SNMPv3 inform messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

COMMAND USAGE

◆ To grant management access to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and the remote user.

PARAMETERS

These parameters are displayed:

- ◆ **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- ◆ **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- ◆ **Remote IP** – The Internet address of the remote device where the user resides.
- ◆ **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v3)

◆ **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:

■ **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)

■ **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.

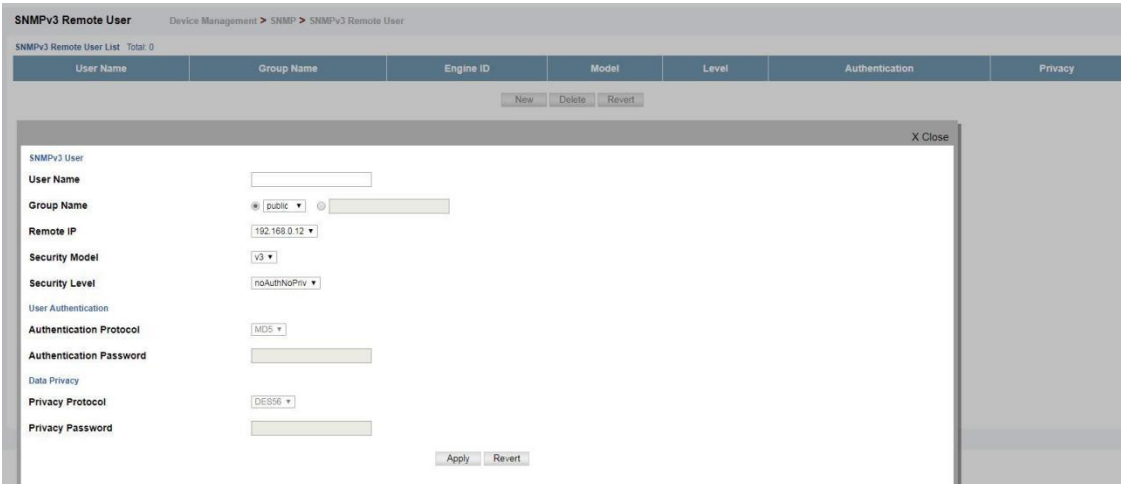
■ **AuthPriv** – SNMP communications use both authentication and encryption.

◆ **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)

◆ **Authentication Password** – A minimum of eight plain text characters is required.

◆ **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.

◆ **Privacy Password** – A minimum of eight plain text characters is required.



The screenshot displays the 'SNMPv3 Remote User' configuration page. At the top, there is a breadcrumb trail: 'Device Management > SNMP > SNMPv3 Remote User'. Below this is a table header for 'SNMPv3 Remote User List' with columns: 'User Name', 'Group Name', 'Engine ID', 'Model', 'Level', 'Authentication', and 'Privacy'. The table currently shows 'Total: 0' users. Below the table are 'New', 'Delete', and 'Revert' buttons. A modal window titled 'SNMPv3 User' is open, showing the configuration form for a new user. The form includes the following fields:

- User Name: [Text input field]
- Group Name: [Dropdown menu showing 'public' and a search icon]
- Remote IP: [Dropdown menu showing '192.168.0.12']
- Security Model: [Dropdown menu showing 'v3']
- Security Level: [Dropdown menu showing 'noAuthNoPriv']
- User Authentication:
 - Authentication Protocol: [Dropdown menu showing 'MD5']
 - Authentication Password: [Text input field]
- Data Privacy:
 - Privacy Protocol: [Dropdown menu showing 'DES56']
 - Privacy Password: [Text input field]

At the bottom of the modal window are 'Apply' and 'Revert' buttons.

Trap

Device Management > SNMP > Trap is used page to specify the host devices to be sent traps and the types of traps to send. Traps indicating status changes are issued by the switch to the specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management software). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

COMMAND USAGE

◆ Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

To send an inform to a SNMPv2c host, complete these steps:

1. Enable the SNMP agent .
2. Create a view with the required notification messages .

3. Configure the group (matching the community string specified on the Configure Trap - Add page) to include the required notify view.

4. Enable trap informs as described in the following pages.

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

1. Enable the SNMP agent .

2. Create a local SNMPv3 user to use in the message exchange process . If the user specified in the trap configuration page does not exist, an SNMPv3 group will be automatically created using the name of the specified local user, and default settings for the read, write, and notify view.

3. Create a view with the required notification messages .

4. Create a group that includes the required notify view .

5. Enable trap informs as described in the following pages.

PARAMETERS

These parameters are displayed:

SNMP Version 1

◆ **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).

◆ **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Default: v1)

◆ **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive) Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.

◆ **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

SNMP Version 2c

◆ **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).

◆ **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.

◆ **Notification Type**

■ **Traps** – Notifications are sent as trap messages.

■ **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)

■ **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)

■ **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

◆ **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive) Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.

◆ **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

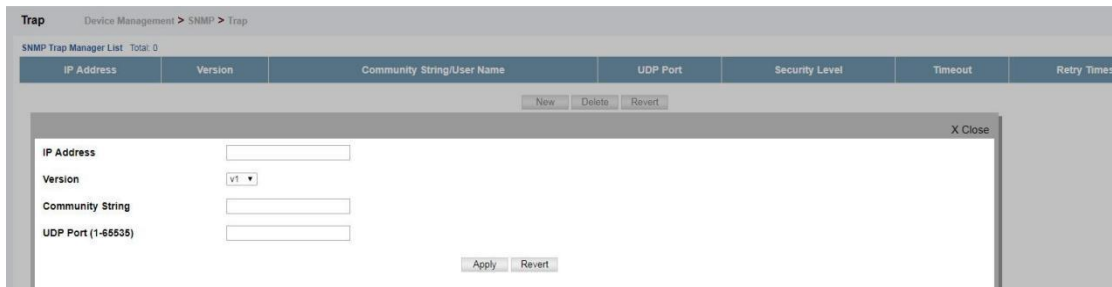
SNMP Version 3

◆ **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).

◆ **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.

◆ **Notification Type**

- **Traps** – Notifications are sent as trap messages.
- **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
- **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
- **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- ◆ **Local User Name** – The name of a local user which is used to identify the source of SNMPv3 trap messages sent from the local switch. (Range: 1-32 characters) If an account for the specified user has not been created, one will be automatically generated.
- ◆ **Remote User Name** – The name of a remote user which is used to identify the source of SNMPv3 inform messages sent from the local switch. (Range: 1-32 characters) If an account for the specified user has not been created, one will be automatically generated.
- ◆ **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)
- ◆ **Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
 - **AuthPriv** – SNMP communications use both authentication and encryption.



Show Statistics

Device Management > SNMP > Show Statistics page is used to show counters for SNMP input and output protocol data units.

PARAMETERS

The following counters are displayed:

- ◆ **SNMP packets input** – The total number of messages delivered to the SNMP entity from the transport service.
- ◆ **Bad SNMP version errors** – The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.
- ◆ **Unknown community name** – The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
- ◆ **Illegal operation for community name supplied** – The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
- ◆ **Encoding errors** – The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.

- ◆ **Number of requested variables** – The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
- ◆ **Number of altered variables** – The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
- ◆ **Get-request PDUs** – The total number of SNMP Get-Request PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- ◆ **Get-next PDUs** – The total number of SNMP Get-Next PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- ◆ **Set-request PDUs** – The total number of SNMP Set-Request PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.
- ◆ **SNMP packets output** – The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
- ◆ **Too big errors** – The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is “tooBig.”
- ◆ **No such name errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is “noSuchName.”
- ◆ **Bad values errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is “badValue.”
- ◆ **General errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is “genErr.”
- ◆ **Response PDUs** – The total number of SNMP Get-Response PDUs which have been accepted and processed by, or generated by, the SNMP protocol entity.
- ◆ **Trap PDUs** – The total number of SNMP Trap PDUs which have been accepted and processed by, or generated by, the SNMP protocol entity.

Show Statistics Device Management > SNMP > Show Statistics			
SNMP Statistics			
SNMP packets input	0	SNMP packets output	0
Bad SNMP version errors	0	Too big errors	0
Unknown community name	0	No such name errors	0
Illegal operation for community name supplied	0	Bad values errors	0
Encoding errors	0	General errors	0
Number of requested variables	0	Response PDUs	0
Number of altered variables	0	Trap PDUs	0
Get-request PDUs	0		
Get-next PDUs	0		
Set-request PDUs	0		

[Refresh](#)

RMON

Global Management

Device Management > RMON > Global Management (Alarm) page is used to define specific criteria that will generate response events. Alarms can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over the set interval). Alarms can be set to respond to rising or falling thresholds. (However, note that after an alarm is triggered it will not be triggered again until the statistical value crosses the opposite bounding threshold and then back across the trigger threshold.

COMMAND USAGE

◆ If an alarm is already defined for an index, the entry must be deleted before any changes can be made.

PARAMETERS

These parameters are displayed:

◆ **Index** – Index to this entry. (Range: 1-65535)

◆ **Variable** – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled. Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.

◆ **Interval** – The polling interval. (Range: 1-31622400 seconds)

◆ **Sample Type** – Tests for absolute or relative changes in the specified variable.

■ **Absolute** – The variable is compared directly to the thresholds at the end of the sampling period.

■ **Delta** – The last sample is subtracted from the current value and the difference is then compared to the thresholds.

◆ **Rising Threshold** – If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. (Range: 0-2147483647)

◆ **Rising Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing above the rising threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)

◆ **Falling Threshold** – If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold. (Range: 0-2147483647)

◆ **Falling Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing below the falling threshold. If there is no corresponding entry

in the event control table, then no event will be generated. (Range: 0-65535)

◆ **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

Global Management		Device Management > RMON > Global Management				
<input type="checkbox"/>	37	Valid	1.3.6.1.2.1.16.1.1.1.6.37	30	Delta	0
<input checked="" type="radio"/> Alarm <input type="radio"/> Event						
Index (1-65535)	<input type="text"/>					
Variable	<input type="text"/>					
Interval (1-31622400)	<input type="text"/>					sec
Sample Type	Absolute ▼					
Rising Threshold (0-2147483647)	<input type="text"/>					
Rising Event Index (0-65535)	<input type="text"/>					
Falling Threshold (0-2147483647)	<input type="text"/>					
Falling Event Index (0-65535)	<input type="text"/>					
Owner	<input type="text"/>					
						<input type="button" value="Apply"/> <input type="button" value="Revert"/>

Device Management > RMON > Global Management (Event) page is used to set the action to take when an alarm is triggered. The response can include logging the alarm or sending a message to a trap manager. Alarms and corresponding events provide a way of immediately responding to critical network problems.

COMMAND USAGE

◆ If an alarm is already defined for an index, the entry must be deleted before any changes can be made.

◆ One default event is configured as follows:

event Index = 1

Description: RMON_TRAP_LOG

Event type: log & trap

Event community name is public

Owner is RMON_SNMP

PARAMETERS

These parameters are displayed:

◆ **Index** – Index to this entry. (Range: 1-65535)

◆ **Type** – Specifies the type of event to initiate:

■ **None** – No event is generated.

■ **Log** – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging.

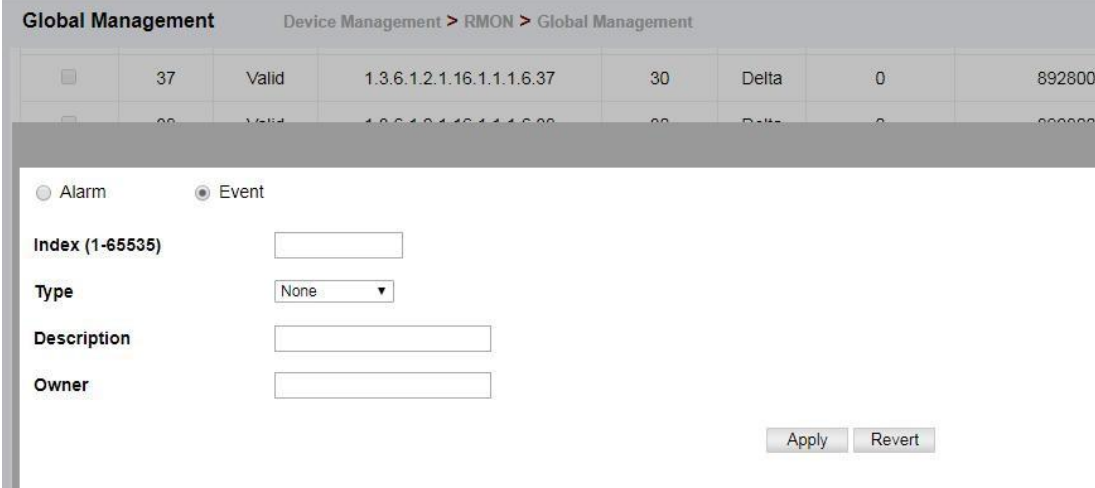
■ **Trap** – Sends a trap message to all configured trap managers.

■ **Log and Trap** – Logs the event and sends a trap message.

◆ **Community** – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts. Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page prior to configuring it here. (Range: 1-127 characters)

◆ **Description** – A comment that describes this event. (Range: 1-127 characters)

◆ **Owner** – Name of the person who created this entry. (Range: 1-127 characters)



Global Management Device Management > RMON > Global Management

<input type="checkbox"/>	37	Valid	1.3.6.1.2.1.16.1.1.1.6.37	30	Delta	0	892800
<input type="checkbox"/>	38	Valid	1.3.6.1.2.1.16.1.1.1.6.38	30	Delta	0	892800

Alarm
 Event

Index (1-65535)

Type

Description

Owner

Interface Management

Device Management > RMON > Interface Management (History) page is used to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A historical record of activity can be used to track down intermittent problems. The record can be used to establish normal baseline activity, which may reveal problems associated with high traffic levels, broadcast storms, or other unusual events. It can also be used to predict network growth and plan for expansion before your network becomes too overloaded.

COMMAND USAGE

◆ Each index number equates to a port on the switch.

◆ If history collection is already enabled on an interface, the entry must be deleted before any changes can be made.

◆ The information collected for each sample includes: input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and network utilization. For a description of the statistics displayed on the Show Details page, refer to "Showing Port or Trunk Statistics".

◆ The switch reserves two index entries for each port. If a default index entry is re-assigned to another port using the Add page, this index will not appear in the Show nor Show Details page for the port to which is normally assigned. For example, if control entry 15 is assigned to port 5, this index entry will be removed from the Show and Show Details page for port 8.

PARAMETERS

These parameters are displayed:

◆ **Port** – The port number on the switch.

◆ **Index** - Index to this entry. (Range: 1-65535)

◆ **Interval** - The polling interval. (Range: 1-3600 seconds; Default: 1800 seconds)

◆ **Buckets** - The number of buckets requested for this entry. (Range: 1-65536; Default: 50)
The number of buckets granted are displayed on the Show page.

◆ **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

Interface Management Device Management > RMON > Interface Management

History Statistics

History Statistics

Port 1

Index (1-65535)

Interval (1-3600) sec

Buckets (1-65535)

Owner

Device Management > RMON > Interface Management (Statistics) page is used to collect statistics on a port, which can subsequently be used to monitor the network for common errors and overall traffic rates.

COMMAND USAGE

◆ If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made.

◆ The information collected for each entry includes: input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, CRC alignment errors, jabbers, fragments, collisions, drop events, and frames of various sizes.

PARAMETERS

These parameters are displayed:

◆ **Port** – The port number on the switch.

◆ **Index** - Index to this entry. (Range: 1-65535)

◆ **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

Interface Management Device Management > RMON > Interface Management

History Statistics

History Statistics

Port 1

Index (1-65535)

Owner

Show Interface Details

Device Management > RMON > Show Interface Details page is used to display interface details of RMON collects.

Show Interface Details Device Management > RMON > Show Interface Details Stacking Unit: 1

History Statistics

Port: 1

RMON History Details Port List Total: 8

History Index	Sample Index	Interval Start	Octets	Packets	Broadcast Packets	Multicast Packets	Undersize Packets	Oversize Packets	Fragments	Jabbers	CRC Align Errors	Collisions	Drop Events	Network Utilization
2	42	00:20:32	0	0	0	0	0	0	0	0	0	0	0	0
2	43	00:21:02	0	0	0	0	0	0	0	0	0	0	0	0
2	44	00:21:32	0	0	0	0	0	0	0	0	0	0	0	0
2	45	00:22:02	0	0	0	0	0	0	0	0	0	0	0	0
2	46	00:22:32	0	0	0	0	0	0	0	0	0	0	0	0
2	47	00:23:02	0	0	0	0	0	0	0	0	0	0	0	0
2	48	00:23:32	0	0	0	0	0	0	0	0	0	0	0	0
2	49	00:24:02	0	0	0	0	0	0	0	0	0	0	0	0

Refresh

Show Interface Details Device Management > RMON > Show Interface Details

History Statistics

Port: 1

RMON Statistics Port Details

Received Octets	0	Collisions	0
Received Packets	0	Drop Events	0
Broadcast Packets	0	Frames of 64 Octets	0
Multicast Packets	0	Frames of 65 to 127 Octets	0
Undersize Packets	0	Frames of 128 to 255 Octets	0
Oversize Packets	0	Frames of 256 to 511 Octets	0
CRC Align Errors	0	Frames of 512 to 1023 Octets	0
Jabbers	0	Frames of 1024 to 1518 Octets	0
Fragments	0		

Refresh

Cluster

Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

Configure Global

The Device Management > Cluster > Configure Global page is used to create a switch cluster.

COMMAND USAGE

First be sure that clustering is enabled on the switch (the default is disabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

PARAMETERS

These parameters are displayed:

- ◆ **Cluster Status** – Enables or disables clustering on the switch. (Default: Disabled)
- ◆ **Commander Status** – Enables or disables the switch as a cluster Commander. (Default: Disabled)
- ◆ **IP Pool** – An “internal” IP address pool that is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.member-ID. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36. Note that you cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled. (Default: 10.254.254.1)
- ◆ **Role** – Indicates the current role of the switch in the cluster; either Commander, Member, or Candidate. (Default: Candidate)
- ◆ **Number of Members** – The current number of Member switches in the cluster.
- ◆ **Number of Candidates** – The current number of Candidate switches discovered in the network that are available to become Members.

Configure Global Device Management > Cluster > Configure Global

Cluster Status	<input checked="" type="checkbox"/> Enabled
Commander Status	<input checked="" type="checkbox"/> Enabled
IP Pool	<input type="text" value="10.254.254.1"/>
Role	Commander
Number of Members	2
Number of Candidates	3

Cluster Member

The Device Management > Cluster > Cluster Member page is used to add Candidate switches to the cluster as Members.

PARAMETERS

These parameters are displayed:

- ◆ **Member ID** – Specify a Member ID number for the selected Candidate switch. (Range: 1-36)
- ◆ **MAC Address** – Select a discovered switch MAC address from the Candidate Table, or enter a specific MAC address of a known switch.

Cluster Member Device Management > Cluster > Cluster Member

Cluster Member List Total: 2

	Member ID	Role	IP Address	MAC Address	Description
<input checked="" type="radio"/>	1	Active Member	10.254.254.2	11-22-33-44-55-33	ES3550MO
<input type="radio"/>	2	Candidate	10.254.254.3	11-22-33-44-55-77	ES3550MO

Member ID (1-36)

MAC Address Candidate 11-22-33-44-55-11 (XX-XX-XX-XX-XX-XX Of XXXXXXXXXXXX)

Cluster Member List Total: 2

	Member ID	Role	IP Address	MAC Address	Description
<input checked="" type="radio"/>	1	Active Member	10.254.254.2	11-22-33-44-55-33	ES3550MO
<input type="radio"/>	2	Candidate	10.254.254.3	11-22-33-44-55-77	ES3550MO

Show Candidate

The Device Management > Cluster > Show Candidate page is used to show Candidate.

Show Candidate Device Management > Cluster > Show Candidate

Cluster Candidate List Total: 4

Role	MAC Address	Description
Candidate	11-22-33-44-55-11	ES3550MO
Active Member	11-22-33-44-55-22	ES3550MO
Candidate	11-22-33-44-55-33	ES3550MO
Candidate	11-22-33-44-55-44	ES3550MO

DNS

DNS service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response. You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

Configure Global

Device Management > DNS > Configure Global page is used to enable domain lookup and set the default domain name.

COMMAND USAGE

◆ To enable DNS service on this switch, enable domain lookup status, and configure one or more name servers .

PARAMETERS

These parameters are displayed:

- ◆ **Domain Lookup** – Enables DNS host name-to-address translation. (Default: Disabled)
- ◆ **Default Domain Name** – Defines the default domain name appended to incomplete host names. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 alphanumeric characters)

Configure Global Device Management > DNS > Configure Global

Domain Lookup Enabled

Default Domain Name

Domain Names

Device Management > DNS > Domain Names page is used to configure a list of name servers to be tried in sequential order.

COMMAND USAGE

- ◆ To enable DNS service on this switch, configure one or more name servers, and enable domain lookup status.
- ◆ When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.
- ◆ If all name servers are deleted, DNS will automatically be disabled. This is done by disabling the domain lookup status.

PARAMETERS

These parameters are displayed:

Name Server IP Address – Specifies the IPv4 or IPv6 address of a domain name server to use for name-to-address resolution. Up to six IP addresses can be added to the name server list.

Domain Names Device Management > DNS > Domain Names

Domain Name List Total: 0

Domain Name
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>

Domain Name

Name Servers

Device Management > DNS > Name Servers is used page to configure a list of name servers to be tried in sequential order.

COMMAND USAGE

- ◆ To enable DNS service on this switch, configure one or more name servers, and enable domain lookup status.
- ◆ When more than one name server is specified, the servers are queried in the specified

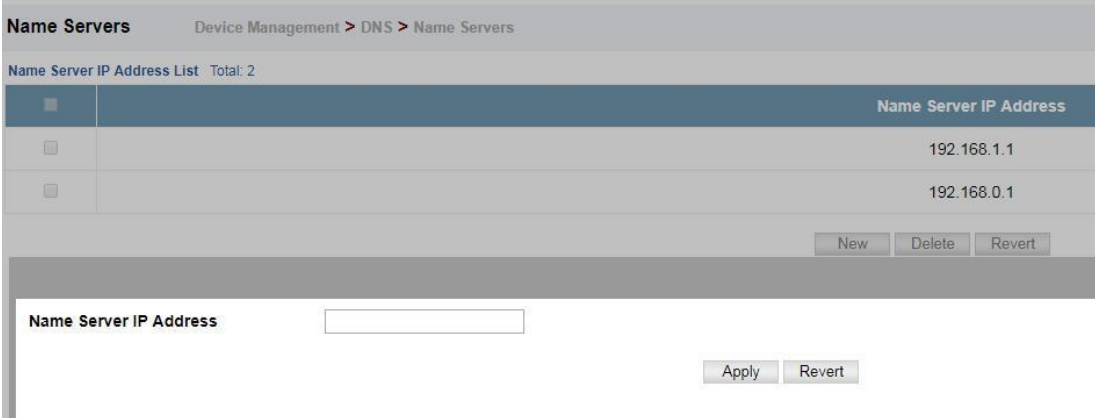
sequence until a response is received, or the end of the list is reached with no response.

◆ If all name servers are deleted, DNS will automatically be disabled. This is done by disabling the domain lookup status.

PARAMETERS

These parameters are displayed:

Name Server IP Address – Specifies the IPv4 or IPv6 address of a domain name server to use for name-to-address resolution. Up to six IP addresses can be added to the name server list.



The screenshot shows the 'Name Servers' configuration page. At the top, the breadcrumb is 'Device Management > DNS > Name Servers'. Below the title, it says 'Name Server IP Address List Total: 2'. There is a table with two columns: a checkbox column and a 'Name Server IP Address' column. The table contains two entries: 192.168.1.1 and 192.168.0.1. Below the table are buttons for 'New', 'Delete', and 'Revert'. At the bottom, there is a 'Name Server IP Address' label followed by an input field and 'Apply' and 'Revert' buttons.

Static Host

Device Management > DNS > Static Host page is used to manually configure static entries in the DNS table that are used to map domain names to IP addresses.

COMMAND USAGE

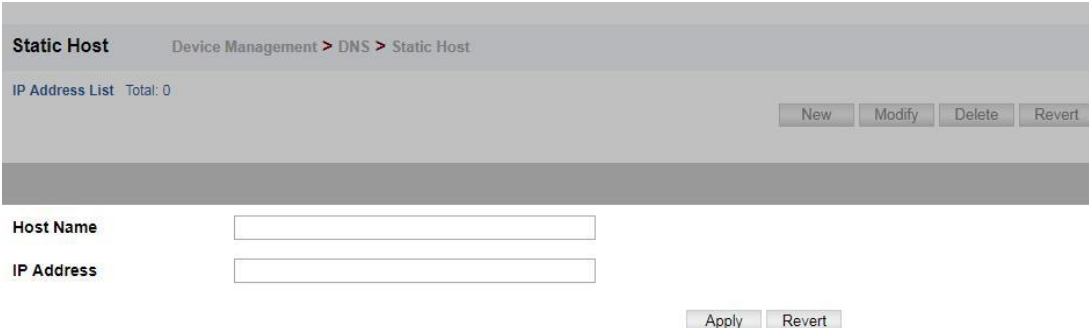
◆ Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.

PARAMETERS

These parameters are displayed:

◆ **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-127 characters)

◆ **IP Address** – Internet address(es) associated with a host name.



The screenshot shows the 'Static Host' configuration page. At the top, the breadcrumb is 'Device Management > DNS > Static Host'. Below the title, it says 'IP Address List Total: 0'. There are buttons for 'New', 'Modify', 'Delete', and 'Revert'. Below this, there are two input fields: 'Host Name' and 'IP Address'. At the bottom, there are 'Apply' and 'Revert' buttons.

Cache

Device Management > DNS > Cache page is used to display entries in the DNS cache that have been learned via the designated name servers.

COMMAND USAGE

◆ Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

PARAMETERS

These parameters are displayed:

- ◆ **No.** – The entry number for each resource record.
- ◆ **Flag** – The flag is always “4” indicating a cache entry and therefore unreliable.
- ◆ **Type** – This field includes CNAME which specifies the host address for the owner, and ALIAS which specifies an alias.
- ◆ **IP** – The IP address associated with this record.
- ◆ **TTL** – The time to live reported by the name server.
- ◆ **Host** – The host name associated with this record.

Cache Device Management > DNS > Cache

Cache Information Total: 3

No.	Flag	Type	IP	TTL	Host
0	4	Host	59.175.132.126	105	spool.grid.sinaedge.com
1	4	CNAME	POINTER TO 0	105	www.sina.com.cn
2	4	Host	59.175.132.126	105	www.sina.com.cn

DHCP

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients when they boot up. If a subnet does not already include a BOOTP or DHCP server, you can relay DHCP client requests to a DHCP server on another subnet, or configure the DHCP server on this switch to support that subnet. When configuring the DHCP server on this switch, you can configure an address pool for each unique IP interface, or manually assign a static IP address to clients based on their hardware address or client identifier. The DHCP server can provide the host's IP address, domain name, gateway router and DNS server, information about the host's boot image including the TFTP server to access for download and the name of the boot file, or boot information for NetBIOS Windows Internet Naming Service (WINS).

Client

Device Management > DHCP > Client page is used to specify the DHCP client identifier for a VLAN interface.

COMMAND USAGE

◆ The class identifier is used identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.

◆ The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator.

PARAMETERS

These parameters are displayed in the web interface:

◆ **VLAN** – ID of configured VLAN.

◆ **Vendor Class ID** – The following options are supported when the check box is marked to enable this feature:

■ **Default** – The default string is ECS4510-28T.

■ **Text** – A text string. (Range: 1-32 characters)

■ **Hex** – A hexadecimal value. (Range: 1-64 characters)

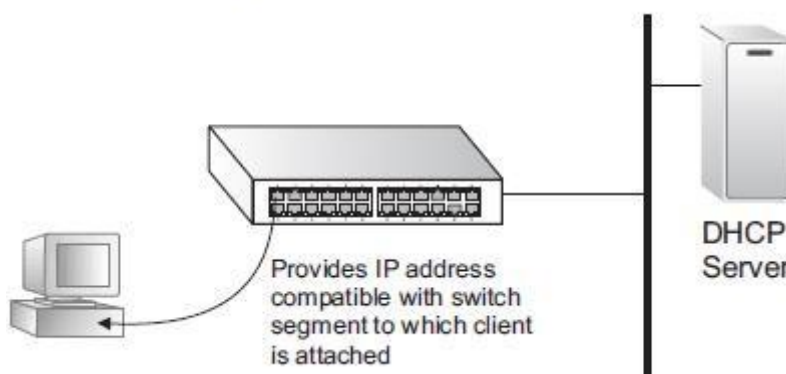
Client Device Management > DHCP > Client

VLAN

Vendor Class ID Default

Relay

Device Management > DHCP > Relay page is used to configure DHCP relay service for attached host devices. If DHCP relay is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then passes the DHCP response received from the server to the client.



COMMAND USAGE

◆ You must specify the IP address for at least one active DHCP server. Otherwise, the switch's DHCP relay agent will not be able to forward client requests to a DHCP server. Up to five DHCP servers can be specified in order of preference. If any of the specified DHCP server addresses are not located in the same network segment with this switch, specify the default router through which this switch can reach other IP subnetworks(see "Configuring Static Routes").

◆ DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

PARAMETERS

These parameters are displayed:

◆ **VLAN ID** – ID of configured VLAN.

◆ **Server IP Address** – Addresses of DHCP servers or relay servers to be used by the switch's DHCP relay agent in order of preference.

◆ **Restart DHCP Relay** – Use this button to re-initialize DHCP relay service.

Note: DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

DHCP Server by VLAN List Total: 1

VLAN	Server IP Address				
1	192.168.2.33	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Click the button to restart DHCP Relay service.

Relay Option82

Device Management > DHCP > Relay Option82 page is used to configure DHCP relay service for attached host devices, including DHCP option 82 information. DHCP provides an option for sending information about its DHCP clients to the DHCP server(specifically, the interface on the relay server through which the DHCP client request was received). Also known as DHCP Relay Option 82, it allows compatible DHCP servers to use this information when assigning IP addresses, or to set other services or policies for clients. Option 82 information contains information which can identify both the relay agent and the interface through which the DHCP request was received:

◆ The DHCP Relay Information Option Remote ID (RID) is the access node identifier – a string used to identify the switch to the DHCP server.

◆ The DHCP Relay Information Option Fields are the Option 82 circuit identification fields (CID – including VLAN ID, stack unit, and port). These fields identify the requesting device by indicating the interface through which the relay agent received the request. If DHCP relay is enabled, and this switch sees a DHCP client request, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Depending on the selected frame format set for the remote-id, this information may specify the MAC address, IP address, or an arbitrary string for the requesting device (that is, the relay agent in this context). By default, the relay agent also fills in the Option 82 circuit-id field with information indicating the local interface over which the switch received the DHCP client request, including the VLAN ID, stack unit, and port. This allows DHCP client-server exchange

messages to be forwarded between the server and client without having to flood them onto the entire VLAN. The switch 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 DHCP relay agent (i.e., this switch). This switch then passes the DHCP response received from the server to the client.

COMMAND USAGE

◆ You must specify the IP address for at least one active DHCP server. Otherwise, the switch's DHCP relay agent will not be able to forward client requests to a DHCP server. Up to five DHCP servers can be specified in order of preference. If any of the specified DHCP server addresses are not located in the same network segment with this switch, specify the default router through which this switch can reach other IP subnetworks.

◆ DHCP Snooping Information Option 82 and DHCP Relay Information Option 82 cannot both be enabled at the same time.

◆ DHCP request packets received by the switch are handled as follows:

■ If a DHCP relay server has been set on the switch, when the switch receives a DHCP request packet without option 82 information from the management VLAN or a non-management VLAN, it will add option 82 relay information and the relay agent's address to the DHCP request packet, and then unicast it to the DHCP server.

■ If a DHCP relay server has been set on the switch, when the switch receives a DHCP request packet with option 82 information from the management VLAN or a non-management VLAN, it will process it according to the configured relay information option policy:

■ If the policy is "replace," the DHCP request packet's option 82 content (the RID and CID sub-option) is replaced with information provided by the switch. The relay agent address is inserted into the DHCP request packet, and the switch then unicasts this packet to the DHCP server.

■ If the policy is "keep," the DHCP request packet's option 82 content will be retained. The relay agent address is inserted into the DHCP request packet, and the switch then unicasts this packet to the DHCP server.

■ If the policy is "drop," the original DHCP request packet is flooded onto the VLAN which received the packet but is not relayed.

◆ DHCP reply packets received by the relay agent are handled as follows: When the relay agent receives a DHCP reply packet with Option 82 information over the management VLAN, it first ensures that the packet is destined for it.

■ If the RID in the DHCP reply packet is not identical with that configured on the switch, the option 82 information is retained, and the packet is flooded onto the VLAN through which it was received.

■ If the RID in the DHCP reply packet matches that configured on the switch, it then removes the Option 82 information from the packet, and sends it on as follows:

■ If the DHCP packet's broadcast flag is on, the switch uses the circuit-id information contained in the option 82 information fields to identify the VLAN connected to the requesting client and then broadcasts the DHCP reply packet to this VLAN.

■ If the DHCP packet's broadcast flag is off, the switch uses the circuit-id information in

option 82 fields to identify the interface connected to the requesting client and unicasts the reply packet to the client.

◆ DHCP packets are flooded onto the VLAN which received them if DHCP relay service is enabled on the switch and any of the following situations apply:

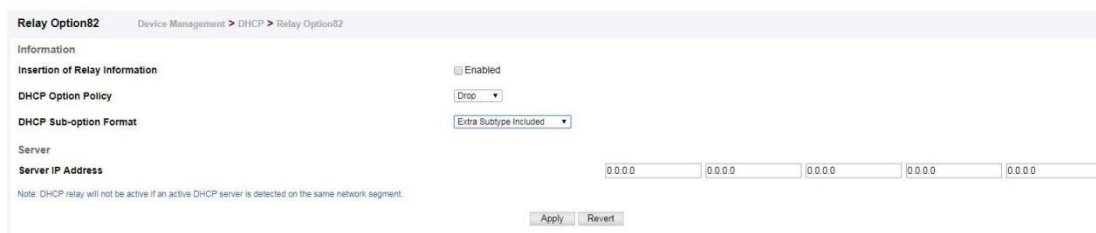
- There is no DHCP relay server set on the switch, when the switch receives a DHCP packet.
- A DHCP relay server has been set on the switch, when the switch receives a DHCP request packet with a non-zero relay agent address field (that is not the address of this switch).
- A DHCP relay server has been set on the switch, when the switch receives DHCP reply packet without option 82 information from the management VLAN.
- The reply packet contains a valid relay agent address field (that is not the address of this switch), or receives a reply packet with a zero relay agent address through the management VLAN.
- A DHCP relay server has been set on the switch, and the switch receives a reply packet on a non-management VLAN.

◆ DHCP relay configuration will not be active if an active DHCP server is detected on the same network segment.

PARAMETERS

These parameters are displayed:

- ◆ **Insertion of Relay Information** – Enable DHCP Option 82 information relay. (Default: Disabled)
- ◆ **DHCP Option Policy** – Specifies how to handle client requests which already contain DHCP Option 82 information:
 - **Drop** - Floods the original request packet onto the VLAN that received it instead of relaying it. (This is the default.)
 - **Keep** - Retains the Option 82 information in the client request, inserts the relay agent's address, and unicasts the packet to the DHCP server.
 - **Replace** - Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information provided by the relay agent itself, inserts the relay agent's address, and unicasts the packet to the DHCP server.
- ◆ **DHCP Sub-option Format** – Specifies whether or not to use the sub-type and sub-length fields in the circuit-ID (CID) and remote-ID (RID) in Option 82 information. (Default: Included)
- ◆ **Server IP Address** – Addresses of DHCP servers or relay servers to be used by the switch's DHCP relay agent in order of preference.



The screenshot shows the configuration page for Relay Option82. The breadcrumb navigation is "Device Management > DHCP > Relay Option82". The page is titled "Relay Option82". Under the "Information" section, there are three settings: "Insertion of Relay Information" is set to "Enabled" (checkbox checked), "DHCP Option Policy" is set to "Drop" (dropdown menu), and "DHCP Sub-option Format" is set to "Extra Subtype Included" (dropdown menu). Under the "Server" section, there is a "Server IP Address" field with five input boxes, each containing "0.0.0.0". A note at the bottom states: "Note: DHCP relay will not be active if an active DHCP server is detected on the same network segment." At the bottom right, there are "Apply" and "Revert" buttons.

Dynamic Provision

Device Management > DHCP > Dynamic Provision is used to enable dynamic provisioning via DHCP.

COMMAND USAGE

DHCPD is the daemon used by Linux to dynamically configure TCP/IP information for client systems. To support DHCP option 66/67, you have to add corresponding statements to the configuration file of DHCPD. Some alternative commands which can be added to the DHCPD to complete the dynamic provisioning process are also described under the ip dhcp dynamic provision command in the CLI Reference Guide. By default, the parameters for DHCP option 66/67 are not carried by the reply sent from the DHCP server. To ask for a DHCP reply with option 66/67, the client can inform the server that it is interested in option 66/67 by sending a DHCP request that includes a 'parameter request list' option. Besides this, the client can also send a DHCP request that includes a 'vendor class identifier' option to the server so that the DHCP server can identify the device, and determine what information should be given to requesting device.

PARAMETERS

These parameters are displayed:

◆ **Dynamic Provision via DHCP Status** – Enables dynamic provisioning via DHCP. (Default: Disabled)



The screenshot shows a breadcrumb trail: **Dynamic Provision** > Device Management > DHCP > Dynamic Provision. Below this, the parameter 'Dynamic Provision via DHCP Status' is shown with a checkbox that is checked, indicating it is 'Enabled'. At the bottom right of the interface, there are two buttons: 'Apply' and 'Revert'.

OAM

The switch provides OAM (Operation, Administration, and Maintenance) remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment). This section describes functions including enabling OAM for selected ports, loopback testing, and displaying remote device information.

Interface

The Device Management > OAM > Interface page is used to enable OAM functionality on the selected port. Not all CPEs support operation and maintenance functions, so OAM is therefore disabled by default. If a CPE supports OAM, this functionality must first be enabled on the connected port to gain access to the configuration functions provided under the OAM menu.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Admin Status** – Enables or disables OAM functions. (Default: Disabled)
- ◆ **Operation State** – Shows the operational state between the local and remote OAM devices. This value is always “disabled” if OAM is disabled on the local interface.

OAM Operation State

State	Description
Disabled	OAM is disabled on this interface via the OAM Admin Status.
Link Fault	The link has detected a fault or the interface is not operational.
Passive Wait	This value is returned only by OAM entities in passive mode and indicates the OAM entity is waiting to see if the peer device is OAM capable.
Active Send Local	This value is used by active mode devices and indicates the OAM entity is actively trying to discover whether the peer has OAM capability but has not yet made that determination.
Send Local And Remote	The local OAM entity has discovered the peer but has not yet accepted or rejected the configuration of the peer.
Send Local And Remote OK	OAM peering is allowed by the local device.
OAM Peering Locally Rejected	The local OAM entity rejects the peering.
OAM Peering Remotely Rejected	The remote OAM entity rejects the peering.
Operational	When the local OAM entity learns that both it and the remote OAM entity have accepted the peering, the state moves to this state.
Non Oper Half Duplex	This state is returned whenever Ethernet OAM is enabled but the interface is in half-duplex operation.

- ◆ **Mode** – Sets the OAM operation mode. (Default: Active)
- **Active** – All OAM functions are enabled.
- **Passive** – All OAM functions are enabled, except for OAM discovery, sending variable request OAMPDUs, and sending loopback control OAMPDUs.
- ◆ **Critical Link Event** – Controls reporting of critical link events to its OAM peer.
- **Dying Gasp** – If an unrecoverable condition occurs, the local OAM entity (i.e., this switch) indicates this by immediately sending a trap message. (Default: Enabled) Dying gasp events are caused by an unrecoverable failure, such as a power failure or device reset.
- **Critical Event** – If a critical event occurs, the local OAM entity indicates this to its peer by setting the appropriate flag in the next OAMPDU to be sent and stores this information in its OAM event log. (Default: Enabled) Critical events include various failures, such as abnormal voltage fluctuations, out-of-range temperature detected, fan failure, CRC error in flash memory, insufficient memory, or other hardware faults.
- ◆ **Errored Frame** – Controls reporting of errored frame link events. An errored frame is a frame in which one or more bits are errored. An errored frame link event occurs if the threshold is reached or exceeded within the specified period. If reporting is enabled and an errored frame link event occurs, the local OAM entity (this switch) sends an Event Notification OAMPDU to the remote OAM entity. The Errored Frame Event TLV includes the

number of errored frames detected during the specified period.

■ **Status** – Enables reporting of errored frame link events. (Default: Enabled)

■ **Window Size** – The period of time in which to check the reporting threshold for errored frame link events. (Range: 10-65535 in units of 10 milliseconds; Default: 10 units of 10 milliseconds, or the equivalent of 1 second)

■ **Threshold Count** – The threshold for errored frame link events. (Range: 1-65535; Default: 1)

Interface Stacking Unit: 1

OAM Port List Total: 4

Port	Admin Status	Operation State	Mode	Critical Link Event		Errored Frame		
				Dying Gasp	Critical Event	Status	Window Size (10-65535 1/10 sec)	Threshold Count (1-65535)
1	<input checked="" type="checkbox"/> Enabled	Link Fault	Active	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	10	65535
2	<input checked="" type="checkbox"/> Enabled	Active Send Local	Active	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	10	1
27	<input type="checkbox"/> Enabled	Operational	Passive	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	10	65535
28	<input type="checkbox"/> Enabled	Non Operation Half Duplex	Passive	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	65535	1

Counters

The Device Management > OAM > Counters page is used to display statistics for the various types of OAM messages passed across each port.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Clear** – Clears statistical counters for the selected ports.
- ◆ **OAMPDU** – Message types transmitted and received by the OAM protocol, including Information OAMPDUs, unique Event OAMPDUs, Loopback Control OAMPDUs, and Organization Specific OAMPDUs.

Counters Stacking Unit: 1

OAM Port Counters Total: 4

	Port	OAMPDU							
		Information		Event Notification		Loopback Control		Organization Specific	
		Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
<input type="checkbox"/>	1	0	0	0	0	0	0	0	0
<input type="checkbox"/>	2	0	0	0	0	0	0	0	0
<input type="checkbox"/>	23	0	0	0	0	0	0	0	0
<input type="checkbox"/>	24	0	0	0	0	0	0	0	0

Event Log

The Device Management > OAM > Event Log page is used to display link events for the selected port.

COMMAND USAGE

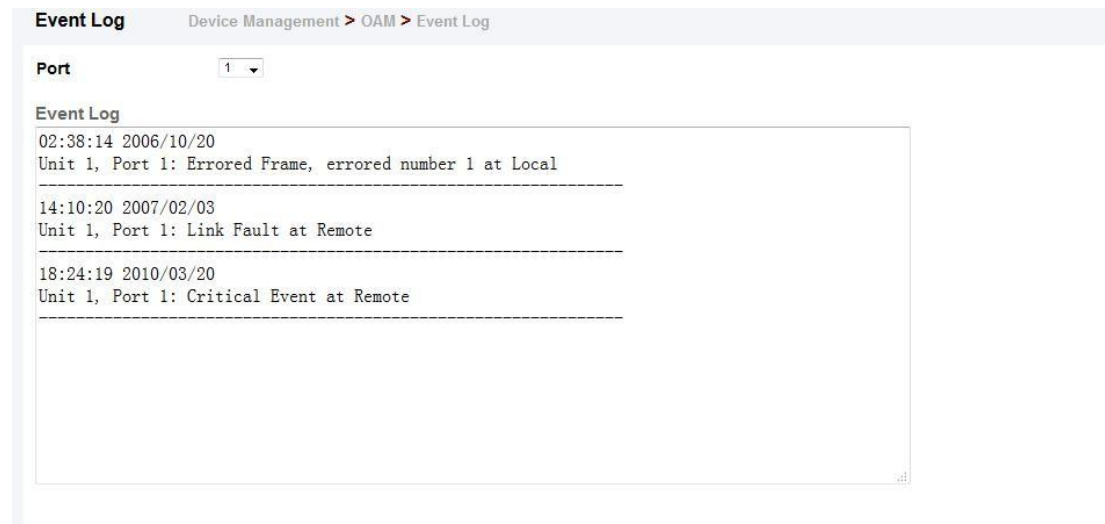
- ◆ When a link event occurs, no matter whether the location is local or remote, this information is entered in OAM event log.
- ◆ When the log system becomes full, older events are automatically deleted to make room for new entries.

◆ The time of locally generated events can be accurately retrieved from the sysUpTime variable. For remotely generated events, the time of an event is indicated by the reception of an Event Notification OAMPDU from the peer.

WEB INTERFACE

To display link events for the selected port:

1. Click Device Management, OAM, Event Log.
2. Select a port from the drop-down list.



Remote Interface

The Device Management > OAM > Remote Interface page is used to display information about attached OAM-enabled devices.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **MAC Address** – MAC address of the OAM peer.
- ◆ **OUI** – Organizational Unit Identifier of the OAM peer.
- ◆ **Remote Loopback** – Shows if remote loopback is supported by the OAM peer.
- ◆ **Unidirectional Function** – Shows if this function is supported by the OAM peer.

If supported, this indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (where traffic flows in one direction only). Some newer physical layer devices support the optional ability to encode and transmit data while one direction of the link is non-operational. This function allows OAM remote fault indication during fault conditions. This switch does not support the unidirectional function, but can parse error messages sent from a peer with unidirectional capability.

- ◆ **Link Monitor** – Shows if the OAM entity can send and receive Event Notification OAMPDUs.
- ◆ **MIB Variable Retrieval** – Shows if the OAM entity can send and receive Variable Request and Response OAMPDUs.

Remote Interface Device Management > OAM > Remote Interface Stacking Unit: 1

OAM Remote Port List Total: 4

Port	MAC Address	OUI	Remote Loopback	Unidirectional Function	Link Monitor	MIB Variable Retrieval
1	0A-02-60-96-90-E0	0A-02-60	Enabled	Enabled	Disabled	Disabled
2	70-E0-06-0F-08-50	70-E0-06	Enabled	Disabled	Disabled	Enabled
23	40-B0-0A-70-10-90	40-B0-0A	Disabled	Enabled	Disabled	Disabled
24	50-20-9C-50-0E-80	50-20-9C	Disabled	Disabled	Disabled	Disabled

Show Loopback Result

Use the Device Management > OAM > Show Loopback Result page is used to display the results of remote loop back testing for each port for which this information is available.

PARAMETERS

These parameters are displayed:

- ◆ **Port** – Port identifier. (Range: 1-12/26)
- ◆ **Packets Transmitted** – The number of loop back frames transmitted during the last loop back test on this interface.
- ◆ **Packets Received** – The number of loop back frames received during the last loop back test on this interface.
- ◆ **Loss Rate** – The percentage of packets transmitted for which there was no response.

Show Loopback Result Device Management > OAM > Show Loopback Result Stacking Unit: 1

Port Remote Test Result List Total: 4

Port	Packets Transmitted	Packets Received	Loss Rate
1	0	0	0.00 %
2	0	0	0.00 %
23	0	0	0.00 %
24	0	0	0.00 %

Loopback Test

The Device Management > OAM > Loopback Test page is used to initiate a loop back test to the peer device attached to the selected port.

COMMAND USAGE

- You can use this command to perform an OAM remote loop back test on the specified port. The port that you specify to run this test must be connected to a peer OAM device capable of entering into OAM remote loop back mode.

- ◆ During a remote loop back test, the remote OAM entity loops back every frame except for OAMPDUs and pause frames.

- ◆ OAM remote loopback can be used for fault localization and link performance testing. Statistics from both the local and remote DTE can be queried and compared at any time during loop back testing.

- ◆ To perform a loopback test, first enable Remote Loop Back Mode, click Test, and then click End. The number of packets transmitted and received will be displayed.

PARAMETERS

These parameters are displayed:

Loopback Mode of Remote Device

- ◆ **Port** – Port identifier. (Range: 1-28)
- ◆ **Loopback Mode** – Shows if loop back mode is enabled on the peer. This attribute must be enabled before starting the loopback test.
- ◆ **Loopback Status** – Shows if loopback testing is currently running.

Loopback Test Parameters

- ◆ **Packets Number** – Number of packets to send. (Range: 1-99999999; Default: 10000)
- ◆ **Packet Size** – Size of packets to send. (Range: 64-1518 bytes; Default: 64 bytes)
- ◆ **Test** – Starts the loop back test.
- ◆ **End** – Stops the loop back test.

Loop Back Status of Remote Device

- ◆ **Result** – Shows the loop back status on the peer. The loop back states shown in this field are described below.

OAM Operation State

State	Description
No Loopback	Operating in normal mode with no loopback in progress.
Initiating Loopback	The local OAM entity is starting the loopback process with its peer. It has yet to receive any acknowledgement that the remote OAM entity has received its loopback command request.
Remote Loopback	The local OAM client knows that the remote OAM entity is in loopback mode.
Terminating Loopback	The local OAM client is in the process of terminating the remote loopback.
Local Loopback	The remote OAM client has put the local OAM entity in loopback mode.
Unknown	This status may be returned if the OAM loopback is in a transition state but should not persist.

■ **Packets Transmitted** – The number of loop back frames transmitted during the last loopback test on this interface.

■ **Packets Received** – The number of loop back frames received during the last loopback test on this interface.

■ **Loss Rate** – The percentage of packets for which there was no response.

Loopback Test Device Management > OAM > Loopback Test

Port 1
Loopback Mode Enabled
Loopback Status Remote Loopback

Packet Number (1-65535)
Packet Size (1-65535) bytes

Result

1000 packets transmitted. 400 packets received. Loss rate is 6.0 %

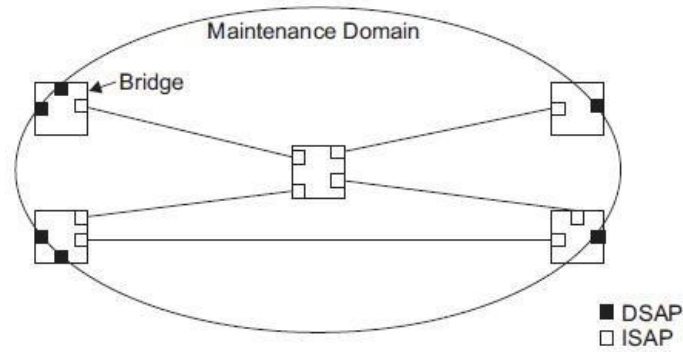
CFM

Connectivity Fault Management (CFM) is an OAM protocol that includes proactive connectivity monitoring using continuity check messages, fault verification through loop back messages, and fault isolation by examining end-to-end connections between provider edge devices or between customer edge devices. CFM is implemented as a service level protocol based on service instances which encompass only that portion of the metropolitan area network supporting a specific customer. CFM can also provide controlled management access to a hierarchy of maintenance domains (such as the customer, service provider, and equipment operator). This switch supports functions for defining the CFM structure, including domains, maintenance associations, and maintenance access points. It also supports fault detection through continuity check messages for all known maintenance points, and cross-check messages which are used to verify a static list of remote maintenance points located on other devices (in the same maintenance association) against those found through continuity check messages. Fault verification is supported using loop back messages, and fault isolation with link trace messages. Fault notification is also provided by SNMP alarms which are automatically generated by maintenance points when connectivity faults or configuration errors are detected in the local maintenance domain.

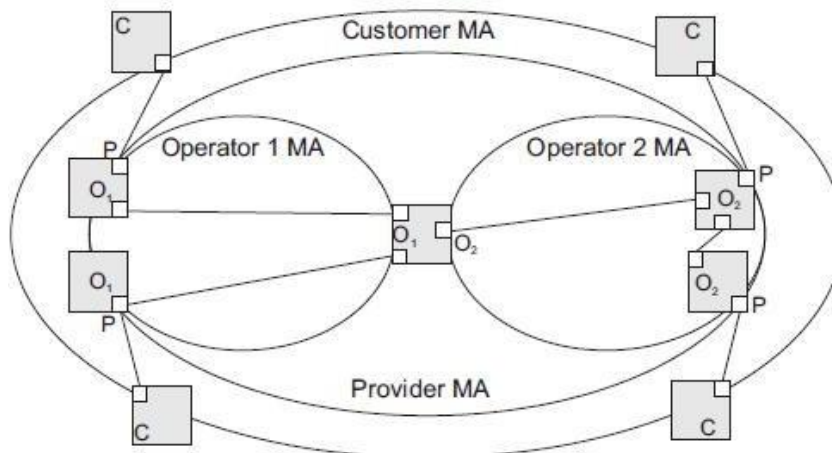
Key Components of CFM

CFM provides restricted management access to each Service Instance using a structured conceptual network based on these components:

- ◆ A Maintenance Domain defines a part of the network controlled by a single operator, and supports management access to the domain through Domain Service Access Points (DSAPs) configured on the domain boundary, as well as connectivity testing between these DSAPs.
- ◆ A Maintenance Association (MA) contains the DSAPs for an individual Service Instance. DSAPs are the primary maintenance points used to monitor connectivity across a maintenance domain, and are the entry points to the paths which interconnect the access points allocated to a service instance.
- ◆ A Maintenance Level allows maintenance domains to be nested in a hierarchical fashion, providing access to the specific network portions required by each operator. Domains at lower levels may be either hidden or exposed to operators managing domains at a higher level, allowing either course or fine fault resolution.
- ◆ Maintenance End Points (MEPs) which provide full CFM access to a Service Instance (i.e., a specific MA), and Maintenance Intermediate Points (MIPs) which are passive entities that merely validate received CFM messages, or respond to link trace and loop back requests. MIPs are the interconnection points that make up all possible paths between the DSAPs within an MA, and may also include interconnection points in lower-level domains if exposed by CFM settings. The following figure shows a single Maintenance Domain, with DSAPs located on the domain boundary, and Internal Service Access Points (ISAPs) inside the domain through which frames may pass between the DSAPs.



The figure below shows four maintenance associations contained within a hierarchical structure of maintenance domains. At the innermost level, there are two operator domains which include access points marked “O1” and “O2” respectively. The users of these domains can see their respective MEPs as well as all the MIPs within their domains. There is a service provider domain at the second level in the hierarchy. From the service provider’s view, the access points marked “P” are visible, and all access points within the operator domains have also been made visible as MIPs according to common practice. And finally, there is a customer domain at the top of the hierarchy. Users at this level can only see the access points marked “C” on the outer domain boundary. Again, normal practice is to hide the internal structure of the network from outsiders to reduce security risks.



Note that the Service Instances within each domain shown above are based on a unique maintenance association for the specific users, distinguished by the domain name, maintenance level, maintenance association’s name, and assigned VLAN.

Basic CFM Operations

CFM uses standard Ethernet frames for sending protocol messages. Both the source and destination address for these messages are based on unicast or multicast MAC addresses, and therefore confined to a single Layer 2 CFM service VLAN. For this reason, the transmission, forwarding, and processing of CFM frames is performed by bridges, not routers. Bridges that do not recognize CFM messages forward them as normal data. There are three basic types of CFM messages, including continuity check, link trace, and loop back. Continuity check messages (CCMs) are multicast within a single Service Instance (i.e., a specific MA), allowing MEPs to discover other MEPs within the same MA, and MIPs to

discover MEPs. Connectivity faults are indicated when a known MEP stops sending CCMs, or a remote MEP configured in a static list does not come up. Configuration errors, such as a cross-connect between different MAs, are indicated when a CCM is received with an incorrect MA identifier or maintenance level. Loop back messages are used for fault verification. These messages can be sent using the MAC address of any destination MEP within the same MA. If the target MEP's identifier has been discovered through CCM messages, then a loop back message can also be sent using the MEPs identifier. A reply indicates that the destination is reachable. Link trace messages are used for fault verification. These messages are multicast frames sent out to track the hop-by-hop path to a target MEP within the same MA. Responses provide information on the ingress, egress, and relay action taken at each hop along the path, providing vital information about connectivity problems. Responses allow the sender to discover all of the maintenance points that would be traversed by a data frame sent to the target MAC address. SNMP traps can also be configured to provide an automated method of fault notification. If the fault notification generator detects one or more defects within the configured time period, and fault alarms are enabled, a corresponding trap will be sent. No further fault alarms are sent until the fault notification generator has been reset by the passage of a configured time period without detecting any further faults. Upon receiving a fault alarm, you should inspect the related SNMP objects for the reporting MEP, diagnose the fault, correct it, and re-examine the MEP's SNMP objects to see whether the fault notification generator has been reset.

Configure Global

Device Management > CFM > Configure Global page is used to configure global settings for CFM, such as enabling the CFM process on the switch, setting the start-up delay for cross-check operations, configuring parameters for the link trace cache, and enabling traps for events discovered by continuity check messages or cross-check messages.

PARAMETERS

These parameters are displayed:

Global Configuration

◆ **CFM Status** – Enables CFM processing globally on the switch.

(Default: Enabled)

To avoid generating an excessive number of traps, the complete CFM maintenance structure and process parameters should be configured prior to enabling CFM processing globally on the switch. Specifically, the maintenance domains, maintenance associations, and maintenance end-points (MEPs) should be configured on each participating bridge using the Configure MD page, Configure MA page, and the Configure MEP page.

When CFM is enabled, hardware resources are allocated for CFM processing.

◆ **MEP Cross Check Start Delay** – Sets the maximum delay that a device waits for remote MEPs to come up before starting the crosscheck operation. (Range: 1-65535 seconds; Default: 10 seconds)

This parameter sets the time to wait for a remote MEP to come up, and the switch starts cross-checking the list of statically configured remote MEPs in the local maintenance domain against the MEPs learned through continuity check messages (CCMs). The cross-check start

delay should be configured to a value greater than or equal to the continuity check message interval to avoid generating unnecessary traps.

Link Trace Cache Settings

◆ **Link Trace Cache** – Enables caching of CFM data learned through link trace messages. (Default: Enabled) A linktrace message is a multicast CFM frame initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating a linktrace reply, up to the point at which the linktrace message reaches its destination or can no longer be forwarded. Use this command attribute to enable the link trace cache to store the results of link trace operations initiated on this device. Use the CFM Transmit Link Trace page to transmit a linktrace message. Linktrace responses are returned from each MIP along the path and from the target MEP. Information stored in the cache includes the maintenance domain name, MA name, MEPID, sequence number, and TTL value.

◆ **Link Trace Cache Hold Time** – The hold time for CFM link trace cache entries. (Range: 1-65535 minutes; Default: 100 minutes) Before setting the aging time for cache entries, the cache must first be enabled in the Linktrace Cache attribute field.

◆ **Link Trace Cache Size** – The maximum size for the link trace cache. (Range: 1-4095 entries; Default: 100 entries) If the cache reaches the maximum number of specified entries, or the size is set to a value less than the current number of stored entries, no new entries are added. To add additional entries, the cache size must first be increased, or purged.

Continuity Check Errors

◆ **Connectivity Check Config** – Sends a trap if this device receives a continuity check message (CCM) with the same maintenance end point identifier (MPID) as its own but with a different source MAC address, indicating that a CFM configuration error exists.

◆ **Connectivity Check Loop** – Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.

◆ **Connectivity Check MEP Down** – Sends a trap if this device loses connectivity with a remote maintenance end point (MEP), or connectivity has been restored to a remote MEP which has recovered from an error condition.

◆ **Connectivity Check MEP Up** – Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which as an expired entry in the archived database. MEP Up traps are suppressed when cross-checking of MEPs is enabled¹¹ because cross-check traps include more detailed status information.

Cross-check Errors

◆ **Cross Check MA Up** – Sends a trap when all remote MEPs in an MA come up. An MA Up trap is sent if cross-checking is enabled, and a CCM is received from all remote MEPs configured in the static list for this maintenance association

◆ **Cross Check MEP Missing** – Sends a trap if the cross-check timer expires and no CCMs have been received from a remote MEP configured in the static list. A MEP Missing trap is sent if cross-checking is enabled¹¹, and no CCM is received for a remote MEP configured in the static list¹².

◆ **Cross Check MEP Unknown** – Sends a trap if an unconfigured MEP comes up. A MEP Unknown trap is sent if cross-checking is enabled¹¹, and a CCM is received from a remote MEP that is not configured in the static list¹².

Configure Global Device Management > CFM > Configure Global

Global Configuration

CFM Status Enabled

MEP Cross Check Start Delay (1-65535) sec

Link Trace Cache Enabled

Link Trace Cache Hold Time (1-65535) min

Link Trace Cache Size (1-4095) entries

SNMP Trap Configuration

Connectivity Check Config Enabled

Connectivity Check Loop Enabled

Connectivity Check MEP Down Enabled

Connectivity Check MEP Up Enabled

Cross Check MA Up Enabled

Cross Check MEP Missing Enabled

Cross Check MEP Unknown Enabled

Configure Interface

CFM processes are enabled by default for all physical interfaces, both ports and trunks. You can use the Device Management > CFM > Configure Interface page to change these settings.

COMMAND USAGE

- ◆ An interface must be enabled before a MEP can be created.
- ◆ If a MEP has been configured on an interface, it must first be deleted before CFM can be disabled on that interface.
- ◆ When CFM is disabled, hardware resources previously used for CFM processing on that interface are released, and all CFM frames entering that interface are forwarded as normal data traffic.

Configure Interface Device Management > CFM > Configure Interface

Interface Port Trunk

Port List Total: 50

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

MD Management

Device Management > CFM > MD Management pages is used to create and configure a Maintenance Domain (MD) which defines a portion of the network for which connectivity faults can be managed. Domain access points are set up on the boundary of a domain to provide end-to-end connectivity fault detection, analysis, and recovery. Domains can be configured in a hierarchy to provide management access to the same basic network resources for different user levels.

COMMAND USAGE

Configuring General Settings

- ◆ Where domains are nested, an upper-level hierarchical domain must have a higher maintenance level than the ones it encompasses. The higher to lower level domain types commonly include entities such as customer, service provider, and operator.
- ◆ More than one domain can be configured at the same maintenance level, but a single domain can only be configured with one maintenance level.
- ◆ If MEPs or Mas are configured for a domain, they must first be removed before you can remove the domain. Maintenance domains are designed to provide a transparent method of verifying and resolving connectivity problems for end-to-end connections. By default, these connections run between the domain service access points (DSAPs) within each MA defined for a domain, and are manually configured. In contrast, MIPs are interconnection points that make up all possible paths between the DSAPs within an MA. MIPs are automatically generated by the CFM protocol when the MIP Creation Type is set to “Default” or “Explicit,” and the MIP creation state machine is invoked (as defined in IEEE 802.1ag). The default option allows MIPs to be created for all interconnection points within an MA, regardless of the domain’s level in the maintenance hierarchy (e.g., customer, provider, or operator). While the explicit option only generates MIPs within an MA if its associated domain is not at the bottom of the maintenance hierarchy. This option is used to hide the structure of network at the lowest domain level.

The diagnostic functions provided by CFM can be used to detect connectivity failures between any pair of MEPs in an MA. Using MIPs allows these failures to be isolated to smaller segments of the network. Allowing the CFM to generate MIPs exposes more of the network structure to users at higher domain levels, but can speed up the process of fault detection and recovery. This trade-off should be carefully considered when designing a CFM maintenance structure. Also note that while MEPs are active agents which can initiate consistency check messages (CCMs), transmit loop back or link trace messages, and maintain the local CCM database, MIPs, on the other hand, are passive agents which can only validate received CFM messages, and respond to loop back and link trace messages. The MIP creation method defined for an MA takes precedence over the method defined on the CFM Domain List.

Configuring Fault Notification

- ◆ A fault alarm can generate an SNMP notification. It is issued when the MEP fault notification generator state machine detects that the configured time period (MEP Fault Notify Alarm Time) has passed with one or more defects indicated, and fault alarms are

enabled at or above the specified priority level (MEP Fault Notify Lowest Priority). The state machine transmits no further fault alarms until it is reset by the passage of a configured time period (MEP Fault Notify Reset Time) without a defect indication. The normal procedure upon receiving a fault alarm is to inspect the reporting MEP's managed objects using an appropriate SNMP software tool, diagnose the fault, correct it, reexamine the MEP's managed objects to see whether the MEP fault notification generator state machine has been reset, and repeat those steps until the fault is resolved.

◆ Only the highest priority defect currently detected is reported in the fault alarm.

Priority levels include the following options:

Remote MEP Priority Levels

Priority Level	Level Name	Description
1	allDef	All defects.
2	macRemErrXcon	DefMACstatus, DefRemoteCCM, DefErrorCCM, or DefXconCCM.
3	remErrXcon	DefErrorCCM, DefXconCCM or DefRemoteCCM.
4	errXcon	DefErrorCCM or DefXconCCM.
5	xcon	DefXconCCM
6	noXcon	No defects DefXconCCM or lower are to be reported.

MEP Defect Descriptions

Defect	Description
DefMACstatus	Either some remote MEP is reporting its Interface Status TLV as not isUp, or all remote MEPs are reporting a Port Status TLV that contains some value other than psUp.
DefRemoteCCM	The MEP is not receiving valid CCMs from at least one of the remote MEPs.
DefErrorCCM	The MEP has received at least one invalid CCM whose CCM Interval has not yet timed out.
DefXconCCM	The MEP has received at least one CCM from either another MAID or a lower MD Level whose CCM Interval has not yet timed out.

PARAMETERS

These parameters are displayed:

Creating a Maintenance Domain

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MD Name** – Maintenance domain name. (Range: 1-43 alphanumeric characters)
- ◆ **MD Level** – Authorized maintenance level for this domain. (Range: 0-7)
- ◆ **MIP Creation Type** – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this domain:

■ **Default** – MIPs can be created for any maintenance association (MA) configured in this domain on any bridge port through which the MA's VID can pass.

■ **Explicit** – MIPs can be created for any MA configured in this domain only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.

■ **None** – No MIP can be created for any MA configured in this domain.

MD Management Device Management > CFM > MD Management

CFM MD List Total: 0

MD Index (1-65535)

MD Name

MD Level (0-7)

MIP Creation Type

MD Details

Device Management > CFM > MD Details page is used to configure details of specify MD.

PARAMETERS

Configuring Detailed Settings for a Maintenance Domain

- ◆ **MD Index** – Domain index. (Range: 1-65535)
 - ◆ **MEP Archive Hold Time** – The time that data from a missing MEP is retained in the continuity check message (CCM) database before being purged. (Range: 1-65535 minutes; Default: 100 minutes) A change to the hold time only applies to entries stored in the database after this attribute is changed.
 - ◆ **MEP Fault Notify Lowest Priority** – The lowest priority defect that is allowed to generate a fault alarm. (Range: 1-6, Default: 2)
 - ◆ **MEP Fault Notify Alarm Time** – The time that one or more defects must be present before a fault alarm is issued. (Range: 3-10 seconds; Default: 3 seconds)
 - ◆ **MEP Fault Notify Reset Time** – The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued. (Range: 3-10 seconds; Default: 10 seconds)
- Device Management > CFM > MA Management pages is used to create and configure the Maintenance Associations (MA) which define a unique CFM service instance. Each MA can be identified by its parent MD, the MD's maintenance level, the VLAN assigned to the MA, and the set of maintenance end points (MEPs) assigned to it.

COMMAND USAGE

MD Details Device Management > CFM > MD Details

MD Index

MEP Archive Hold Time (1-65535) min

MEP Fault Notify Lowest Priority (1-6)

MEP Fault Notify Alarm Time (3-10) sec

MEP Fault Notify Reset Time (3-10) sec

MA Management

Creating a Maintenance Association

◆ Use the Configure MA – Add screen to create an MA within the selected MD, map it to a customer service instance (S-VLAN), and set the manner in which MIPs are created for this service instance. Then use the MEP List to assign domain service access points (DSAPs) to this service instance.

- ◆ An MA must be defined before any associated DSAPs or remote MEPs can be assigned.
- ◆ Multiple domains at the same maintenance level cannot have an MA on the same VLAN.
- ◆ Before removing an MA, first remove the MEPs assigned to it.
- ◆ For a detailed description of the MIP types, refer to the Command Usage section.

Configuring Detailed Settings for a Maintenance Association

◆ CCMs are multicast periodically by a MEP in order to discover other MEPs in the same MA, and to assure connectivity to all other MEPs/MIPs in the MA.

◆ Each CCM received is checked to verify that the MEP identifier field sent in the message does not match its own MEP ID, which would indicate a duplicate MEP or network loop. If these error types are not found, the CCM is stored in the MEP's local database until aged out.

◆ If a maintenance point fails to receive three consecutive CCMs from any other MEP in the same MA, a connectivity failure is registered.

◆ If a maintenance point receives a CCM with an invalid MEPID or MA level or an MA level lower than its own, a failure is registered which indicates a configuration error or cross-connect error (i.e., overlapping MAs).

◆ The interval at which CCMs are issued should be configured to detect connectivity problems in a timely manner, as dictated by the nature and size of the MA.

◆ The maintenance of a MIP CCM database by a MIP presents some difficulty for bridges carrying a large number of Service Instances, and for whose MEPs are issuing CCMs at a high frequency. For this reason, slower CCM transmission rates may have to be used.

PARAMETERS

These parameters are displayed:

Creating a Maintenance Association

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MA Name** – MA name. (Range: 1-43 alphanumeric characters) Each MA name must be unique within the CFM domain.
- ◆ **Primary VLAN** – Service VLAN ID. (Range: 1-4093) This is the VLAN through which all CFM functions are executed for this MA.
- ◆ **MIP Creation Type** – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this MA:
 - **Default** – MIPs can be created for this MA on any bridge port through which the MA's VID can pass.
 - **Explicit** – MIPs can be created for this MA only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.

■ **None** – No MIP can be created for this MA.

MA Management Device Management > CFM > MA Management

MD Index

CFM MA List Total: 0

MA Index	MA Name	Primary VLAN
<input type="button" value="New"/>		

MD Index

MA Index (1-2147483647)

MA Name

Primary VLAN (1-4094)

MIP Creation Type

MA Details

Device Management > CFM > MA Details page is used to configure details of specify MA.

PARAMETERS

Configuring Detailed Settings for a Maintenance Association

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MA Name Format** – Specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICC-based format.
 - **Character String** – IEEE 802.1ag defined character string format. This is an IETF RFC 2579 DisplayString.
 - **ICC Based** – ITU-T SG13/SG15 Y.1731 defined ICC based format.
- ◆ **Interval Level** – The delay between sending CCMs. The setting for this parameter is expressed as levels 4 through 7, which in turn map to specific intervals of time. (Options: 4 - 100 ms, 5 - 1 sec, 6 - 10 sec, 7 - 60 sec)
- ◆ **Connectivity Check** – Enables transmission of CCMs. (Default: Disabled)
- ◆ **Cross Check** – Enables cross-checking between a static list of MEPs assigned to other devices within the same maintenance association and the MEPs learned through CCMs. Before starting the cross-check process, first configure the remote MEPs that exist on other devices inside the maintenance association using the Remote MEP List. These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational. The cross-check start delay, which sets the maximum delay this device waits for a remote MEP to come up before starting the cross-check operation, is a domain-level parameter. To set this parameter, use the CFM MD Configuration screen.
- ◆ **AIS Status** – Enables/disables suppression of the Alarm Indication Signal (AIS). (Default: Disabled)
- ◆ **AIS Period** – Configures the period at which AIS is sent in an MA. (Range: 1 or 60seconds;

Default: 1 second)

◆ **AIS Transmit Level** – Configure the AIS maintenance level in an MA. (Range: 0-7; Default is 0)

AIS Level must follow this rule: AIS Level >= Domain Level

◆ **AIS Suppress Alarm** – Enables/disables suppression of the AIS. (Default: Disabled)

MA Details	
Device Management > CFM > MA Details	
MD Index	1 ▾
MA Index	1 ▾
MA Name Format	Character String ▾
Interval Level (4-7)	4
Connectivity Check	<input checked="" type="checkbox"/> Enabled
Cross Check	<input checked="" type="checkbox"/> Enabled
AIS Status	<input checked="" type="checkbox"/> Enabled
AIS Period	1 ▾
AIS Transmit Level (0-7)	0
AIS Suppress Alarm	<input type="checkbox"/> Enabled

MEP Management

Device Management > CFM > MEP Management page is used to configure Maintenance End Points (MEPs). MEPs, also called Domain Service Access Points (DSAPs), must be configured at the domain boundary to provide management access for each maintenance association.

COMMAND USAGE

◆ CFM elements must be configured in the following order: (1) maintenance domain at the same level as the MEP to be configured, (2) maintenance association within the domain, and (3) finally the MEPs using the MEP List.

◆ An interface may belong to more than one domain, or to different MAs in different domains.

◆ To change the MEP's MA or the direction it faces, first delete the MEP, and then create a new one.

PARAMETERS

These parameters are displayed:

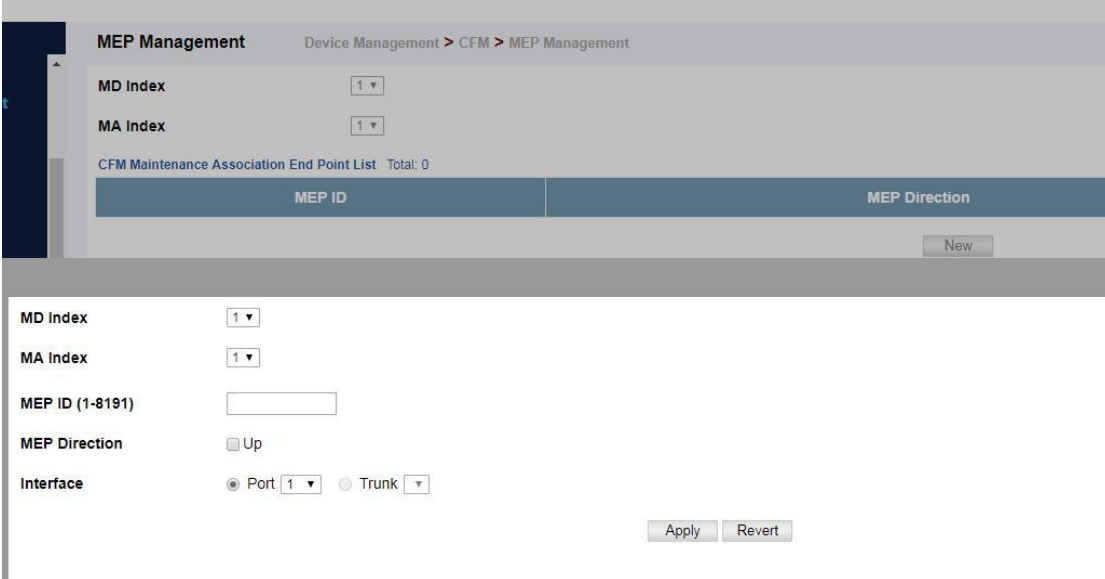
◆ **MD Index** – Domain index. (Range: 1-65535)

◆ **MA Index** – MA identifier. (Range: 1-2147483647)

◆ **MEP ID** – Maintenance end point identifier. (Range: 1-8191)

◆ **MEP Direction** – Up indicates that the MEP faces inward toward the switch cross-connect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism. If the **Up** option is not selected, then the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.

◆ **Interface** – Indicates a port or trunk.



MEP Management Device Management > CFM > MEP Management

MD Index

MA Index

CFM Maintenance Association End Point List Total: 0

MEP ID	MEP Direction
<input type="button" value="New"/>	

MD Index

MA Index

MEP ID (1-8191)

MEP Direction Up

Interface Port Trunk

Remote MEP Management

Device Management > CFM > Remote MEP Management page is used to specify remote maintenance end points (MEPs) set on other CFM-enabled devices within a common MA. Remote MEPs can be added to a static list in this manner to verify that each entry has been properly configured and is operational. When cross-checking is enabled, the list of statically configured remote MEPs is compared against the MEPs learned through continuity check messages (CCMs), and any discrepancies reported via SNMP traps.

COMMAND USAGE

- ◆ All MEPs that exist on other devices inside a maintenance association should be statically configured to ensure full connectivity through the cross-check process.
- ◆ Remote MEPs can only be configured if local domain service access points (DSAPs) have already been created at the same maintenance level and in the same MA. DSAPs are MEPs that exist on the edge of the domain, and act as primary service access points for end-to-end cross-check, loopback, and link-trace functions.
- ◆ The MEP cross-check start delay which sets the maximum delay that a device waits for remote MEPs to come up before starting the crosscheck operation can be configured on the Configure Global page.
- ◆ SNMP traps for continuity check events discovered by cross-check operations can also be configured on the Configure Global page.

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MEP ID** – Identifier for a maintenance end point which exists on another CFM-enabled device within the same MA. (Range: 1-8191)

Remote MEP Management
Device Management > CFM > Remote MEP Management

MD Index

MA Index

CFM Remote Maintenance Association End Point List Total: 0

MEP ID
New

MD Index

MA Index

MEP ID (1-8191)

Transmit Link Trace

Device Management > CFM > Transmit Link Trace page is used to transmit link trace messages (LTMs). These messages can isolate connectivity faults by tracing the path through a network to the designated target node (i.e., a remote maintenance end point).

COMMAND USAGE

- ◆ LTMs can be targeted to MEPs, not MIPs. Before sending a link trace message, be sure you have configured the target MEP for the specified MA.
- ◆ If MAC address of target MEP has not been learned by any local MEP, then the linktrace may fail. Use the Show Remote MEP page to verify that a MAC address has been learned for the target MEP.
- ◆ LTMs are sent as multicast CFM frames, and forwarded from MIP to MIP, with each MIP generating a link trace reply, up to the point at which the LTM reaches its destination or can no longer be forwarded.
- ◆ LTMs are used to isolate faults. However, this task can be difficult in an Ethernet environment, since each node is connected through multipoint links. Fault isolation is even more challenging since the MAC address of the target node can age out in several minutes. This can cause the traced path to vary over time, or connectivity lost if faults cause the target MEP to be isolated from other MEPs in an MA.
- ◆ When using the command line or web interface, the source MEP used by to send a link trace message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.
- ◆ Parameters controlling the link trace cache, including operational state, entry hold time, and maximum size can be configured on the Configure Global page.

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **Source MEP ID** – The identifier of a source MEP that will send the link trace message. (Range: 1-8191)

◆ Target

■ **MEP ID** – The identifier of a remote MEP that is the target of a link trace message. (Range: 1-8191)

■ **MAC Address** – MAC address of a remote MEP that is the target of a link trace message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxxxx

◆ **TTL** – The time to live of the link trace message. (Range: 0-255 hops)

Transmit Link Trace Device Management > CFM > Transmit Link Trace

MD Index	<input type="text" value="1"/>
MA Index	<input type="text" value="1"/>
Source MEP ID (1-8191)	<input type="text"/>
Target	<input checked="" type="radio"/> MEP ID (1-8191) <input type="text"/> <input type="radio"/> MAC Address <input type="text"/> (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxxxx)
TTL (0-255)	<input type="text"/>

Transmit Loopback

Device Management > CFM > Transmit Loopback page is used to transmit Loopback Messages (LBMs). These messages can be used to isolate or verify connectivity faults by submitting a request to a target node (i.e., a remote MEP or MIP) to echo the message back to the source.

COMMAND USAGE

- ◆ Loopback messages can be used for fault verification and isolation after automatic detection of a fault or receipt of some other error report. Loopback messages can also used to confirm the successful restoration or initiation of connectivity. The receiving maintenance point should respond to the loop back message with a loopback reply.
- ◆ The point from which the loopback message is transmitted (i.e., a local DSAP) and the target maintenance point must be within the same MA.
- ◆ If the continuity check database does not have an entry for the specified maintenance point, an error message will be displayed.
- ◆ When using the command line or web interface, the source MEP used by to send a loopback message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **Source MEP ID** – The identifier of a source MEP that will send the loopback message. (Range: 1-8191)
- ◆ **Target**
 - **MEP ID** – The identifier of a remote MEP that is the target of a loopback message. (Range: 1-8191)

■ **MAC Address** – MAC address of a remote MEP that is the target of a loopback message.

This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or
XXXXXXXXXXXX

◆ **Count** – The number of times the loopback message is sent. (Range: 1-1024)

◆ **Packet Size** – The size of the loopback message. (Range: 64-1518 bytes; Default: 64 bytes)

Transmit Loopback Device Management > CFM > Transmit Loopback

MD Index	<input type="text" value="1"/>	
MA Index	<input type="text" value="1"/>	
Source MEP ID (1-8191)	<input type="text"/>	
Target	<input checked="" type="radio"/> MEP ID (1-8191) <input type="text"/> <input type="radio"/> MAC Address <input style="width: 150px;" type="text"/> (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)	
Counts (1-1024)	<input type="text"/>	
Packet Size (64-1518)	<input type="text"/>	bytes

Result

Transmit Delay Measure

Device Management > CFM > Transmit Delay Measure page is used to send periodic delay-measure requests to a specified MEP within a maintenance association.

COMMAND USAGE

- ◆ Delay measurement can be used to measure frame delay and frame delay variation between MEPs.
- ◆ A local MEP must be configured for the same MA before you can use this function.
- ◆ If a MEP is enabled to generate frames with delay measurement (DM) information, it periodically sends DM frames to its peer MEP in the same MA., and expects to receive DM frames back from it.
- ◆ Frame delay measurement can be made only for two-way measurements, where the MEP transmits a frame with DM request information with the TxTimeStampf (Timestamp at the time of sending a frame with DM request information), and the receiving MEP responds with a frame with DM reply information with TxTimeStampf copied from the DM request information, RxTimeStampf (Timestamp at the time of receiving a frame with DM request information), and TxTimeStamptb (Timestamp at the time of transmitting a frame with DM reply information): Frame Delay =
(RxTimeStamptb-TxTimeStampf)-(TxTimeStamptb-RxTimeStampf)
- ◆ The MEP can also make two-way frame delay variation measurements based on its ability to calculate the difference between two subsequent two-way frame delay measurements.

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)

◆ **Source MEP ID** – The identifier of a source MEP that will send the delay-measure message. (Range: 1-8191)

◆ **Target**

■ **MEP ID** – The identifier of a remote MEP that is the target of a delay-measure message. (Range: 1-8191)

■ **MAC Address** – MAC address of a remote MEP that is the target of a delay-measure message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

◆ **Count** – The number of times to retry sending the message if no response is received before the specified timeout. (Range: 1-5; Default: 5)

◆ **Packet Size** – The size of the delay-measure message. (Range: 64-1518 bytes; Default: 64 bytes)

◆ **Interval** – The transmission delay between delay-measure messages. (Range: 1-5 seconds; Default: 1 second)

◆ **Timeout** – The timeout to wait for a response. (Range: 1-5 seconds; Default: 5 seconds)

Transmit Delay Measure
Device Management > CFM > Transmit Delay Measure

MD Index	<input type="text" value="1"/>	
MA Index	<input type="text" value="1"/>	
Source MEP ID (1-8191)	<input type="text"/>	
Target	<input checked="" type="radio"/> MEP ID (1-8191) <input type="text"/> <input type="radio"/> MAC Address <input type="text"/> (xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx)	
Counts (1-5)	<input type="text"/>	
Packet Size (64-1518)	<input type="text"/>	bytes
Interval (1-5)	<input type="text"/>	sec
Timeout (1-5)	<input type="text"/>	sec

Result

Show Local MEP

Device Management > CFM > Show Local MEP page is used to show information for the MEPs configured on this device.

PARAMETERS

These parameters are displayed:

◆ **MEP ID** – Maintenance end point identifier.

◆ **MD Name** – Maintenance domain name.

◆ **Level** – Authorized maintenance level for this domain.

◆ **Direction** – Direction in which the MEP communicates CFM messages:

■ Down indicates that the MEP is facing away from the switch, and transmits CFM messages

towards, and receives them from, the direction of the physical medium.

■ **Up** indicates that the MEP faces inward toward the switch crossconnect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism.

- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **Interface** – Physical interface of this entry (either a port or trunk).
- ◆ **CC Status** – Shows administrative status of CCMs.
- ◆ **MAC Address** – MAC address of this MEP entry.

Show Local MEP Device Management > CFM > Show Local MEP

CFM Local Maintenance Association End Point Information Total: 1

MEP ID	MD Name	Level	Direction	Primary VLAN	Interface	CC Status	MAC Address
1	md1	3	Down	1	Unit 1 / Port 1	Enabled	00-00-01-03-00-02

Show Local MEP Details

Device Management > CFM > Show Local MEP Details page is used to show detailed CFM information about a local MEP in the continuity check database.

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MEP ID** – Maintenance end point identifier. (Range: 1-8191)
- ◆ **MD Name** – The maintenance domain for this entry.
- ◆ **MA Name** – Maintenance association to which this remote MEP belongs.
- ◆ **MA Name Format** – The format of the Maintenance Association name, including primary VID, character string, unsigned Integer 16, or RFC 2865 VPN ID.
- ◆ **Level** – Maintenance level of the local maintenance point.
- ◆ **Direction** – The direction in which the MEP faces on the Bridge port (up or down).
- ◆ **Interface** – The port to which this MEP is attached.
- ◆ **CC Status** – Shows if the MEP will generate CCM messages.
- ◆ **MAC Address** – MAC address of the local maintenance point. (If a CCM for the specified remote MEP has never been received or the local MEP record times out, the address will be set to the initial value of all Fs.)
- ◆ **Defect Condition** – Shows the defect detected on the MEP.
- ◆ **Received RDI** – Receive status of remote defect indication (RDI) messages on the MEP.
- ◆ **AIS Status** – Shows if MEPs within the specified MA are enabled to send frames with AIS information following detection of defect conditions.
- ◆ **AIS Period** – The interval at which AIS information is sent.
- ◆ **AIS Transmit Level** – The maintenance level at which AIS information will be sent for the specified MEP.
- ◆ **Suppress Alarm** – Shows if the specified MEP is configured to suppress sending frames containing AIS information following the detection of defect conditions.
- ◆ **Suppressing Alarms** – Shows if the specified MEP is currently suppressing sending frames containing AIS information following the detection of defect conditions.

Show Local MEP Details Device Management > CFM > Show Local MEP Details

MD Index: 1 ▼

MA Index: 1 ▼

MEP ID: 1 ▼

Query

MD Name: md1

MA Name: ma1

MA Name Format: Character String

Level: 3

Direction: Down

Interface: Eth 1/1

CC Status: Enabled

MAC Address: 00-00-01-03-00-02

Defect Condition: defRemoteCCM

Received RDI: False

AIS Status: Enabled

Show Local MIP

Device Management > CFM > Show Local MIP page is used to show the MIPs on this device discovered by the CFM protocol.

PARAMETERS

These parameters are displayed:

- ◆ **MD Name** – Maintenance domain name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **Interface** – Physical interface of this entry (either a port or trunk).

Show Local MIP Device Management > CFM > Show Local MIP

CFM Local Maintenance Association Intermediate Point Information Total: 49

MD Name	Level	MA Name	Primary VLAN	Interface
md1	3	ma1	1	Unit 1 / Port 2
md1	3	ma1	1	Unit 1 / Port 3
md1	3	ma1	1	Unit 1 / Port 4
md1	3	ma1	1	Unit 1 / Port 5
md1	3	ma1	1	Unit 1 / Port 6
md1	3	ma1	1	Unit 1 / Port 7
md1	3	ma1	1	Unit 1 / Port 8
md1	3	ma1	1	Unit 1 / Port 9

Show Remote MEP

Device Management > CFM > Show Remote MEP page is used to show MEPs located on

other devices which have been discovered through continuity check messages, or statically configured in the MEP database and verified through cross-check messages.

PARAMETERS

These parameters are displayed:

- ◆ **MEP ID** – Maintenance end point identifier.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **MEP Up** – Indicates whether or not this MEP is functioning normally.
- ◆ **Remote MAC Address** – MAC address of the remote maintenance point. (If a CCM for the specified remote MEP has never been received or the remote MEP record times out, the address will be set to the initial value of all Fs.)

Show Remote MEP						
Device Management > CFM > Show Remote MEP						
CFM Remote Maintenance Association End Point Information Total: 1						
MEP ID	MA Name	Level	Primary VLAN	MEP Up	Remote MAC Address	
2	ma1	3	1	No	Not Configured	

Show Remote MEP Details

Device Management > CFM > Show Remote MEP Details is used page to show detailed information for MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database and verified through cross-check messages.

PARAMETERS

These parameters are displayed:

- ◆ **MD Index** – Domain index. (Range: 1-65535)
- ◆ **MA Index** – MA identifier. (Range: 1-2147483647)
- ◆ **MEP ID** – Maintenance end point identifier. (Range: 1-8191)
- ◆ **MD Name** – Maintenance domain name.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Level** – Authorized maintenance level for this domain.
- ◆ **MAC Address** – MAC address of this MEP entry.
- ◆ **Primary VLAN** – Service VLAN ID.
- ◆ **Incoming Port** – Port to which this remote MEP is attached.
- ◆ **CC Lifetime** – Length of time to hold messages about this MEP in the CCM database.
- ◆ **Age of Last CC Message** – Length of time the last CCM message about this MEP has been in the CCM database.
- ◆ **Frame Loss** – Percentage of transmitted frames lost.
- ◆ **CC Packet Statistics** – The number of CCM packets received successfully and those with errors.
- ◆ **Port State** – Port states include:
 - Up – The port is functioning normally.
 - Blocked – The port has been blocked by the Spanning Tree Protocol.
 - No port state – Either no CCM has been received, or nor port status TLV was received in

the last CCM.

◆ **Interface State** – Interface states include:

- No Status – Either no CCM has been received, or no interface status TLV was received in the last CCM.
 - Up – The interface is ready to pass packets.
 - Down – The interface cannot pass packets.
 - Testing – The interface is in some test mode.
 - Unknown – The interface status cannot be determined for some reason.
 - Dormant – The interface is not in a state to pass packets but is in a pending state, waiting for some external event.
 - Not Present – Some component of the interface is missing.
 - isLowerLayerDown – The interface is down due to state of the lower layer interfaces.
- ◆ **Crosscheck Status** – Shows if crosscheck function has been enabled.

Show Link Trace Cache

Device Management > CFM > Show Link Trace Cache page is used to show information about link trace operations launched from this device.

PARAMETERS

These parameters are displayed:

- ◆ **Hops** – The number hops taken to reach the target MEP.
- ◆ **MA** – Maintenance association name.
- ◆ **IP/Alias** – IP address or DNS alias of the target device's CPU.
- ◆ **Forwarded** – Shows whether or not this link trace message was forwarded. A message is not forwarded if received by the target MEP.
- ◆ **Ingress MAC Address** – MAC address of the ingress port on the target device.
- ◆ **Egress MAC Address** – MAC address of the egress port on the target device.
- ◆ **Ingress Action** – Action taken on the ingress port:
 - IngOk – The target data frame passed through to the MAC Relay Entity.
 - IngDown – The bridge port's MAC_Operational parameter is false. This value could be returned, for example, by an operationally Down MEP that has another Down MEP at a higher MD level on the same bridge port that is causing the bridge port's MAC_Operational parameter to be false.
 - IngBlocked – The ingress port can be identified, but the target data frame was not forwarded when received on this port due to active topology management, i.e., the bridge port is not in the forwarding state.
 - IngVid – The ingress port is not in the member set of the LTM's VIDs, and ingress filtering is enabled, so the target data frame was filtered by ingress filtering.
- ◆ **Egress Action** – Action taken on the egress port:
 - EgrOk – The targeted data frame was forwarded.
 - EgrDown – The Egress Port can be identified, but that bridge port's MAC_Operational parameter is false.
 - EgrBlocked – The egress port can be identified, but the data frame was not passed through the egress port due to active topology management, i.e., the bridge port is not in

the forwarding state.

■ **EgrVid** – The Egress Port can be identified, but the bridge port is not in the LTM’s VID member set, and was therefore filtered by egress filtering.

◆ **Reply** – Reply action:

■ **FDB** – Target address found in forwarding database.

■ **MPDB** – Target address found in the maintenance point database.

■ **HIT** – Target located on this device.

Show Link Trace Cache								
Device Management > CFM > Show Link Trace Cache								
CFM Link Trace Cache Information Total: 0								
Hops	MA	IP Address/Alias	Forwarded	Ingress MAC Address	Egress MAC Address	Ingress Action	Egress Action	Reply

Show Fault Notification Generator

Device Management > CFM > Show Fault Notification Generator page is used to display configuration settings for the fault notification generator.

PARAMETERS

These parameters are displayed:

- ◆ **MEP ID** – Maintenance end point identifier.
- ◆ **MD Name** – Maintenance domain name.
- ◆ **MA Name** – Maintenance association name.
- ◆ **Highest Defect** – The highest defect that will generate a fault alarm. (This is disabled by default.)
- ◆ **Lowest Alarm** – The lowest defect that will generate a fault alarm.
- ◆ **Alarm Time** – The time a defect must exist before a fault alarm is issued.
- ◆ **Reset Time** – The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued.

Show Fault Notification Generator						
Device Management > CFM > Show Fault Notification Generator						
CFM Fault Notification Generator Information Total: 1						
MEP ID	MD Name	MA Name	Highest Defect	Lowest Alarm	Alarm Time (sec)	Reset Time (sec)
1	md1	ma1	deRemoteCCM	macRemErrXcon	3	10

Show Continuity Check Error

Device Management > CFM > Show Continuity Check Error page is used to display the CFM continuity check errors logged on this device.

PARAMETERS

These parameters are displayed:

- ◆ **Level** – Maintenance level associated with this entry.
- ◆ **Primary VLAN** – VLAN in which this error occurred.
- ◆ **MEP ID** – Identifier of remote MEP.
- ◆ **Interface** – Port at which the error was recorded.
- ◆ **Remote MAC** – MAC address of remote MEP.
- ◆ **Reason** – Error types include:
 - **LEAK** – MA x is associated with a specific VID list14, one or more of the VIDs in this MA can

pass through the bridge port, no MEP is configured facing outward (down) on any bridge port for this MA, and some other MA y, at a higher maintenance level, and associated with at least one of the VID(s) also in MA x, does have a MEP configured on the bridge port.

■ **VIDS** – MA x is associated with a specific VID list¹⁴, an MEP is configured facing inward (up) on this MA on the bridge port, and some other MA y, associated with at least one of the VID(s) also in MA x, also has an Up MEP configured facing inward (up) on some bridge port.

■ **EXCESS_LEV** – The number of different MD levels at which MIPs are to be created on this port exceeds the bridge's capabilities.

■ **OVERLAP_LEV** – A MEP is created for one VID at one maintenance level, but a MEP is configured on another VID at an equivalent or higher level, exceeding the bridge's capabilities.

◆ **MA Name** – The maintenance association for this entry.

Show Continuity Check Error						
Device Management > CFM > Show Continuity Check Error						
CFM Continuity Check Error Information Total: 0						
Level	Primary VLAN	MEP ID	Interface	Remote MAC	Reason	MA Name

Time Setting

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock. If the clock is not set manually or via SNTP, the switch will only record the time from the factory default set at the last bootup. When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

Configure time

The Device Management > Time Setting > Configure time page is used to set the system time on the switch manually without using SNTP.

PARAMETERS

The following parameters are displayed:

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

Configure time Device Management > Time Setting > Configure time

Current Time 2008-11-20 14:28:50

Maintain Type

14 Hours 28 Minutes 50 Seconds

11 Month 20 Day 2008 Year

Configure time Device Management > Time Setting > Configure time

Current Time 2008-11-20 14:28:50

Maintain Type

SNTP Configuration

SNTP Polling Interval (16-16384) sec

SNTP Server

The Device Management > Time Setting > SNTP Server page is used to specify the IP address for up to three SNTP time servers.

PARAMETERS

The following parameters are displayed:

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

SNTP Server Device Management > Time Setting > SNTP Server

SNTP Server IP Address 1

SNTP Server IP Address 2

SNTP Server IP Address 3

NTP Server

The Device Management > Time Setting > NTP Server page is used to add the IP address for up to 50 NTP time servers.

PARAMETERS

The following parameters are displayed:

◆ **NTP Server IP Address** – Adds the IPv4 or IPv6 address for up to 50 time servers. The switch will poll the specified time servers for updates when the clock maintenance type is set to NTP on the System > Time (Configure General) page. It issues time synchronization requests at a fixed interval of 1024 seconds. The switch will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.

◆ **Version** – Specifies the NTP version supported by the server. (Fixed: Version 3)

◆ **Authentication Key** – Specifies the number of the key in the NTP Authentication Key List to use for authentication with the configured server. NTP authentication is optional. If enabled on the System > Time (Configure General) page, you must also configure at least one key on the System > Time (Add NTP Authentication Key) page. (Range: 1-65535)

NTP Server Stacking Unit: 1

Device Management > Time Setting > NTP Server

NTP Server List Total: 10

Server IP Address	Version	Authentication Key
10.1.0.1	3	2
10.2.0.1	3	8
10.3.0.1	1	65535
10.4.0.1	2	1000
10.5.0.1	2	1000
10.6.0.1	2	1000
10.7.0.1	2	1000
10.8.0.1	2	1000
10.9.0.1	2	1000
10.10.0.1	2	1000

New Delete Revert

NTP Server IP Address

Version 3

Authentication Key (1-65535) (optional)

Apply Revert

NTP authentication Key

The Device Management > Time Setting > NTP Authentication Key page is used to add an entry to the authentication key list.

PARAMETERS

The following parameters are displayed:

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

NTP Authentication Key Stacking Unit: 1

Device Management > Time Setting > NTP Authentication Key

NTP Authentication Key List Total: 30

Authentication Key	Key Context
1	test
2	abc
3	abc
4	abc
5	abc
6	abc
7	abc
8	abc
9	abc
10	abc

New Delete Revert

Configure Time Zone

The Device Management > Time Setting > Configure Time Zone page is used to set the time zone.

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

PARAMETERS

The following parameters are displayed:

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



Configure Summer Time

The Device Management > Time Setting > Configure Summer Time page is used to set the system clock forward during the summer months (also known as daylight savings time). In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

Parameters

The following parameters are displayed in the web interface:

General Configuration

- ◆ **Summer Time in Effect** – Shows if the system time has been adjusted.
- ◆ **Status** – Shows if summer time is set to take effect during the specified period.
- ◆ **Name** – Name of the time zone while summer time is in effect, usually an acronym. (Range: 1-30 characters)
- ◆ **Mode** – Selects one of the following configuration modes. (The Mode option can only be managed when the Summer Time Status option has been set to enabled for the switch.)
 - Predefined Mode* – Configures the summer time status and settings for the switch using predefined configurations for several major regions of the world. To specify the time

corresponding to your local time when summer time is in effect, select the predefined summer-time zone appropriate for your location.

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

◆ **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 1-120 minutes)

◆ **From** – Start time for summer-time offset.

◆ **To** – End time for summer-time offset.

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

◆ **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 1-120 minutes)

◆ **From** – Start time for summer-time offset.

◆ **To** – End time for summer-time offset.

Configure Summer Time Device Management > Time Setting > Configure Summer Time

Summer Time in Effect: No

Status: Enabled

Name:

Mode: Recurring

Recurring Mode Configuration

Offset (1-120): minutes

From: Week 1st Day Sunday Month January Time 00:00 (HH:MM)

To: Week 1st Day Sunday Month January Time 00:00 (HH:MM)

Apply Revert

Event Log

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

Show System Logs

The Device Management > Event Log > Show System Logs page is used to display System Logs This page allows you to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset)

and up to 4096 entries in permanent flash memory.

Show System Logs Device Management > Event Log > Show System Logs

Log Type RAM Flash

System RAM Logs

```
[363] 06:41:22 2018-09-08
"LLDP remote tables changed."
level: 6, module: 5, function: 1, and event no: 1
-----
[362] 06:41:22 2018-09-08
"LLDP remote table changed on Eth 1/6."
level: 6, module: 112, function: 1, and event no: 1
-----
[361] 06:37:08 2018-09-08
"LLDP remote tables changed."
level: 6, module: 5, function: 1, and event no: 1
-----
[360] 06:37:08 2018-09-08
"LLDP remote table changed on Eth 1/6."
level: 6, module: 112, function: 1, and event no: 1
-----
```

Configure Global

The Device Management > Event Log > Configure Global page is used to enable or disable event logging, and specify which levels are logged to RAM or flash memory. Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

PARAMETERS

These parameters are displayed:

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

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

0	Emergency	System unusable
---	-----------	-----------------

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

Configure Global Device Management > Event Log > Configure Global

Status Enabled

History Flash Level 3 - Error ▼

History RAM Level 7 - Debugging ▼

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

Apply Revert

Remote

The Device Management > Event Log > Remote page is used to send log messages to syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.

PARAMETERS

These parameters are displayed:

◆ **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)

◆ **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service. The attribute specifies the facility type tag sent in syslog messages (see RFC 3164). This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)

◆ **Logging Trap Level** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)

◆ **Server IP Address** – Specifies the IPv4 or IPv6 address of a remote server which will be sent syslog messages.

Remote Device Management > Event Log > Remote

Remote Log Status Enabled

Logging Facility 23 - Local use 7 ▼

Logging Trap Level 7 - Debugging messages ▼

Server IP Address 1 Port

Server IP Address 2 Port

Server IP Address 3 Port

Server IP Address 4 Port

Server IP Address 5 Port

Apply Revert

SMTP

The Device Management > Event Log > SMTP page is used to alert system administrators of problems by sending SMTP (Simple Mail Transfer Protocol) email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

Parameters

These parameters are displayed:

- ◆ **SMTP Status** – Enables/disables the SMTP function. (Default: Enabled)
- ◆ **Severity** – Sets the syslog severity threshold level used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default: Level 7)
- ◆ **Email Source Address** – Sets the email address used for the “From” field in alert messages. You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch. (Range: 1-41 characters)
- ◆ **Email Destination Address** – Specifies the email recipients of alert messages. You can specify up to five recipients.
- ◆ **Server IP Address** – Specifies a list of up to three recipient SMTP servers. IPv4 or IPv6 addresses may be specified. The switch attempts to connect to the listed servers in sequential order if the first server fails to respond. For host name-to-IP address translation to function properly, host name lookup must be enabled, and one or more DNS servers specified.




The screenshot shows the SMTP configuration page with the following fields and values:

Parameter	Value
SMTP Status	<input checked="" type="checkbox"/> Enabled
Severity	7 - Debugging
E-mail Source Address	<input type="text"/>
E-mail Destination Address 1	<input type="text"/>
E-mail Destination Address 2	<input type="text"/>
E-mail Destination Address 3	<input type="text"/>
E-mail Destination Address 4	<input type="text"/>
E-mail Destination Address 5	<input type="text"/>
Server IP Address 1	<input type="text"/>
Server IP Address 2	<input type="text"/>
Server IP Address 3	<input type="text"/>

Buttons: Apply, Revert

File Management

Device Management > File Management page is used to manage the file in device. User can upload configuration file to PC, download runtime file to device. Copy a configuration file to another configuration file.



File List	Total	4		
File Name	File Type	Start-Up	Modify Time	Size (bytes)
<input type="checkbox"/> S5600-28TS-R-P001B001V0156.bin	Operation Code	Y	2018-08-23 00:51:41	19310996
<input type="checkbox"/> S5600-28TS-R-P001B001V0157.bin	Operation Code	N	2018-08-23 00:53:33	19310996
<input type="checkbox"/> Factory_Default_Config.cfg	Config File	N	2018-08-23 00:47:47	455
<input type="checkbox"/> startup1.cfg	Config File	Y	2018-08-23 00:47:45	1739

Buttons: Startup Copy Delete Revert

Copying Files via FTP/TFTP or HTTP

In the Device Management> File Management page, click copy button to download firmware or configuration settings using FTP, TFTP or HTTP. You can also set the switch to use new firmware or configuration settings without overwriting the current version. Just download the file using a different name from the current version, and then set the new file as the startup file.

The following parameters are displayed:

◆ **Copy Type** – The firmware copy operation includes these options:

■ **FTP Upload** – Copies a file from an FTP server to the switch.

■ **HTTP Upload**– Copies a file from a management station to the switch.

■ **TFTP Upload** – Copies a file from a TFTP server to the switch.

◆ **FTP/TFTP Server IP Address** – The IP address of an FTP/TFTP server.

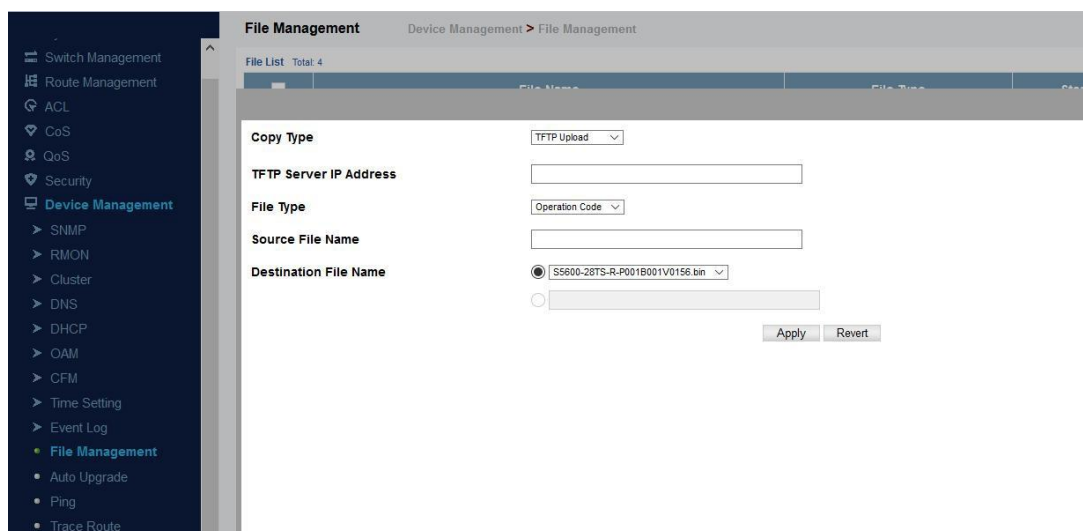
◆ **User Name** – The user name for FTP server access.

◆ **Password** – The password for FTP server access.

◆ **File Type** – Specify Operation Code to copy firmware.

◆ **File Name** – The file name should not contain slashes (\ or /), and the maximum length for file names is 32 characters for files on the switch or 128 characters for files on the server.

(Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)



File Management Device Management > File Management

File List Total: 4

Copy Type TFTP Upload

TFTP Server IP Address

File Type Operation Code

Source File Name

Destination File Name
 S5600-28TS-R-P001B001V0156.bin

Buttons: Apply Revert

Saving the Running Configuration to a Local File

In the Device Management > File Management page, click copy button to save the current configuration settings to a local file on the switch. The configuration settings are not automatically saved by the system for subsequent use when the switch is rebooted. You must save these settings to the current startup file, or to another file which can be subsequently set as the startup file.

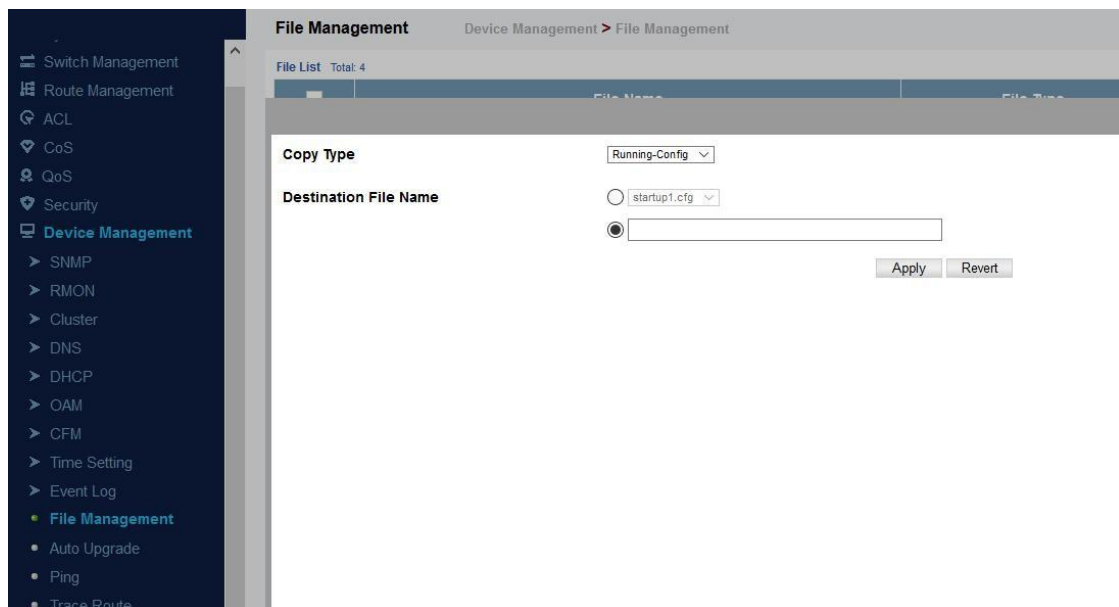
The following parameters are displayed:

◆ **Copy Type** – The copy operation includes this option:

■ Running-Config – Copies the current configuration settings to a local file on the switch.

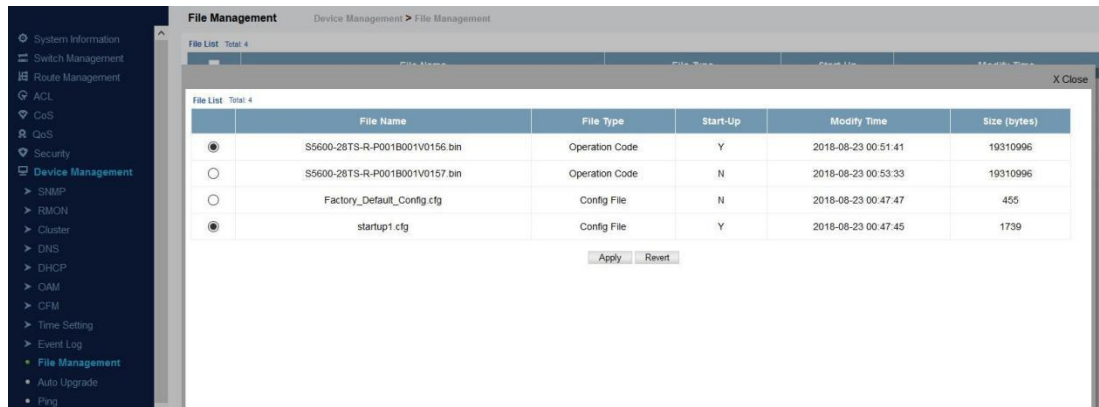
◆ **Destination File Name** – Copy to the currently designated startup file, or to a new file. The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

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



Setting the Startup File

In the Device Management > File Management page, click StartUp button to specify the firmware or configuration file to use for system initialization.



Auto Upgrade

Device Management > Auto Upgrade page is used to automatically download an operation code file when a file newer than the currently installed one is discovered on the file server. After the file is transferred from the server and successfully written to the file system, it is automatically set as the startup file, and the switch is rebooted.

USAGE GUIDELINES

- ◆ If this feature is enabled, the switch searches the defined URL once during the bootup sequence.
- ◆ FTP (port 21) and TFTP (port 69) are both supported. Note that the TCP/UDP port bindings cannot be modified to support servers listening on non-standard ports.
- ◆ The host portion of the upgrade file location URL must be a valid IPv4 IP address. DNS host names are not recognized. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- ◆ The path to the directory must also be defined. If the file is stored in the root directory for the FTP/TFTP service, then use the “/” to indicate this (e.g., ftp://192.168.0.1/).
- ◆ The file name must not be included in the upgrade file location URL. The file name of the code stored on the remote server must be *ECS4510-Series.bix* (using upper case and lower case letters exactly as indicated here). Enter the file name for other switches described in this manual exactly as shown on the web interface.
- ◆ The FTP connection is made with PASV mode enabled. PASV mode is needed to traverse some fire walls, even if FTP traffic is not blocked. PASV mode cannot be disabled.
- ◆ The switch-based search function is case-insensitive in that it will accept a file name in upper or lower case (i.e., the switch will accept *ECS4510-SERIES.BIX* from the server even though *ECS4510-SERIES.bix* was requested). However, keep in mind that the file systems of many operating systems such as Unix and most Unixlike systems (FreeBSD, NetBSD, OpenBSD, and most Linux distributions, etc.) are case-sensitive, meaning that two files in the same directory, *ecs4510-series.bix* and *ECS4510-SERIES.bix* are considered to be unique files. Thus, if the upgrade file is stored as *ECS4510-SERIES.bix* (or even *EcS4510-SERIES.bix*) on a case sensitive server, then the switch (requesting *ecs4510-series.bix*) will not be upgraded

because the server does not recognize the requested file name and the stored file name as being equal. A notable exception in the list of case-sensitive Unix-like operating systems is Mac OS X, which by default is case-insensitive. Please check the documentation for your server's operating system if you are unsure of its file system's behavior.

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

PARAMETERS

The following parameters are displayed:

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

The following syntax must be observed:

tftp://host[/filedir]/

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

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

- **ftp://** – Defines FTP protocol for the server connection.
- **username** – Defines the user name for the FTP connection. If the user name is omitted, then “anonymous” is the assumed user name for the connection.
- **password** – Defines the password for the FTP connection. To differentiate the password from the user name and host portions of the URL, a colon (:) must precede the password,

and an “at” symbol (@), must follow the password. If the password is omitted, then “” (an empty string) is the assumed password for the connection.

■ *host* – Defines the IP address of the FTP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. DNS host names are not recognized.

■ *filedir* – Defines the directory, relative to the FTP server root, where the upgrade file can be found. Nested directory structures are accepted. The directory name must be separated from the host, and in nested directory structures, from the parent directory, with a prepended forward slash “/”.

■ */* – The forward slash must be the last character of the URL.

Examples

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

■ `tftp://192.168.0.1/`

The image file is in the TFTP root directory.

■ `tftp://192.168.0.1/switch-opcode/`

The image file is in the “switch-opcode” directory, relative to the TFTP root.

■ `tftp://192.168.0.1/switches/opcode/`

The image file is in the “opcode” directory, which is within the “switches” parent directory, relative to the TFTP root. The following examples demonstrate the URL syntax for an FTP server at IP address 192.168.0.1 with various user name, password and file location options presented:

■ `ftp://192.168.0.1/`

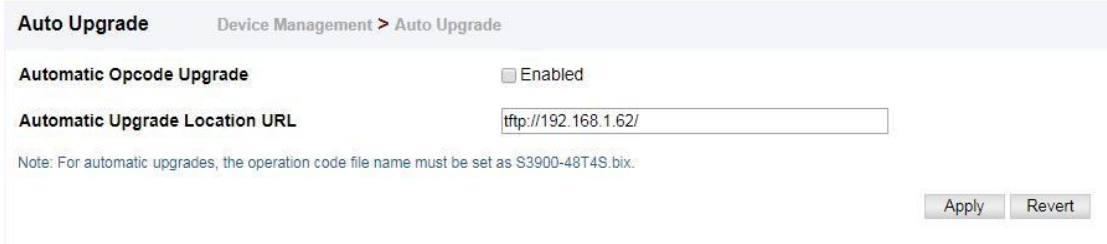
The user name and password are empty, so “anonymous” will be the user name and the password will be blank. The image file is in the FTP root directory.

■ `ftp://switches:upgrade@192.168.0.1/`

The user name is “switches” and the password is “upgrade”. The image file is in the FTP root.

■ `ftp://switches:upgrade@192.168.0.1/switches/opcode/`

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



Ping

The Device Management > Ping page is used to send ICMP echo request packets to another node on the network.

PARAMETERS

These parameters are displayed:

◆ **Host Name/IP Address** – IP address or alias of the host.

- ◆ **Probe Count** – Number of packets to send. (Range: 1-16)
- ◆ **Packet Size** – Number of bytes in a packet. (Range: 32-512 bytes)

The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

COMMAND USAGE

- ◆ Use the ping command to see if another site on the network can be reached.
- ◆ The following are some results of the **ping** command:
 - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
 - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
 - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
 - *Network or host unreachable* - The gateway found no corresponding entry in the route table.

Ping Device Management > Ping

Host Name/IP Address	<input type="text"/>
Probe Count (1-16)	<input type="text" value="5"/>
Data Size (IPv4 : 32-512, IPv6 : 0-1500)	<input type="text"/> bytes

Note: For IPv4 Data Size,
 0 - 31 changed to 32 bytes
 32 - 512 is valid input
 513 - 1500 changed to 512 bytes
 < 0 or > 1500 not valid input

Trace Route

The Device Management > Trace Route page is used to show the route packets take to the specified destination.

Parameters

These parameters are displayed:

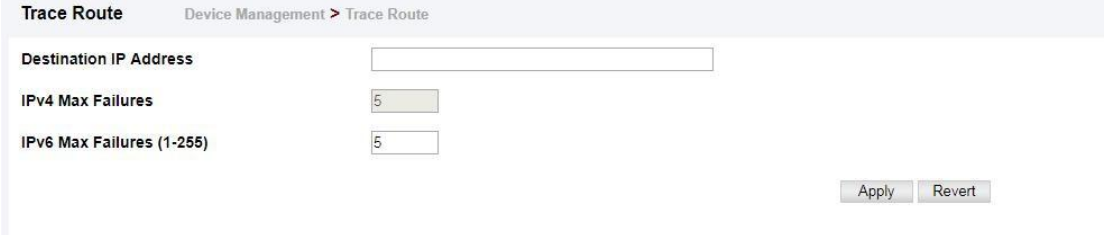
- ◆ **Destination IP Address** – Alias or IPv4/IPv6 address of the host.
- ◆ **IPv4 Max Failures** – The maximum number of failures before which the trace route is terminated. (Fixed: 5)
- ◆ **IPv6 Max Failures** – The maximum number of failures before which the trace route is terminated. (Range: 1-255; Default: 5)

Command Usage

- ◆ Use the trace route function to determine the path taken to reach a specified destination.
- ◆ A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- ◆ The trace route function first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning

an “ICMP port unreachable” message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the “Request Timed Out” message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

◆ The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the trace route is sent.



System Reboot

The Device Management > System Reboot page is used to restart the switch immediately, at a specified time, after a specified delay, or at a periodic interval.

Command Usage

- ◆ This command resets the entire system.
- ◆ When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory.

Parameters

The following parameters are displayed:

System Reload Information

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

System Reload Configuration

- ◆ **Reset Mode** – Restarts the switch immediately or at the specified time(s).
- **Immediately** – Restarts the system immediately.
- **In** – Specifies an interval after which to reload the switch. (The specified time must be equal to or less than 24 days.)
- **hours** – The number of hours, combined with the minutes, before the switch resets. (Range: 0-576)
- **minutes** – The number of minutes, combined with the hours, before the switch resets. (Range: 0-59)
- **At** – Specifies a time at which to reload the switch.
- **DD** – The day of the month at which to reload. (Range: 01-31)

- MM - The month at which to reload. (Range: 01-12)
- YYYY - The year at which to reload. (Range: 1970-2037)
- HH - The hour at which to reload. (Range: 00-23)
- MM - The minute at which to reload. (Range: 00-59)
- **Regularly** – Specifies a periodic interval at which to reload the switch. *Time*
- HH - The hour at which to reload. (Range: 00-23)
- MM - The minute at which to reload. (Range: 00-59) *Period*
- Daily - Every day.
- Weekly - Day of the week at which to reload. (Range: Sunday ... Saturday)
- Monthly - Day of the month at which to reload. (Range: 1-31)

System Reboot Device Management > System Reboot

System Reload Information:
No configured settings for reloading.

System Reload Configuration:

Reset Mode



 <https://www.fs.com>



All statements, technical information, and recommendations related to the products here are based upon information believed to be reliable or accurate. However, the accuracy or completeness thereof is not guaranteed, and no responsibility is assumed for any inaccuracies. Please contact FS for more information.