SOLTECH
Solution of optical & Network

SFC8000HP
Managed Industrial Power over Ethernet Switch

User's Manual

8-Port 10/100/1000-T(802.3at)
2-Slot SFP (100/1000/2.5Gbps) Switch

www.soltech.co.kr

CONTENTS

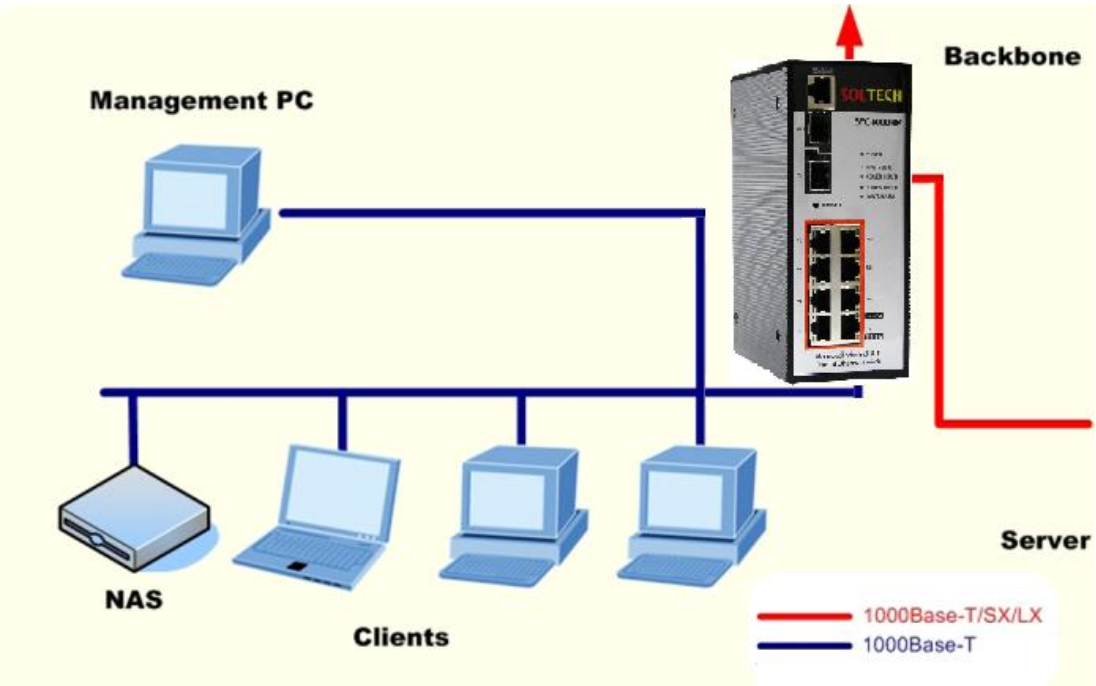
1 Introduction

1.1 PRODUCT INTRODUCTION

SFC8000HP is a Managed Industrial Gigabit Ethernet Switch which has 8 RJ-45 10/100/1000Mbps ports, 2 100M/1000M/2.5GBase-SX/LX SFP slots and non-blocking wire-speed function.

Gigabit Ethernet Switch can transmit a huge data through 20Gbps internal Switch fabric into backbone or high-power servers in security topology.

SFC8000HP can find 8K MAC address, provides wired Packet transmit function without any packet loss. Its high throughput of data provides convenience to users when upgrade to Gigabit network. It also supports Carrier Ethernet and guarantee high safety of transmitting data.



1.2 PRODUCT SEPCIFICATION

○ Physical Port

- 8port 10/100/1000M Base-T
- 2port SFP slots Port 9 and Port 10
- Reset button for system management

○ Generic Features

- Comply with IEEE802.3, 10Base-T, IEEE 802.3u, 100Base-TX, IEEE 802.3ab, 1000Base-T,
- IEEE 802.3z, 100/1000Base-SX/LX, Ethernet standard
- Auto-MDI/MDI-X detection on each RJ-45 port

- Prevents packet loss with back pressure (half-duplex) and 802.3x PAUSE frame flow control (Full-duplex)
- 8K MAC address table, automatic source address learning and ageing
- 20Gbps Switch fabric, non-blocking Switch architecture
- Up to 10K Bytes Jumbo frame support at all speed (10/100/1000 Mbps)

○ layer2-Switching

- Support port-based and 802.1q VLAN function, up to 64VLAN groups
- 802.1w Rapid-Spanning Tree protocol support
- Link Aggregation support static mode and LACP (802.3ad) - up to 4 Trunk groups, each trunk for up to maximum 8 ports
- IGMP Snooping - multicast filtering

○ Quality of Service

- 8 QoS classes per port
- Traffic class assignment based on 802.1p tag, or DSCP field
- Multicast and Broadcast Storm Control as well as Flooding Control

○ Security

- Port Mirroring support for dedicated port monitoring
- 802.1X port-Base access control, RADIUS Server Authentication
- Static MAC Address assign destination MAC address at specifies port

○ Management

- Remote Web management interface

- Firmware upgrade through web interface
- Cable Diagnostics technology
- Support SNMPv1 with RFC-1213/1573-Interface group, Ethernet MIB
- SNMP Trap

○ Power over Ethernet

- Complies with IEEE 802.3af / IEEE 802.3at Power over Ethernet End-Span PSE
- Up to 8 IEEE 802.af devices powered
- Up to 4 IEEE 802.at devices powered
- Support af PoE Power up to 15.4 Watts for each PoE ports
- Support at PoE power up to 30 Watts for each PoE ports
- Auto detect powered device (PD)
- Circuit protection prevent power interference between ports
- PoE Management

  * IEEE 802.3af and IEEE 802.3at mode switch control

  * PoE power usage threshold control

  * Total PoE usage threshold control

  * Per port PoE function enable/disable

  * PD classification detection

PRODUCT SPECIFICATION

Hardware Specification	
Copper ports	8-Port 10/100/1000 Base-T Auto MDI/MDI-X
SFP Slots	2-Port 100M/1000M/2.5G Base-SX/LX
Switch architecture	Store-and-Forward
Switch backbone	20Gbps
Switch throughput	14.8Mpps
MAC Address Table	8K entries
Data Buffer	512KB On-chip frame buffer
Flow Control	Back pressure for half duplex, IEEE 802.3x Pause Frame for full duplex
Dimension	61 x 110 x 157(W*D*H) Unit: mm
Power Requirement	54~56V DC
Power Consumption	10 Watts maximum
Reset Button	< 2sec : No Action

	< 10sec : Default Reset (keep ip address) > 10sec : Factory Reset (reset ip address to default ip)
Alarm Contact	1 relay output with current carrying capacity of 12~24VDC @ 1A
Digital Input	1 input with the same ground, but electrically isolated from the electronics. Max. input current: 10 mA
Layer 2 Functions	
Management Interface	Web Browser, SNMPv1, v2c, v3 monitor and SNMP Trap
Port configuration	- Port disable/enable. Auto-negotiation 10/100/1000Mbps full and half duplex mode selection - Flow Control disable / enable
VLAN	Port-Based / 802.1Q Tagged Based VLAN, Up to 255 VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE) MAC-based VLAN Protocol-based VLAN Voice VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN groups, out of 4096 VLAN ID

Link Aggregation	IEEE 802.3ad LACP / Static Trunk Supports 5 groups of 8-Port trunk support
QoS	4 Priority Queue and traffic classification based on 802.1p priority, DSCP field in IP packet
IGMP/MLD snooping	IGMP (v1/v2/v3) Snooping, up to 255 multicast Groups MLD (v1/v2) Snooping, up to 255 multicast Groups
Access Control List	IP-Based ACL / MAC-Based ACL Up to 123 entries
Bandwidth Control	Per port bandwidth control Ingress : 500Kb ~ 1000Mbps Egress: 500Kb ~ 1000Mbps
Port Mirror	One to Multi-port and the monitor mode is RX
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-1643 Ethernet MIB RFC-2863 Interface MIB RFC-2665 Ether-Like MIB

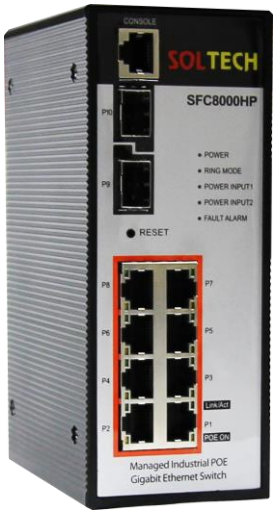
	RFC-2819 RMON MIB (Group 1,2,3,9) RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC-2933 IGMP-STD_MIB RFC3411 SNMP-Frameworks-MIB IEEE 802.1X PAE LLDP MAU_MIB
Carrier Ethernet	ERPS
Standards Conformance	
Network Standards	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX/100Base-FX Fast Ethernet IEEE 802.3z Gigabit Ethernet (SX/LX) IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1D Spanning tree protocol IEEE 802.1w Rapid Spanning Tree protocol IEEE 802.1s Multiple spanning tree protocol

	IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2
Operating Temperature	-40~80°C
Storage Temperature	-45~85°C
Operating Humidity	5% to 90%, relative humidity, non-condensing
Storage Humidity	5% to 95%, relative humidity, non-condensing
Power over Ethernet	
PoE Standard	IEEE 802.3af POE / PSE IEEE 802.3at POE / PSE

PoE Power Supply Type	End-Span
PoE Power output	Per port 52V DC, 600mA Max. 30 Watts
PoE Power Budget	250W
Max. number of Class 4 PD	8

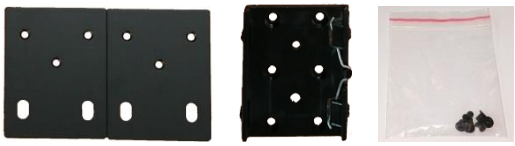
1.3 CONTENTS

- Managed Industrial Gigabit Ethernet Switch X 1
- User Manual CD X 1
- Wall Mount bracket, DIN-Rail Mount bracket, Screw



SFC8000HP

Manual CD



Wall Mount bracket, DIN-Rail Mount bracket, Screw

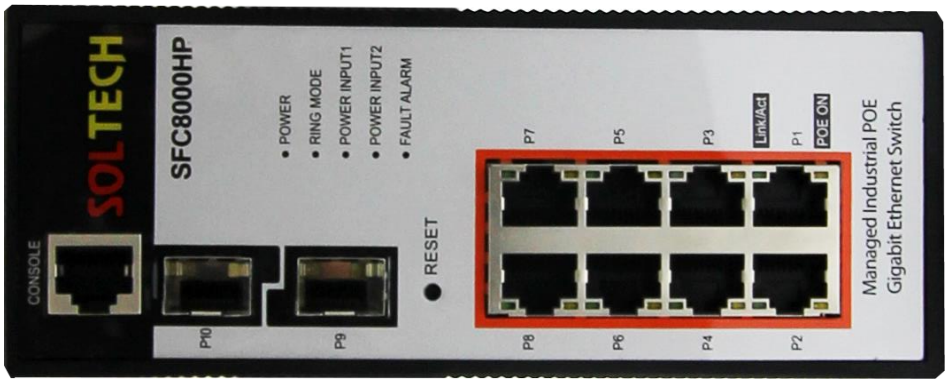
Note : Please re-package all of contents.

2 Exterior

2.1 SIZE

SFC8000HP's size is 61mm(W) X 110mm(D) X 157mm(H).

2.2 FRONT PANEL



There are 8pcs of RJ-45 10/100/1000Mbps ports, 2pcs of 100M/1000M/2.5GBase-SX/LX optical ports. CONSOLE port is for setting the device.

2.3 LED CONDITION

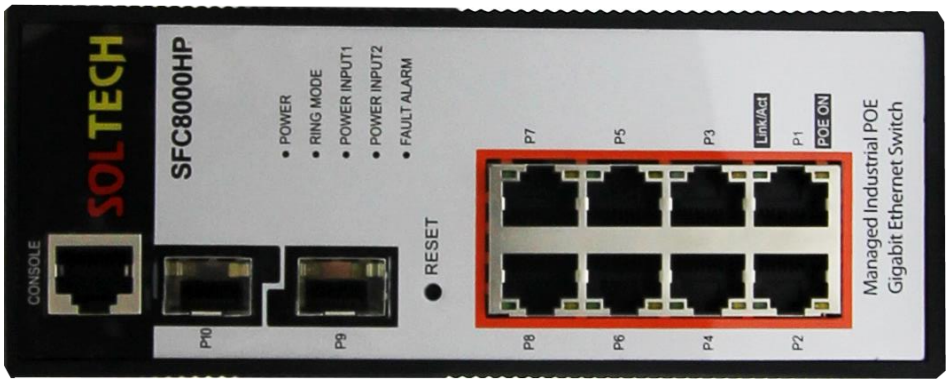
- **Front LED indicators of SFC8000HP**

LED	Color	Function
Power	**Green**	Switch powered
Power Input1	**Green**	Power input into Power Input1
Power Input2	**Green**	Power Input into Power Input2
P9	**Green** **YELLOW**	**Lights** : #9 Fiber port 1000M link on / **Blinks** : Data transmitting **Lights** : #9 Fiber port 100M link on / **Blinks** : Data transmitting
P10	**Green** **YELLOW**	**Lights** : #10 Fiber port 1000M link on / **Blinks** : Data transmitting **Lights** : #10 Fiber port 100M link on / **Blinks** : Data transmitting

- **RJ-45 LED indicators of SFC8000HP**

LED	Color	Function

P1, P2, P3, P4, P5, P6, P7, P8	**Green** **YELLOW**	**Lights** : 10/100/1000 link on / **Blinks** : Data transmitting **Lights** : PoE function on



SFC8000HP LED panel

Notice:

If you push a RESET button of Gigabit Ethernet Switch more than 2 seconds, all LEDs are flickering and every setting value(excluding IP address) will be initialized. If you push a RESET button of Gigabit Ethernet Switch more than 10 seconds, all LEDs are flickering fast and every setting value will be initialized.

2.4 CONNECT POWER INPUT

Bottom panel of Gigabit Ethernet Switch has two power inputs (Power1, Power2). They can accept 54~56 VDC power.

Bottom Panels of SFC8000HP

Power Notice:

1. The device needs power; it does not work until power is supplied. If your network has to work always, Please use an UPS(Uninterrupted Power Supply) to prevent data loss or stopping the device.

2. A surge suppressor can protect Gigabit Ethernet Switch or power adaptor from useless surge or electric current.

2.5 CONNECTING I/O PORT

Bottom panel of Gigabit Ethernet Switch has two I/O input(I/O IN1, I/O IN2) and I/O output(I/O OUT1, I/O OUT2).

Bottom Panels of SFC8000HP

Notice:

1. Please use only 12~24VDC for I/O input.
2. Please use only 12~24VDC for I/O output and less than 1A electric current. More than 1A electric current is prohibited to use.

3 Installation of bracket

Wall Mount bracket and DIN-Rail Mount bracket are enclosed as a basic contents of SFC8000HP. SFC8000HP can be installed on the wall or DIN-rail using these brackets. To install the bracket, please refer the pictures below.

Wall mount bracket

DIN-Rail mount bracket

4 Installation of product

This section explains how to install Gigabit Ethernet Switch and how to connect switch.

Please refer below process to finish installation of Gigabit Ethernet Switch.

4.1 INSTALLATION OF SFC8000HP

Step 1: Prepare 52~56VDC 10W power supply and SFC8000HP.

Step 2: Please keep some spaces between Gigabit Ethernet Switch and surrounding objects for ventilation.

Step 3: Connect the switch into network devices.

A. Please connect a network cable into 10/100/1000M RJ-45 port and SFP slot on front of switch.

B. Please connect a network cable(the other side of cable) into network devices like printer sever, work station or router.

Notice:

It needs more than UTP Category 5 standard network cable to connect into Gigabit Ethernet Switch.

Step 4: Power supply of switch

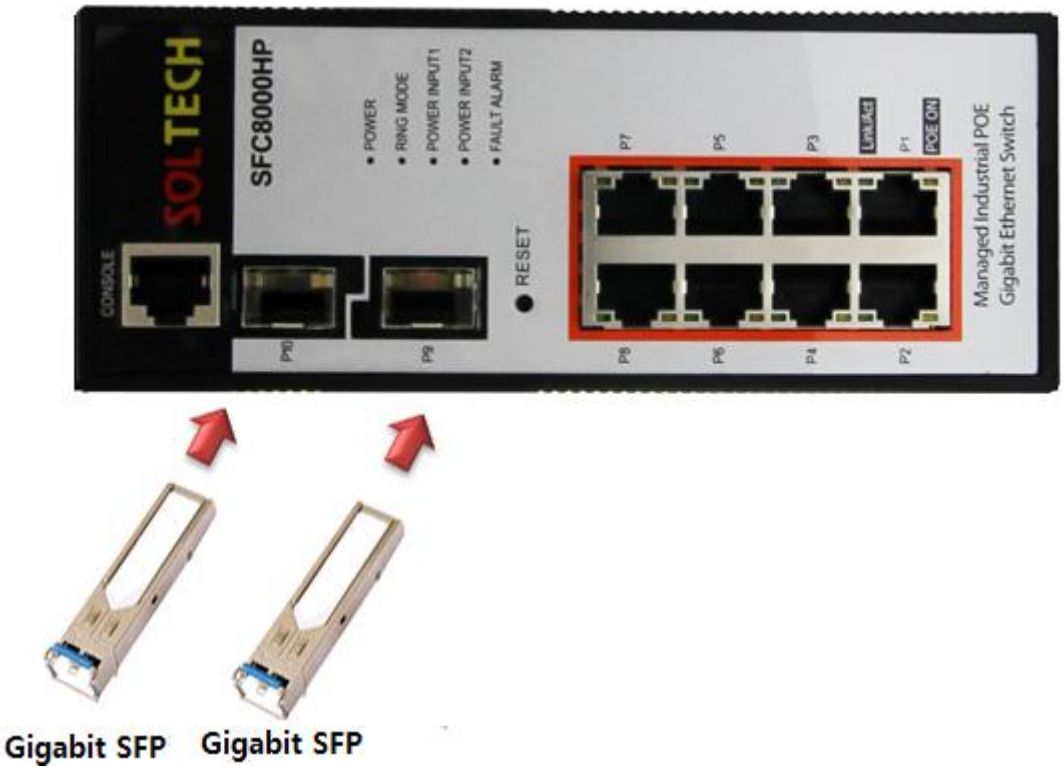
A. Please connect a power cable into the Gigabit Ethernet Switch.

B. Put a plug into the outlet.

LED(Green) of Gigabit Ethernet Switch is always turned on.

4.2 INSTALLATION OF SFP MODULE

Note: SFP transceiver is hot-pluggable and hot-swappable. Uses must turn off Gigabit Ethernet Switch when you plug in or plug out SFP modules.



Plug-in the SFP transceiver

Please check below before connecting other switch, work station or media converter.

1. Check the transmission part of SFP modules they are the same media type or not.
   For example: 1000BASE-SX to 1000BASE-SX and 1000BASE-LX to 1000BASE-LX.

2. Check fiber optic cable type and SFP modules. They have to be the same.

-> If you connect 1000BASE-SX SFP transmission, users have to use multi-mode fiber optic cable, duplex LC type.

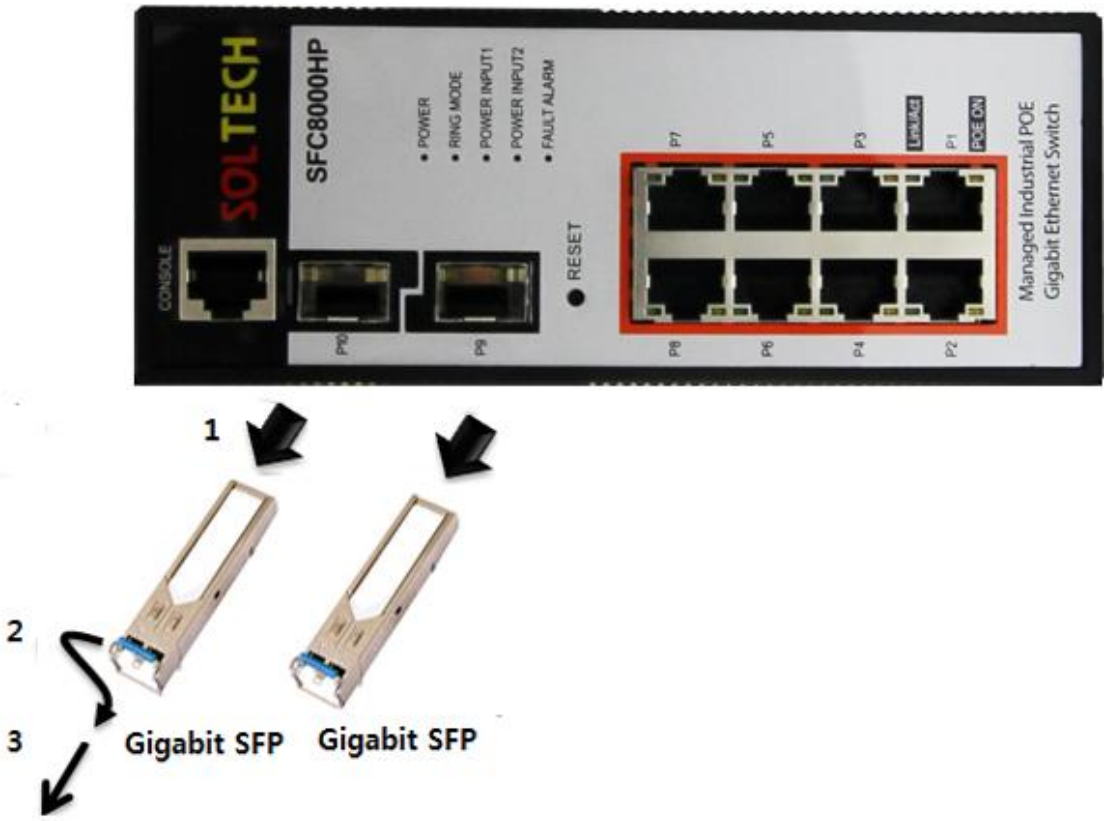
-> If you connect 1000BASE-LX SFP transmission, users have to use single-mode fiber optic cable, duplex LC type.

4.3 CONNECTING OPTICAL CABLE

1. Connect a duplex LC network cable into SFP transceiver.
2. Connect a cable(the other side of cable) into a fiber NIC of work station or media converter which has SFP slots.
3. Check the LED LNK/ACT of SFP slot and SFP transceiver.
4. If the link is failed, please check the connecting type of SFP slot. It needs "1000 Force" link mode, it works some fiber NIC or media converters.

4.4 REMOVING TRANSCEIVER MODULE

1. Check any networking activity with networking administrator. Or disband the port using management interface in advance.
2. Remove the cable smoothly.
3. Hold a handle of SFP transceiver.
4. Pull out the SFP transceiver smoothly.



Pull out the SFP transceiver

Notice:

Please do not pull out the SFP transceiver wildly. It can damage the Gigabit Ethernet Switch or SFP slot.

5 Web management system

5.1 WEB LOGIN

WEB management of SFC8000HP sets as follow.

1. Users must know IP Address of SFC8000HP to WEB set.

2. Connect AP (LAN interface) with PC (LAN port) using enclosed LAN cable.

3. Access WEB using IP address of AP.

4. Default value of IP/ID is as follow.

IP Address : 192.168.10.100

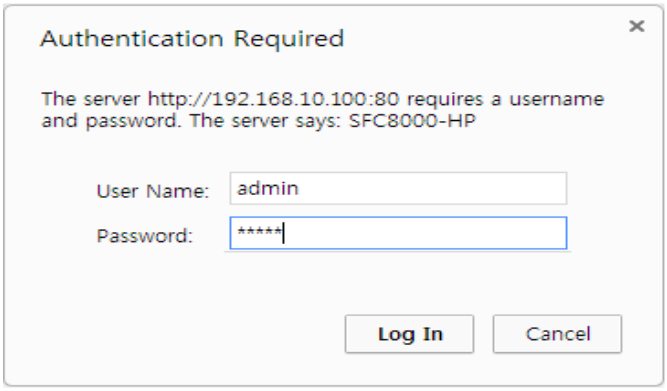
Subnet Mask: 255.255.255.0

Gateway : no default value

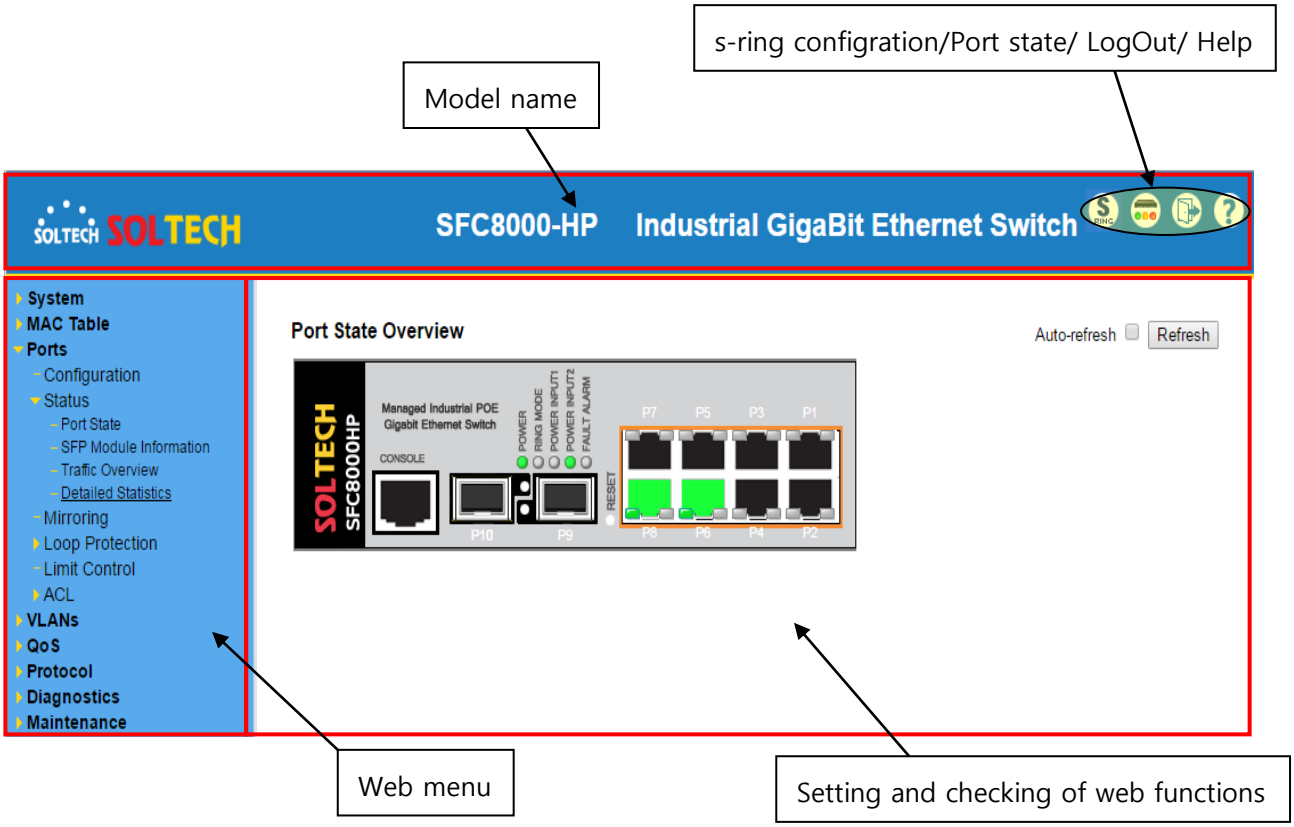
Login ID : admin

Login Password : admin

<Chrome authentication screen >



5.2 WEB SCREEN CONFIGURATION



[Panel Display]

Shows port image of switch which is controlled by web. It can be set to indicate information of port including mode, uplink and down link. Click image of port to open port statistics.

State	Disabled	Down	Link(100M)	Link(1G)	Link(2.5G)	PoE(100M)	PoE(1G)
RJ-45 Ports							
SFP Ports							

••••••Check functions of web menu••••••

■ **System**	This section provides configuration of System information.
■ **MAC Table**	This section provides configuration of MAC information.
■ **Ports**	This section provides configuration of Port information.
■ **VLANs**	This section provides configuration of VLAN information.
■ **QoS**	This section provides configuration of QoS information.
■ **Protocol**	This section provides configuration of Protocol information.
■ **Diagnostics**	This section provides configuration of Diagnostics information.
■ **Maintenance**	This section provides configuration of Maintenance information.

5.3 SYSTEM

This section provides system menu about indication and configuration of management details of switch.

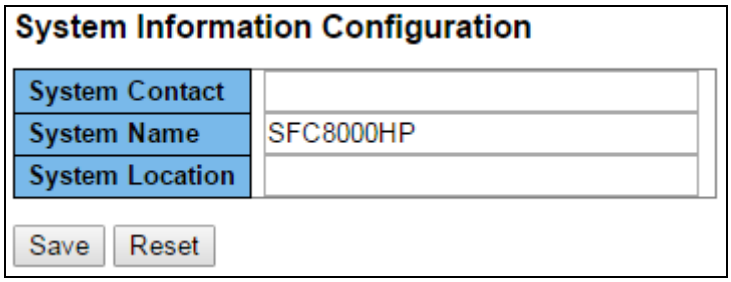
■ **Information**	Checking and configuration of switch information.
■ **IP**	Configure IP basic settings, control IP interfaces and IP routes.
■ **Time**	System Time : User can designate System Time arbitrary. Time Zone Daylight Saving : Change switch's time by its location. NTP : Change switch's time

■ **Syslog**	Setting and checking log message.
■ **Security**	Setting and checking security of switch.
■ **Green Ethernet**	Setting and checking LED brightness or power saving.
■ **PoE**	Checking PoE information, PoE working and PoE schedule.
■ **Digital I/O**	Setting and checking Digital I/O.

5.3.1 INFORMATION

5.3.1.1 Information Configuration

Configuration of switch information.



Object	Description
● **System Contact**	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
● **System Name**	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space

	characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
• **System Location**	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.1.2 Information status

The switch system information is provided here.

System Information

System	
Contact	
Name	SFC8000HP
Location	
Hardware	
MAC Address	00-12-6d-12-34-56
Time	
System Date	2016-05-18T09:50:16+09:00
System Uptime	0d 00:04:53
Software	
Software Version	SFC8000HP 1.0.1.5
Software Date	2016-05-18T07:58:12+09:00
System Temperature	
Current	38.625 'C (101.525 'F)
Minimum	38.375 'C (101.075 'F)
Maximum	38.750 'C (101.750 'F)
Average	38.625 'C (101.525 'F)

	Object	Description
•	**Contact**	The system contact configured in Configuration | System | Information | System Contact.
•	**Name**	The system name configured in Configuration | System | Information | System Name.
•	**Location**	The system location configured in Configuration | System | Information | System Location.
•	**MAC Address**	The MAC Address of this switch.
•	**System Data**	The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
•	**System Uptime**	The period of time the device has been operational.
•	**Software Version**	The software version of this switch.
•	**Software Data**	The date when the switch software was produced.
•	**The Internal templature**	Shows the intenal templature of switch.
•	**Current**	Shows the current intenal templature of switch.
•	**Minimum**	Shows the minimum intenal templature of switch.
•	**Maximum**	Shows the maximum intenal templature of switch.
•	**Average**	Shows the average intenal templature of switch.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

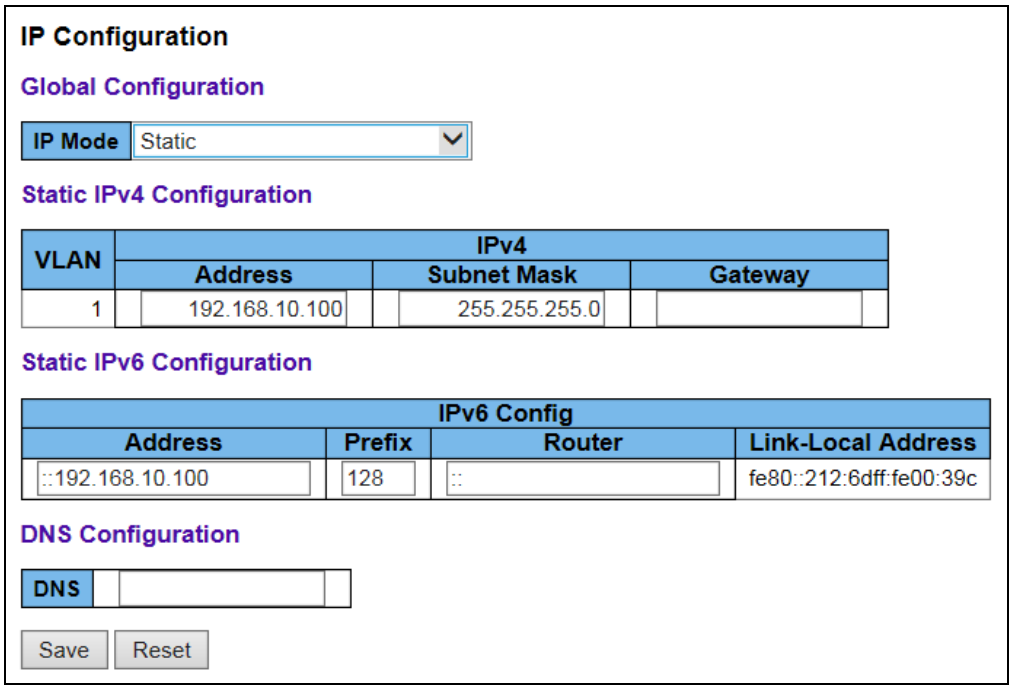
Refresh: Click to refresh the page.

5.3.2 IP CONFIGURATION

Can set IP address. Users can choose between dynamic IP address and static IP address.

5.3.2.1 IP Configuration

Can set IP address, Subnet Mask, Gateway, DNS.



	Object	Description
•	**Mode**	Set IP Static, DHCP.
•	**Address**	Set IPv4 address. (Default = 192.168.10.100)
•	**SubnetMask**	Set Subnet Mask. (Default = 255.255.255.0)
•	**Gateway**	Set Gateway address.
•	**Address**	Set IPv6 address. (Default = ::192.168.10.100)
•	**Prefix**	Set prefix value of IPv6 (Default = 128)

• **Router**	Set IP which is connected router to IPv6.
• **Link-Local Adress**	Show connected link-local address value.
• **DNS**	Set DNS.

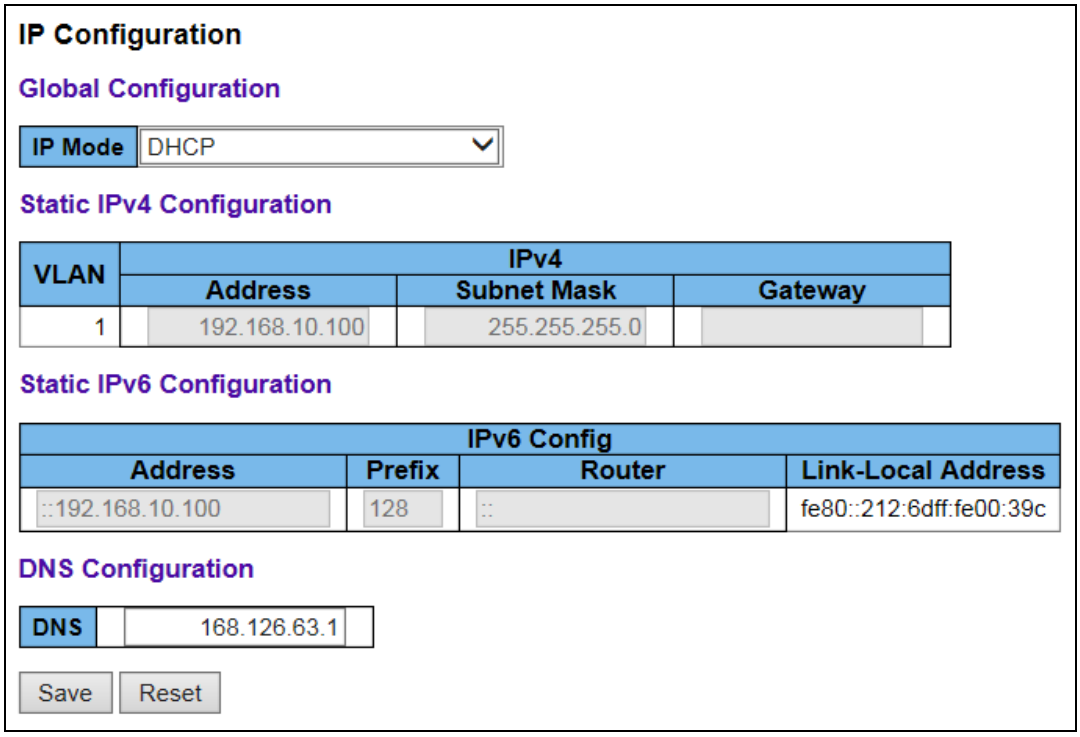
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.2.2 DHCP Configuration

Gain IP address from DHCP sever.



Object	Description
• **Mode**	Set IP Static, DHCP.
• **DNS**	Set DNS.

Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

5.3.2.3 IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbor cache (ARP cache) status.

IP Interfaces Auto-refresh [Refresh]

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
OS:lo	IPv6	fe80::1/64	
VLAN1	LINK	00-12-6d-12-34-56	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.10.36/24	
VLAN1	IPv6	fe80::212:6dff:fe12:3456/64	
VLAN1	IPv6	::192.168.10.36/128	

IP Routes

Network	Gateway	Status
0.0.0.0/0	VLAN1:192.168.10.1	<UP GATEWAY HW_RT>
127.0.0.1/32	OS:lo:127.0.0.1	<UP HOST>
192.168.10.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	OS:lo:127.0.0.1	<UP>
::1/128	OS:lo:::1	<UP HOST>
::192.168.10.36/128	OS:lo:12:6d12:3456::	<UP HOST>
fe80::1/128	OS:lo:fe80::1::1	<UP>
fe80::1::1/128	OS:lo	<UP HOST>
fe80::2::/128	VLAN1	<UP>
fe80::2::212:6dff:fe12:3456/128	OS:lo:12:6d12:3456::	<UP HOST>
ff01::1::/128	OS:lo:::1	<UP>
ff01::2::/128	VLAN1	<UP>
ff02::1::/128	OS:lo:::1	<UP>
ff02::2::/128	VLAN1	<UP>

ARP Table (Neighbour cache)

IP Address	Link Address
192.168.10.1	VLAN1:64-e5-99-68-29-dc
192.168.10.8	VLAN1:08-9e-01-d3-b7-32
192.168.10.9	VLAN1:08-9e-01-97-92-bb
::192.168.10.36	VLAN1:00-12-6d-12-34-56
fe80::212:6dff:fe12:3456	VLAN1:00-12-6d-12-34-56

Object	Description
• **Interface**	The name of the interface.
• **Type**	The address type of the entry. This may be **LINK** or **IPv4**.
• **Address**	The current address of the interface (of the given type).
• **Status**	The status flags of the interface (and/or address).
• **Network**	The destination IP network or host address of this route.
• **Gateway**	The gateway address of this route.
• **Status**	The status flags of the route.
• **IP Address**	The IP address of the entry.
• **Link Address**	The Link (MAC) address for which a binding to the IP address given exist..

Buttons

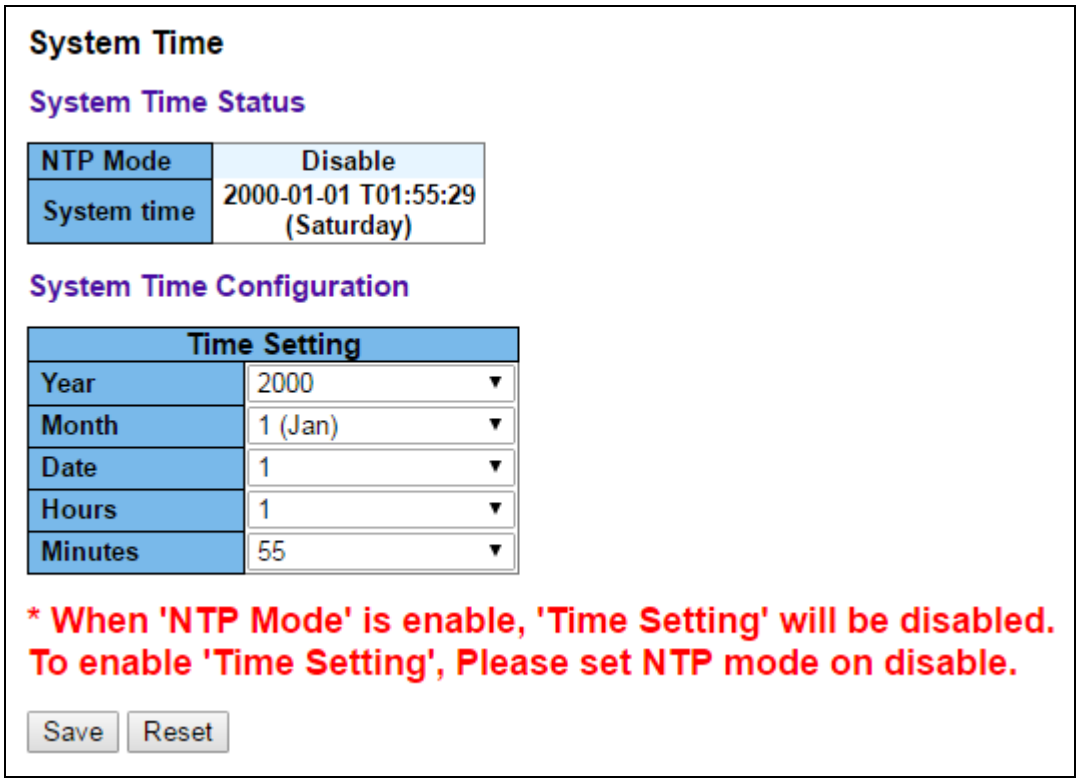
Auto-refresh : Click to refresh the page immediately.

Refresh: Check this box to refresh the page automatically. Automatic refresh occurs every seconds.

5.3.3 TIME

5.3.3.1 System Time

System Time setting for the device.



	Object	Description
•	**NTP Mode**	Indicate using NTP or not.
•	**System time**	Indicate Systime Time
•	**Year**	Setting year of System Time
•	**Month**	Setting month of System Time
•	**Date**	Setting date of System Time
•	**Hours**	Setting hour of System Time
•	**Minutes**	Setting minute of System Time

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

NTP: Click to move to NTP

Refresh: Click to refresh

5.3.3.2 NTP

Configure NTP on this page.

NTP Configuration

Mode	Disabled
Server 1	time.kriss.re.kr
Server 2	ntp.postech.ac.kr
Server 3	time.bora.net
Server 4	
Server 5	

Save Reset

Object	Description
• **Mode**	Indicates the NTP mode operation. Possible modes are: **Enabled**: Enable NTP client mode operation. **Disabled**: Disable NTP clinet mode operation.
• **Server**	Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

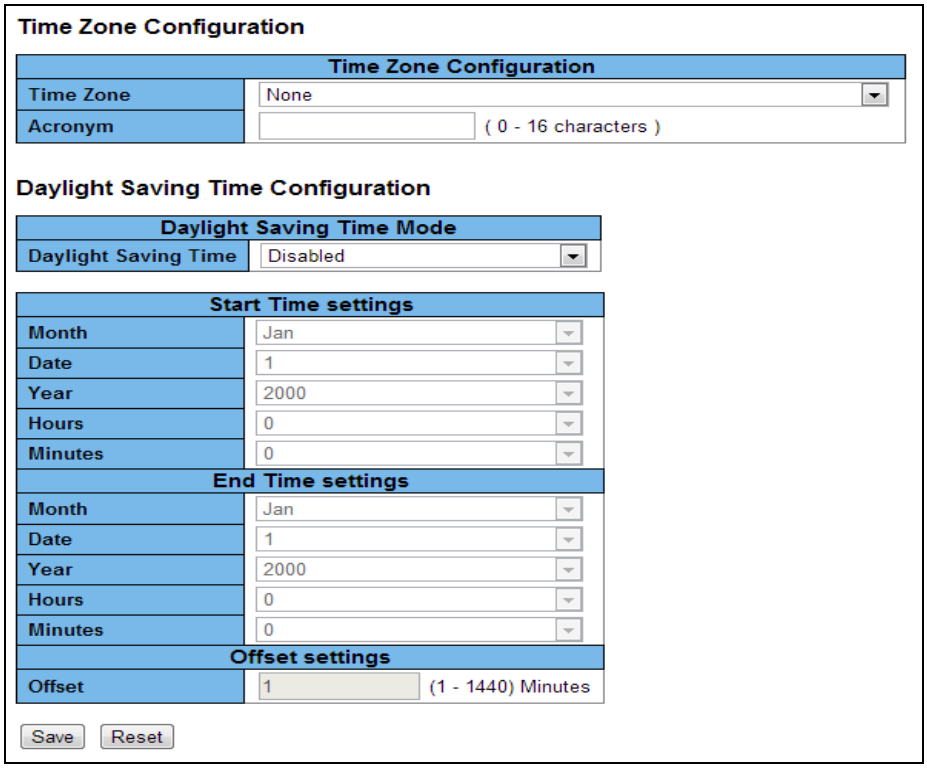
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.3.3 Time Zone Configuration

This page allows you to configure the Time Zone.



Object	Description
• **Time zone**	Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.
• **Acronym**	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 alpha-numeric characters and can contain '-', '_'

	or '.')
• **Daylight Saving Time**	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)
• **Week**	Select the starting week number.
• **Day**	Select the starting day.
• **Month**	Select the starting month.
• **Hours**	Select the starting hour.
• **Minutes**	Select the starting minute.
• **Offset**	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Buttons

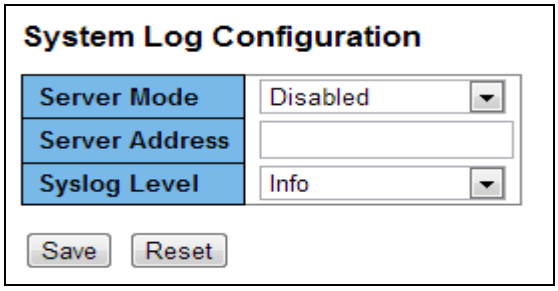
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.4 SYSLOG

5.3.3.4.1 Syslog Configuration

Configure System Log on this page.



Object	Description
• **Server Mode**	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: **Enabled**: Enable server mode operation. **Disabled**: Disable server mode operation.
• **Server Adress**	Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.
• **Syslog Level**	Indicates what kind of message will send to syslog server. Possible modes are: **Info**: Send informations, warnings and errors. **Warning**: Send warnings and errors. **Error**: Send errors.

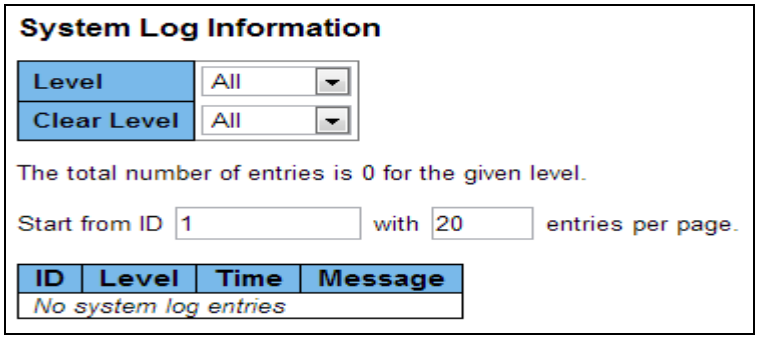
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.3.4.2 Syslog Status

The switch system log information is provided here.



Object	Description
• **ID**	The ID (>= 1) of the system log entry.
• **Level**	The level of the system log entry. The following level types are supported: **Info**: Information level of the system log. **Warning**: Warning level of the system log. **Error**: Error level of the system log. **All**: All levels.
• **Time**	The time of the system log entry.
• **Message**	The message of the system log entry.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Updates the system log entries, starting from the current entry ID.

Clear: Flushes the selected log entries.

|<<: Updates the system log entries, starting from the first available entry ID.

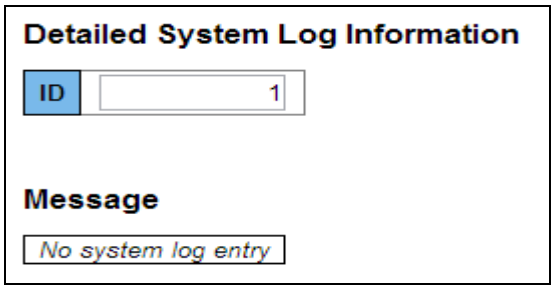
<<: Updates the system log entries, ending at the last entry currently displayed.

[>>]: Updates the system log entries, starting from the last entry currently displayed

[>>|]: Updates the system log entries, ending at the last available entry ID.

5.3.3.4.3 Detailed Log

The switch system detailed log information is provided here.



Object	Description
• **ID**	The ID (>= 1) of the system log entry.
• **Message**	The detailed message of the system log entry.

Buttons

[Refresh]: Updates the system log entry to the current entry ID.

[|<<]: Updates the system log entry to the first available entry ID.

[<<]: Updates the system log entry to the previous available entry ID.

[>>]: Updates the system log entry to the next available entry ID.

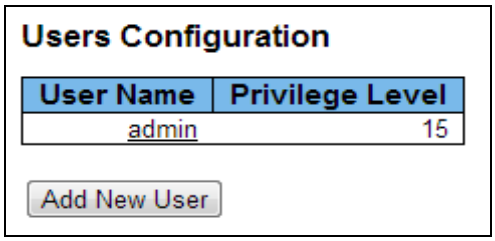
[>>|]: Updates the system log entry to the last available entry ID.

5.3.5 SECURITY

5.3.5.1 Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.

The displayed values for each user are:



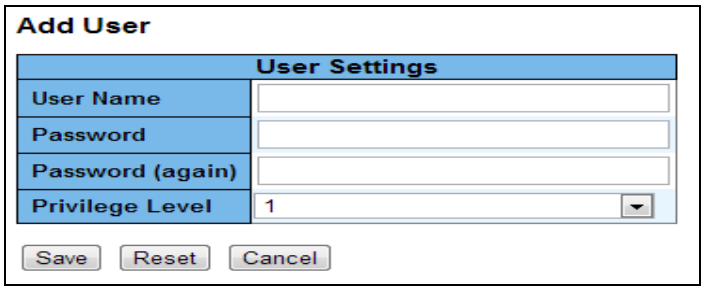
Object	Description
• User Name	The name identifying the user. This is also a link to Add/Edit User.
• Privilege Level	The privilege level of the user. The allowed range is **1** to **15**. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account

Buttons

Add New User: Click to add a new user.

When put the Add New User buttons, User setting page will be appeared.

This page configures a user.



Object	Description
• **User Name**	A string identifying the user name that this entry should belong to. The allowed string length is **1** to **31**. The valid user name is a combination of letters, numbers and underscores.
• **Password**	The password of the user. The allowed string length is **0** to **31**.
• **Privelege Level**	The privilege level of the user. The allowed range is **1** to **15**. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to undo any changes made locally and return to the Users.

5.3.5.2 Privilege Levels

This page provides an overview of the privilege levels.

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
DDM	5	10	5	10
Debug	15	15	15	15
Dhcp_Client	5	10	5	10
Diagnostics	5	10	5	10
EEE	5	10	5	10
Green_Ethernet	5	10	5	10
IP2		10	5	10
		10	5	10
	5		5	
	5			
Spanning_Tree	5	10		10
System	5	10	1	10
Timer	5	10	5	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
sFlow	5	10	5	10

Save Reset

Object	Description
• **Group Name**	The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details: System: Contact, Name, Location, Timezone, Daylight Saving Time, Log. Security: Authentication, System Access Management, Port

	(contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard. IP: Everything except 'ping'. Port: Everything except 'VeriPHY'. Diagnostics: 'ping' and 'VeriPHY'. Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.
• **Privilege Levels**	Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

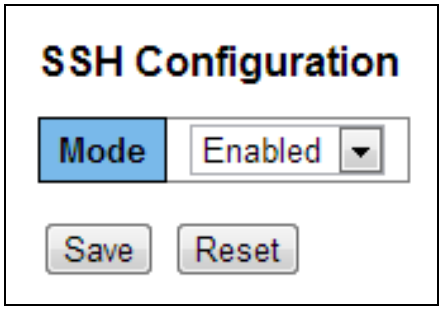
Buttons

Save: Click to save changes..

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.5.3 SSH

Secure Shell (SSH) is a cryptographic network protocol for secure data communication. Its encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet.



	Object	Description
•	**Mode**	Indicates the SSH mode operation. Possible modes are: **Enabled**: Enable SSH mode operation. **Disabled**: Disable SSH mode operation.

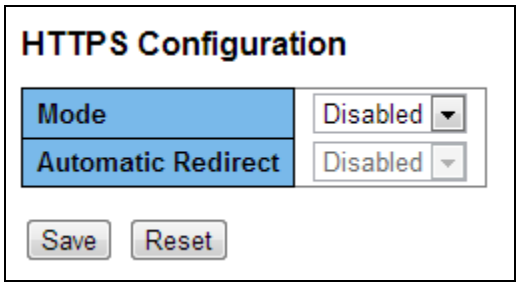
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.5.4 HTTPS

HTTPS provides cryptographic network communication. It uses for world wide web which needs strong security like payment or log on (in business).



Object	Description

• **Mode**	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: **Enabled**: Enable HTTPS mode operation. **Disabled**: Disable HTTPS mode operation.
• **Automatic Redirect**	Indicates the HTTPS redirect mode operation. It only significant if HTTPS mode "Enabled" is selected. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are: **Enabled**: Enable HTTPS redirect mode operation. **Disabled**: Disable HTTPS redirect mode operation.

Buttons

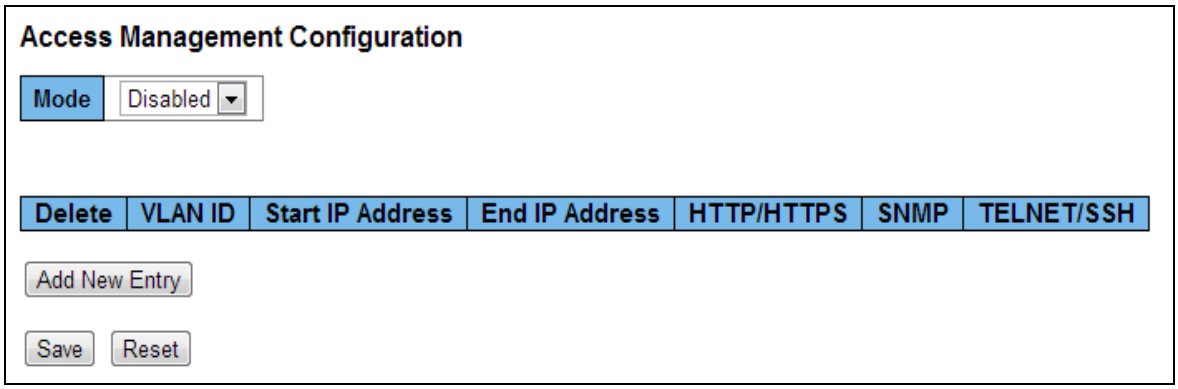
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.5.5 Access Management

■ 5.4.5.5.1 Configuration

Configure access management table on this page. The maximum number of entries is **16**. If the application's type matches any one of the access management entries, it will allow access to the switch.



Object	Description
• **Mode**	Indicates the access management mode operation. Possible modes are: **Enabled**: Enable access management mode operation. **Disabled**: Disable access management mode operation.
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **VLAN ID**	Indicates the VLAN ID for the access management entry.
• **Start IP Address**	Indicates the start IP address for the access management entry.
• **End IP Address**	Indicates the end IP address for the access management entry.
• **HTTP/HTTPS**	Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
• **SNMP**	Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
• **TELNET/SSH**	Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons

Add New Entry: Click to add a new access management entry.

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

■ 5.4.5.5.2 Status

This page provides statistics for access management.

Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Object	Description
• **Interface**	The interface type through which the remote host can access the switch.
• **Received Packts**	Number of received packets from the interface when access management mode is enabled.
• **Allowed Packets**	Number of allowed packets from the interface when access management mode is enabled.
• **Discarded Packets**	Number of discarded packets from the interface when access management mode is enabled.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

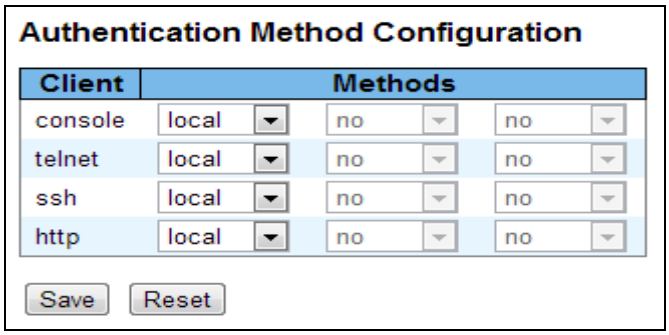
[Refresh]: Click to refresh the page immediately.

[Clear]: Clear all statistics.

5.3.5.6 Auth Method

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.

The table has one row for each client type and a number of columns, which are:



Object	Description
• **Client**	The management client for which the configuration below applies.
• **Methods**	Method can be set to one of the following values: •no: Authentication is disabled and login is not possible. •local: Use the local user database on the switch for authentication. •radius: Use remote RADIUS server(s) for authentication. •tacacs+: Use remote TACACS+ server(s) for authentication. Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

Buttons

Save: Click to save changes.

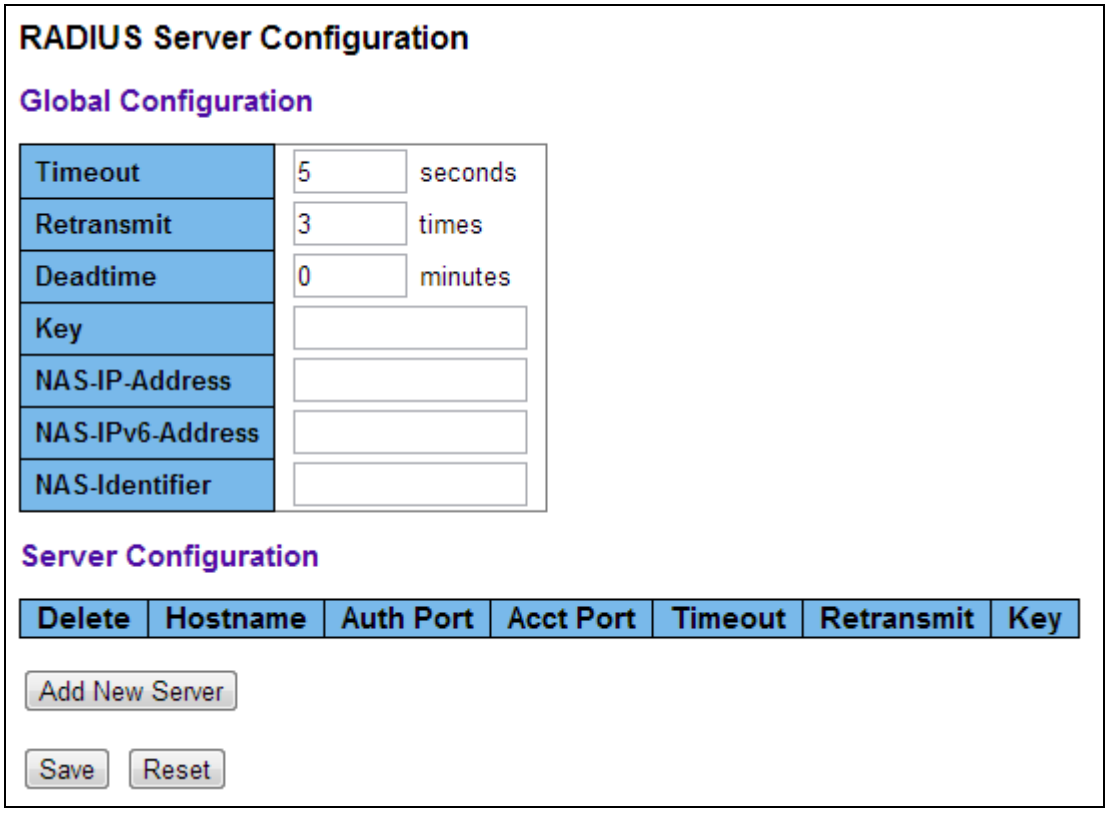
Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.5.7 AAA

5.3.5.7.1 RADIUS

5.3.5.7.1.1 Configuration

This page allows you to configure the RADIUS servers.



Object	Description
• **Timeout**	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
• **Retransmit**	Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
• **Deadtime**	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server

	has been configured.
• **Key**	The secret key - up to 63 characters long - shared between the RADIUS server and the switch.
• **NAS-IP-Address**	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
• **NAS-IPv6-Address**	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
• **NAS-Identifier**	The identifier - up to 255 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.
• **Delete**	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
• **Hostname**	The IP address or hostname of the RADIUS server.
• **Auth Port**	The UDP port to use on the RADIUS server for authentication.
• **Acct Port**	The UDP port to use on the RADIUS server for accounting.
• **Timeout**	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
• **Retransmit**	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
• **key**	This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

[Add New Server]: Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

[Delete]: can be used to undo the addition of the new server.

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values..

5.3.5.7.1.2 Status

5.3.5.7.1.2.1 RADIUS OVERVIEW

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

Object	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	The current status of the server. This field takes one of

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

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds

Refresh: Click to refresh the page immediately.

- **5.3.5.7.1.2.2 RADIUS DETATILS**

This page provides detailed statistics for a particular RADIUS server.

RADIUS Authentication Statistics for Server #1

Server #1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:0
State			Disabled
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:0
State			Disabled
Round-Trip Time			0 ms

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Use the server select box to switch between the backend servers to show details for.

Object	Description
• **AccessAccepts**	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
• **AccessRejects**	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
• **AccessChallenges**	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
• **MalformedAccess Responses**	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
• **BadAuthenticators**	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
• **UnknownTypes**	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

• **PacketsDropped**	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason..
• **AccessRequests**	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
• **AccessRetransmissions**	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
• **PendingRequests**	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
• **Timeouts**	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
• **IP Address**	IP address and UDP port for the authentication server in question.
• **State**	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in

	parentheses. This state is only reachable when more than one server is enabled.
• **Round-Trip Time**	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Object	Description
• **Responses**	The number of RADIUS packets (valid or invalid) received from the server.
• **MalformedResponses**	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
• **BadAuthenticators**	The number of RADIUS packets containing invalid authenticators received from the server.
• **UnknownTypes**	The number of RADIUS packets of unknown types that were received from the server on the accounting port..
• **PacketsDropped**	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
• **Requests**	The number of RADIUS packets sent to the server. This does not include retransmissions.
• **Retransmissions**	The number of RADIUS packets retransmitted to the RADIUS accounting server.
• **PendingRequests**	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This

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

Buttons

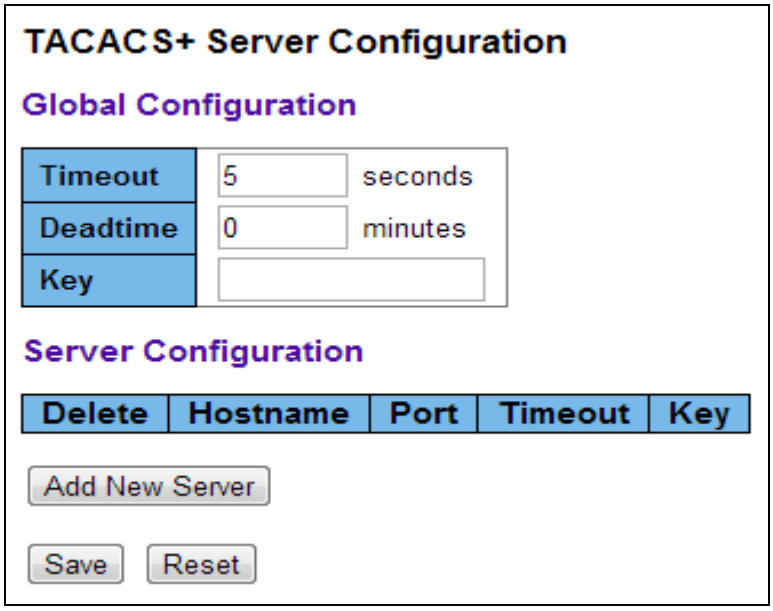
Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

■ 5.3.5.7.2 TACACS+

This page allows you to configure the TACACS+ servers..
These setting are common for all of the TACACS+ servers.



Object	Description
• **Timeout**	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

• **Deadtime**	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
• **Key**	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch..
• **Delete**	To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.
• **Hostname**	The IP address or hostname of the TACACS+ server.
• **Port**	The TCP port to use on the TACACS+ server for authentication.
• **Timeout**	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
• **key**	This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

[Add New Server]: Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

[Delete]: can be used to undo the addition of the new server.

[Save]: Click to save changes

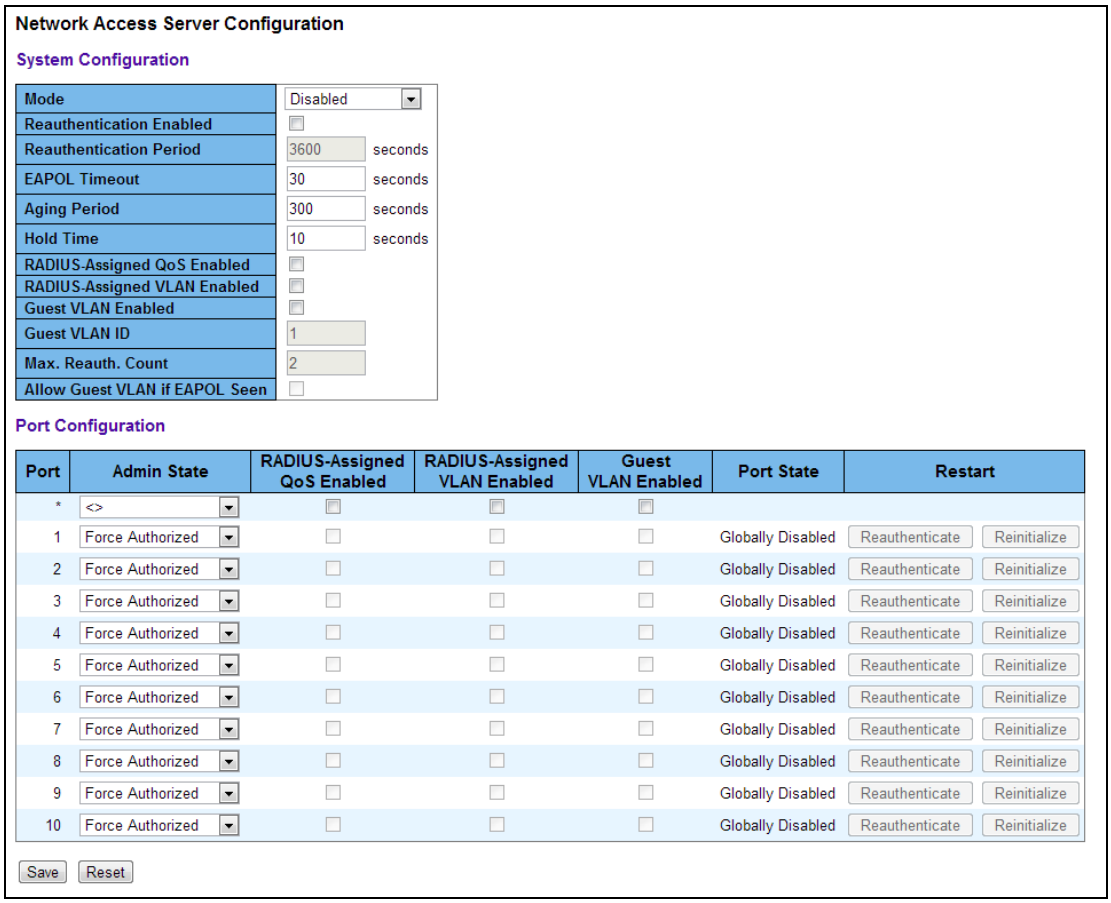
[Reset]: Click to undo any changes made locally and revert to previously saved values.

5.3.5.8 NAS

■ 5.3.5.8.1 Configuration

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The NAS configuration consists of two sections, a system- and a port-wide.



Object	Description
● **Mode**	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

• **Reauthentication Enabled**	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).
• **Reauthentication Period**	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
• **EAPOL Timeout**	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.
• **Aging Period**	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • Single 802.1X • Multi 802.1X • MAC-Based Auth. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will

	get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
• **Hold Time**	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • Single 802.1X • Multi 802.1X • MAC-Based Auth. If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
• **RADIUS-Assigned QoS Enabled**	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server

	assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.
• **RADIUS-Assigned VLAN Enabled**	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.
• **Guest VLAN Enabled**	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.
• **Guest VLAN ID**	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].

• **Max. Reauth. Count**	The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].
• **Allow Guest VLAN if EAPOL Seen**	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.
• **Port**	The port number for which the configuration below applies.
• **Admin State**	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:
• **RADIUS-Assigned QoS Enabled**	When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class

	(which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.
• **RADIUS-Assigned VLAN Enabled**	When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e.
• **Guest VLAN Enabled**	When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.
• **Port State**	The current state of the port. It can undertake one of the following values: Globally Disabled: NAS is globally disabled. Link Down: NAS is globally enabled, but there is no link on the port. Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. Unauthorized: The port is in Force Unauthorized or a

	single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
• **Restart**	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized. Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons

Save: Click to refresh the page.

Reset: Click to save changes.

Cancel: Click to undo any changes made locally and revert to previously saved values.

5.3.5.8.2 Status

5.3.5.8.2.1 Switch

This page provides an overview of the current NAS port states.

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				

Object	Description
• **Port**	The switch port number. Click to navigate to detailed NAS statistics for this port.
• **Admin State**	The switch port number. Click to navigate to detailed NAS statistics for this port.
• **Port State**	The current state of the port. Refer to NAS Port State for a description of the individual states.
• **Last Source**	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
• **Last ID**	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

• **QoS Class**	QoS Class assigned to the port by the RADIUS server if enabled.
• **Port VLAN ID**	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

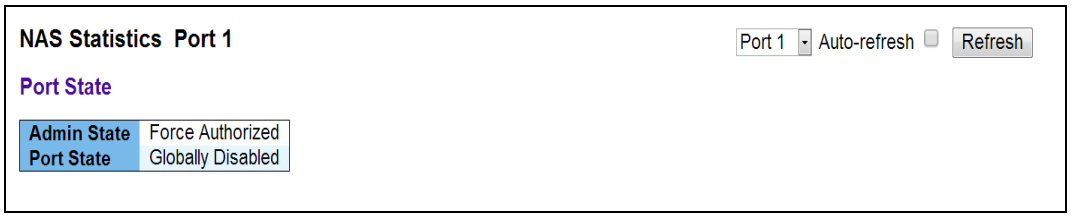
Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

• 5.3.5.8.2.1 Port

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only.

Use the port select box to select which port details to be displayed.



Object	Description

• **Admin State**	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
• **Port State**	The current state of the port. Refer to NAS Port State for a description of the individual states.
• **QoS Class**	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
• **Port VLAN ID**	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

5.3.5.9 Port Security

■ 5.4.5.9.1 Switch

This page shows the Port Security status. Port Security is a module with no direct configuration.

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-
9	----	Disabled	-	-
10	----	Disabled	-	-

Object	Description
• User Module Name	The full name of a module that may request Port Security services.
• ABBR	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.
• Port	The port number for which the status applies. Click the port number to see the status for this particular port.
• Users	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
• State	Shows the current state of the port. It can take one of four values: **Disabled**: No user modules are currently using the Port Security service. **Ready**: The Port Security service is in use by at least one

	user module, and is awaiting frames from unknown MAC addresses to arrive. **Limit Reached**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. **Shutdown**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.
• **Mac Count**	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

■ 5.3.5.9.2 Port

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration.

Object	Description
• **MAC Address & VLAN ID**	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
• **State**	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
• **Time of Addition**	Shows the date and time when this MAC address was first seen on the port.
• **Age/Hold**	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

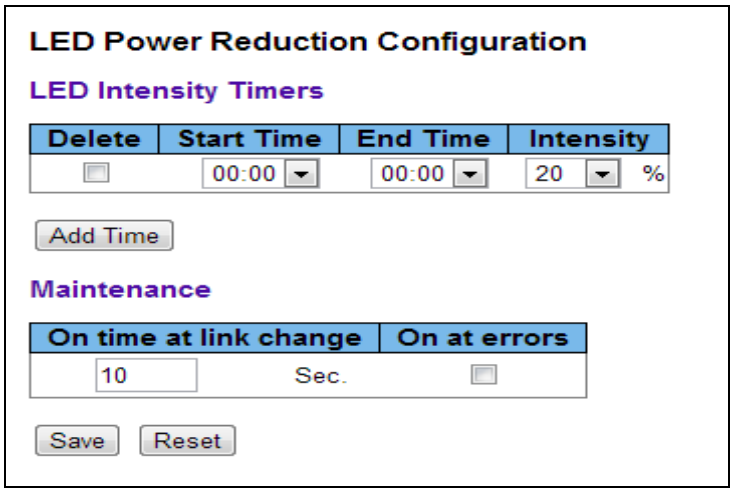
Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds

Refresh: Click to refresh the page immediately.

5.3.6. GREEN ETHERNET

5.3.6.1 LED

Can set the LED brightness and time the used.



Object	Description
• **Start Time**	The time at which the LEDs intensity shall be set to the corrsponding intensity.
• **End Time**	The time at which the LEDs intensity shall be set to a new intensity. If no intensity is specified for the next hour, the intensity is set to default intensity.
• **Intensity**	The LEDs intensity (100% = Full power, 0% = LED off).
• **Maintenance Time**	When a network administrator does maintenance of the switch (e.g. adding or moving users) he might want to have full LED intensity during the maintenance period . Therefore it is possible to specify that the LEDs shall use full intensity a specific period of time. Maintenance Time is the number of seconds that the LEDs will have full intensity after either a port has changed link state, or the LED pushbutton has been pushed.

Buttons

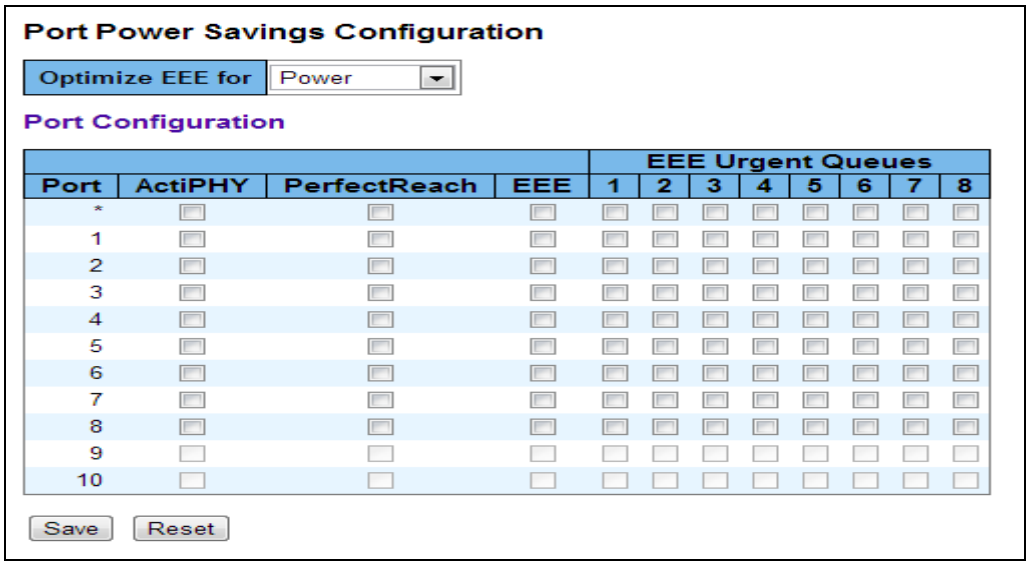
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.6.2 Port Power Savings

5.3.5.10.2.1 Configuration

This page allows the user to configure the port power savings features.



Object	Description
• Port	The switch port number of the logical port.
• ActiPHY	Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.

• **PerfectReach**	Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.
• **EEE**	Controls whether EEE is enabled for this switch port. For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency. If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.
• **EEE Urgent Queues**	Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.3.5.10.2.2 Status

This page provides the current status for EEE.

Port Power Savings Status

Port	Link	EEE	LP EEE Cap	EEE Savings	ActiPhy Savings	PerfectReach Savings
1		X	X	X	X	X
2		X	X	X	X	X
3		X	X	X	X	X
4		X	X	X	X	X
5		X	X	X	X	X
6		X	X	X	X	X
7		X	X	X	X	X
8		X	X	X	X	X
9		X	X	X	X	X
10		X	X	X	X	X

Object	Description
• **Port**	This is the logical port number for this row.
• **Link**	Shows if the link is up for the port (green = link up, red = link down).
• **EEE**	Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).
• **LP EEE Cap**	Shows if the link partner is EEE capable.
• **EEE Savings**	Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.
• **ActiPhy Savings**	Shows if the system is currently saving power due to ActiPhy.
• **PerfectReach Savings**	Shows if the system is currently saving power due to PerfectReach.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

5.3.7 POE

5.3.7.1 Configuration

This page configures POE group.

PoE Configuration Refresh

Global Configuration

PoE Mode	Enable

Port Configuration

Port	PoE Schedule Mode	PoE Type and Power Limit			
		Conf	Stat	Power Limit	Consume Power
1	Disable	802.3at	Disable	31.00	0.00
2	Disable	802.3at	Disable	31.00	0.00
3	Disable	802.3at	Disable	31.00	0.00
4	Disable	802.3at	Disable	31.00	0.00
5	Disable	802.3at	Disable	31.00	0.00
6	Disable	802.3at	Disable	31.00	0.00
7	Disable	802.3at	Disable	31.00	0.00
8	Disable	802.3at	Disable	31.00	0.00
Total	-------	-------	-------	248.00	0.00

The maximum power limitation of the system is The maximum poe power will vary depending on power supply's capacity W.

Save Reset

Object	Description
• **POE Mode**	Setting of POE.
• **Port**	A port which uses POE.
• **PoE Schedule Mode**	Indicate using PoE schdule or not
• **Conf**	Set a limitation method of POE equipment. Disable : Do not use POE. 802.3af : Supported only 802.3af(15W limit). 802.3at : Supported only 802.3at(31W limit). Manual : Users can assign limited watt value between 5W and 31W. Auto : Supported both 802.3af and 802.3at.

	In cace of 802.3af: Supproted until 15W per a port. In cace of 802.3at: Supproted until 31W per a port. But, if the whole output is more than 124W, output of some ports can be limitted automatically.
• **Stat**	Indicate connecting condition of POE equipment. Disable : Not conntected. Enable : Connected.
• **Power Limit**	Change watt value of designated port. * Manual mode only.
• **Consume Power**	Amount of consuming power

Buttons

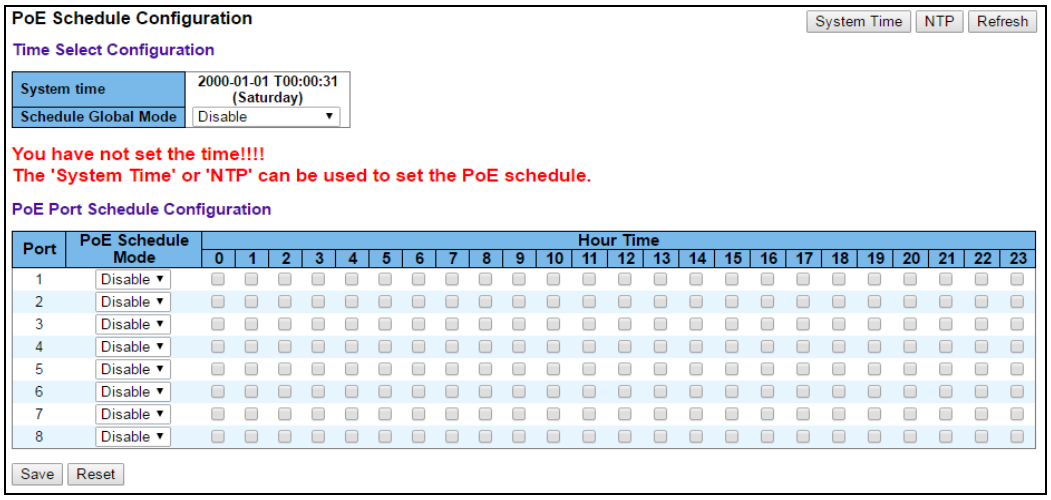
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page.

5.3.7.2 Schedule

This section constitutes POE schedule.



*** To use PoE schedule, please set System Time or NTP mode. If Systime is changed, PoE schedule will be working.**

Object	Description
• **System time**	Show System Time
• **Schedule Global Mode**	Set using PoE Schedule ot not
• **Port**	A port which is set PoE Schedule
• **PoE Schedule Mode**	Set Enable or Disable of PoE Schedule
• **Hour Time**	Designate time when use PoE Schedule

Buttons

Save: Click to save

Reset: Click to reset to previous saving data

Refresh: Click to refresh

System Time: Click to move System Time

NTP: Click to move NTP

5.3.7.3 Status

This page shows status of POE group.

PoE Status Auto-refresh Refresh

Global Status

Input Voltage [V]	54.20
Temperature [°C]	57.00
Max Temperature [°C]	57.00

Global Mode Status

PoE Global Mode	Schedule Global Mode
Enable	Disable

Port Status

Port	PoE Mode		Schedule Mode		Current [mA]	Consumption [W]		Link
	Conf	Stat	Conf	Stat	Stat	Limit	Stat	Stat
1	802.3at	Disable	Disable	Active	0.00	0.00	0.00	Disable
2	802.3at	Disable	Disable	Active	0.00	0.00	0.00	Disable
3	802.3at	Disable	Disable	Active	0.00	0.00	0.00	Disable
4	802.3at	Disable	Disable	Active	0.00	0.00	0.00	Disable
5	802.3at	Disable	Disable	Active	0.00	0.00	0.00	Disable
6	802.3at	Disable	Disable	Active	0.00	31.00	0.00	Enable
7	802.3at	Disable	Disable	Active	0.00	0.00	0.00	Disable
8	802.3at	Disable	Disable	Active	0.00	31.00	0.00	Enable
Total	-------	-------	-------	-------	0.00	62.00	0.00	-------

	Object	Description
•	**Input Voltage**	Indicate input voltage.
•	**Temperature**	Indicate temperature.
•	**Max Temperature**	Indicate max temperature.
•	**PoE Global Mode**	Activation of PoE Global Mode or not.
•	**Schedule Global Mode**	Activation of Schedule Global Mode or not.
•	**Port**	A port which uses POE.
•	**PoE Mode Conf**	Indicate PoE mode(af/at).
•	**PoE Mode Stat**	PoE state of connected port
•	**Schedule Mode Conf**	Using PoE Schedue or not
•	**Schedule Mode Stat**	PoE state as shcedue (Active/Inactive)
•	**Current[mA] stat**	Indicate electric current value[mA] of appointed port.
•	**Consumption[W]**	Indicate limitted W value of appointed port.

	Limit	
•	**Consumption[W] stat**	Indicate current W value of appointed port.
•	**Link stat**	Indicate Link status of of appointed port.

Buttons

Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

5.3.8 DIGITAL I/O

This page is used to configure the Digital Input/Output group.

Digital Input/Output Control Configuration

Digital Output Configuration

Digital Output	Status	Mode	Polarity
Digital Output1		Disable	Active Low
Digital Output2		Disable	Active Low

System Power Configuration

Power	Status	Mode	Output			
			Syslog	SNMPTemp	DigitalOutput1	DigitalOutput2
Power1		Disable	☐	☐	☐	☐
Power2		Disable	☐	☐	☐	☐

Digital Input Configuration

Digital Input	Status	Mode	Polarity	Output			
				Syslog	SNMPTemp	DigitalOutput1	DigitalOutput2
Digital Input1		Disable	Active High	☐	☐	☐	☐
Digital Input2		Disable	Active High	☐	☐	☐	☐

System Temperature Configuration

Temperature	Status		Limit [℃]		Mode	Output			
						Syslog	SNMPTemp	DigitalOutput1	DigitalOutput2
Temperature1	Temperature	42.125[℃]	High	80	Disable	☐	☐	☐	☐
	Status		Low	20					

System Port Configuration

Port	Status	mode	Output	
			DigitalOutput1	DigitalOutput2
port1		Disable	☐	☐
port2		Disable	☐	☐
port3		Disable	☐	☐
port4		Disable	☐	☐
port5		Disable	☐	☐
port6		Disable	☐	☐
port7		Disable	☐	☐
port8		Disable	☐	☐
port9		Disable	☐	☐
port10		Disable	☐	☐

* Please make sure to activate Syslog, SNMP before you set up the Syslog, SNMP of 'Output'.

Save Reset

Object	Description
Digital Output Configuration	
• **Digital Output**	It is the name of Digital Output.(Digital Output is OUT1 and Digital Output is OUT 2)
• **Mode**	Set the mode of the Digital Output.
• **Polarity**	Set the polarity of the Digital Output.
• **Status**	It shows the status of the Digital Output.

System Power Configuration	
• **Power**	It is the name of the power.
• **Status**	It shows the status of the Power. (Normal : green, Fail: dark gray)
• **Mode**	Set the mode of the Power.
• **Output**	Set whether to send out the status of the Power to Output. (Please make sure syslog and SNMP are set before you set up 'Output'.)
Digital Input Configuration	
• **Digital Input**	It is the name of Digital Input.
• **Mode**	Set the mode of Digital Input.
• **Polarity**	Set the polarity of the Digital Input.
• **Status**	It shows the status of the Digital Input.
• **Output**	Set whether to send out the status of the Digital input to Output. (Please make sure syslog and SNMP are set before you set up 'Output'.)
System Temperature Configuration	
• **Temperature**	It is the name of the Temperature.
• **Mode**	Set the mode of the Temperature.
• **Status**	It shows the status of the Temperature. Temperature : It shows the present temperature of the equipment. Status : (Normal : green, Fail: dark gray)
• **Limit**	High : Set the high temperature limit among the High-setup temperature range. Low : Set the low temperature limit among the Low-setup temperature range.

• **Output**	Set whether to send out the status of the Temperature to Output. (Please make sure syslog and SNMP are set before you set up 'Output'.)
	System Port Configuration
• **Port**	Name of System Port
• **Status**	State of System Port
• **Mode**	Mode of System Port
• **Output**	Set state of System Port sending Output or not

Buttons

Save: Click to save

Reset: Click to undo any changes made locally and revert to previously saved values.

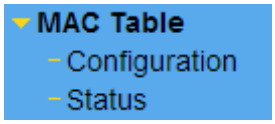
Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh

Syslog: Click to move Syslog – Configuration

SNMP Trap: Click to move SNMP - Trap

5.4 MAC TABLE



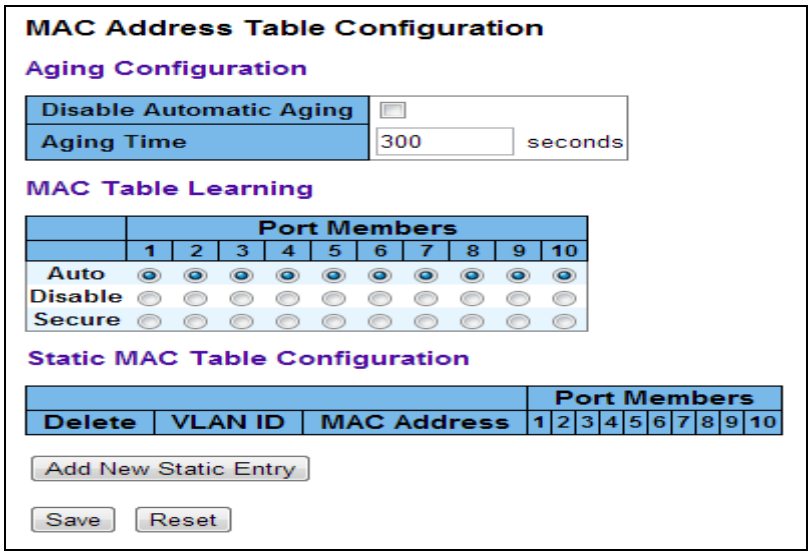
Indicate general setting detail of switch and configure.

In Mac Table, there are two chapters. In these chapters provide Mac information as below.

■	**Configuration**	Set Mac Table.
■	**Status**	Check Mac Table.

5.4.1 CONFIGURATION

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.



	Object	Description
●	**Disable Automatic Aging**	Disable Automatic Aging
●	**Aging time**	Configure aging time by entering a value here in seconds; for example, Age time seconds. The allowed range is 10 to 1000000 seconds.
●	**Auto**	Learning is done automatically as soon as a frame with unknown SMAC is received.
●	**Disable**	No learning is done.

• **Secure**	Only static MAC entries are learned, all other frames are dropped. Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

[Add New Static Entry]: Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

5.4.2 STATUS

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members										
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10
Dynamic	1	00-08-9F-0B-5E-61		✓									
Dynamic	1	00-08-9F-DA-A7-71		✓									
Dynamic	1	00-11-A9-B7-2D-96										✓	
Dynamic	1	00-12-6D-00-00-FD										✓	
Static	1	00-27-C6-3E-9F-84	✓										
Dynamic	1	08-9E-01-97-92-BB		✓									
Dynamic	1	08-9E-01-D3-B7-32		✓									
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Static	1	33-33-FF-00-00-00	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Static	1	33-33-FF-3E-9F-84	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Dynamic	1	EC-55-F9-BF-F9-5C		✓									
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Object	Description
•	**Type**	Indicates whether the entry is a static or a dynamic entry.
•	**MAC address**	The MAC address of the entry.
•	**VLAN**	The VLAN ID of the entry.
•	**Port Members**	The ports that are members of the entry.

Buttons

Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

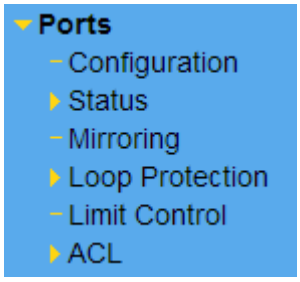
[Refresh]: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

[Cancel]: Flushes all dynamic entries..

<< : Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

>> : Updates the table, starting with the entry after the last entry currently displayed.

5.5 PORTS



Indicate general setting detail of switch and configure.

In Ports, there are six chapters. In these chapters provide Ports information as below.

■ **Configuration**	Set each port.
■ **Status**	Check each port.
■ **Mirroring**	To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.
■ **Loop protection**	Users can inspect or change configuration of loop.
■ **Limit Control**	Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below. The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

■ **ACL**	The Limit Control configuration consists of two sections, a system- and a port-wide. Set access control list, ACL port and speed limit.

5.5.1 CONFIGURATION

This page displays current port configurations. Ports can also be configured here.

Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>				9600	<>
1		1Gfdx	Auto	✕	✕		9600	Discard
2		Down	Auto	✕	✕		9600	Discard
3		Down	Auto	✕	✕		9600	Discard
4		Down	Auto	✕	✕		9600	Discard
5		Down	Auto	✕	✕		9600	Discard
6		Down	Auto	✕	✕		9600	Discard
7		Down	Auto	✕	✕		9600	Discard
8		Down	Auto	✕	✕		9600	Discard
9		1Gfdx	Auto	✕	✕		9600	
10		Down	Auto	✕	✕		9600	

Save Reset

	Object	Description
●	**Port**	This is the logical port number for this row.
●	**Link**	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
●	**Current Link Speed**	Provides the current link speed of the port.
●	**Configured Link Speed**	Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:

	Disabled - Disables the switch port operation. **Auto** - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. **10Mbps HDX** - Forces the cu port in 10Mbps half duplex mode. **10Mbps FDX** - Forces the cu port in 10Mbps full duplex mode. **100Mbps HDX** - Forces the cu port in 100Mbps half duplex mode. **100Mbps FDX** - Forces the cu port in 100Mbps full duplex mode. **1Gbps FDX** - Forces the port in 1Gbps full duplex **2.5Gbps FDX** - Forces the Serdes port in 2.5Gbps full duplex mode. **SFP_Auto_AMS** - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode with SFP preferred. Cu port is set in Auto mode. **100-FX** - SFP port in 100-FX speed. Cu port disabled. **100-FX_AMS** - Port in AMS mode with SFP preferred. SFP port in 100-FX speed. Cu port in Auto mode. **1000-X** - SFP port in 1000-X speed. Cu port disabled. **1000-X_AMS** - Port in AMS mode with SFP preferred. SFP port in 1000-X speed. Cu port in Auto mode.
• **Flow Control**	When **Auto Speed** is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx

	column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
• **Maximum Frame Size**	Enter the maximum frame size allowed for the switch port, including FCS.
• **Excessive Collision Mode**	Configure port transmit collision behavior. **Discard**: Discard frame after 16 collisions (default). **Restart**: Restart backoff algorithm after 16 collisions.

Buttons

[Save]: Click to save changes.

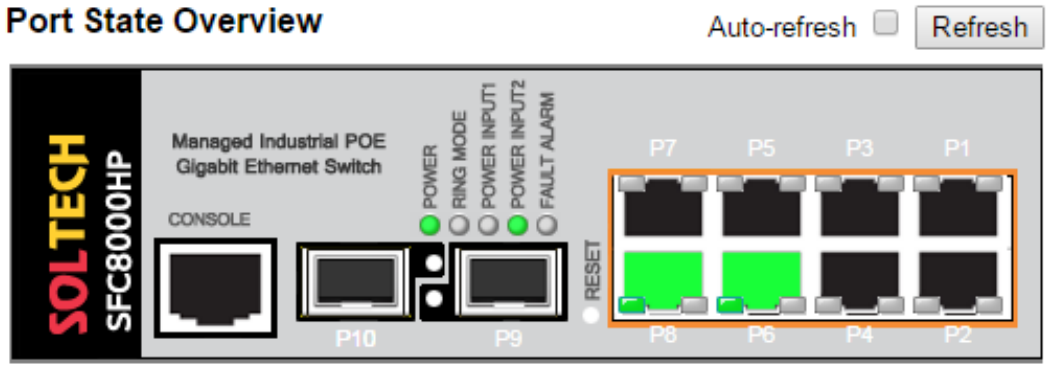
[Reset]: Click to undo any changes made locally and revert to previously saved values.

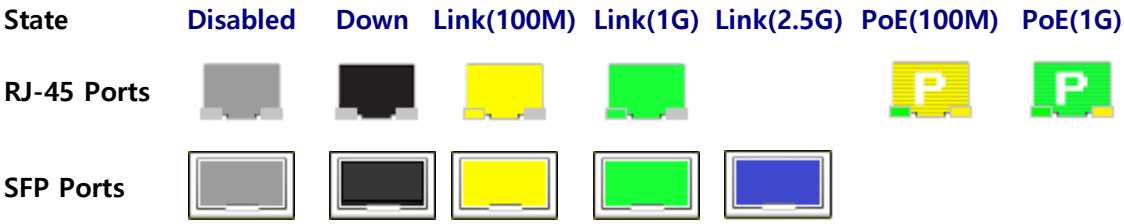
[Refresh]: Click to refresh the page.

5.5.2 STATUS

5.5.2.1 Port State

This page provides an overview of the current switch port states.





	Object	Description
●	**reset**	Change setting value into default value, if push it more than 2 seconds. If push it more than 10 seconds, all of setting value are changed into default value including IP(192.168.10.100).
●	**Power**	Turned on LED when power is supplied.
●	**Ring Mode**	Turned on when S-ring is set. **Master** : Blink LED cyclically. **Slave** : Turned LED always.
●	**Power Input1**	Turned on LED when Power input 1 is connected.
●	**Power Input2**	Turned on LED when Power input 2 is connected.
●	**Failt Alaram**	If there is no connection among neighboring equipment when S-ring-Slave is set. Turned on LED. If S-ring is not configurated by ring type when S-ring-Masrer is set. Turned on LED.
	Object	**Description**

● **reset**	Change setting value into default value, if push it more than 2 seconds. If push it more than 10 seconds, all of setting value are changed into default value including IP(192.168.10.100).
● **Power**	Turned on LED when power is supplied.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh : Click to refresh the page.

5.5.2.2 SFP Moudule Information

This page is used to configure the DDM group.

SFP Module Information Status

Status

Port	Serial Number	Speed	Wavelength (nm)	Temperature (°C)	Voltage (V)	Current (mA)	Tx Power(dBm)	Rx Power (dBm)
9	S1231240320177	1G	1310	0.0000	0.0000	0.0000	0.0000	0.0000
10	---	---	---	---	---	---	---	---

	Object	Description
●	**Port**	SFP is connected to the port number.
●	**Serial Number**	Serial Number is the value of the SFP module.
●	**Speed**	Transmission speed of the SFP module.
●	**Wavelength**	The wavelength(Bandwidth) of the SFP module. The unit is (nm).
●	**temperature**	The temperature of the SFP module. The unit is (Â°C) DDM function is only supported by the module.

• **Voltage**	SFP module input voltage. The unit is (V) DDM function is only supported by the module.
• **Current**	Amount of current consumption of the SFP module. The unit is (mA) DDM function is only supported by the module.
• **Tx Power**	SFP optical module transmit power. The unit is (dBm) DDM function is only supported by the module.
• **Rx Power**	SFP module optical receiver sensitivity. The unit is (dBm) DDM function is only supported by the module.

Buttons

Auto-refresh ☐ : Check this box to enable an automatic refresh of the page at regular intervals.

Refresh : Click to refresh the page immediately.

5.5.2.3 Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.

Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	444516	5150	35998190	1864934	0	0	372370	0	23
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	4374	443746	1559507	35855586	0	0	0	0	3
10	0	0	0	0	0	0	0	0	0

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Packets**	The number of received and transmitted packets per port.
• **Bytes**	The number of received and transmitted bytes per port.
• **Error**	The number of frames received in error and the number of incomplete transmissions per port.
• **Drops**	The number of frames discarded due to ingress or egress congestion.
• **Filtered**	The number of received frames filtered by the forwarding process.

Buttons

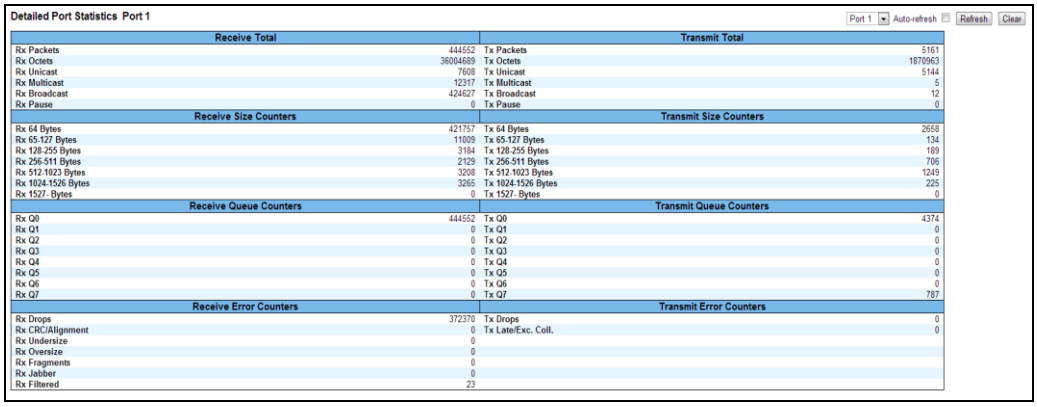
Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Cancel: Clears the counters for all ports.

5.5.3.4 Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.



Detailed Port Statistics Port 1

Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	444552	Tx Packets	5161
Rx Octets	36004689	Tx Octets	1870963
Rx Unicast	7608	Tx Unicast	5144
Rx Multicast	12317	Tx Multicast	5
Rx Broadcast	424627	Tx Broadcast	12
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	421757	Tx 64 Bytes	2658
Rx 65-127 Bytes	11009	Tx 65-127 Bytes	134
Rx 128-255 Bytes	3184	Tx 128-255 Bytes	189
Rx 256-511 Bytes	2129	Tx 256-511 Bytes	706
Rx 512-1023 Bytes	3208	Tx 512-1023 Bytes	1249
Rx 1024-1526 Bytes	3265	Tx 1024-1526 Bytes	225
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	444552	Tx Q0	4374
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	787
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	372370	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	23		

Object	Description
• **Rx and Tx Packets**	The number of received and transmitted (good and bad) packets.
• **Rx and Tx Octets**	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
• **Rx and Tx Unicast**	The number of received and transmitted (good and bad) unicast packets.
• **Rx and Tx Multicast**	The number of received and transmitted (good and bad) multicast packets.
• **Rx and Tx Broadcast**	The number of received and transmitted (good and bad) broadcast packets.
• **Rx and Tx Pause**	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
• **Rx Drops**	The number of frames dropped due to lack of receive buffers or egress congestion.
• **Rx CRC/Alignment**	The number of frames received with CRC or alignment errors.
• **Rx Undersize**	The number of short[1] frames received with valid CRC.
• **Rx Oversize**	The number of long[2] frames received with valid CRC.
• **Rx Fragments**	The number of short[1] frames received with invalid CRC.
• **Rx Jabber**	The number of long[2] frames received with invalid CRC.

• **Rx Filtered**	The number of received frames filtered by the forwarding process. [1]Short frames are frames that are smaller than 64 bytes. [2]Long frames are frames that are longer than the configured maximum frame length for this port.
• **Tx Drops**	The number of frames dropped due to output buffer congestion.
• **Tx Late/Exc.**	The number of frames dropped due to excessive or late collisions.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

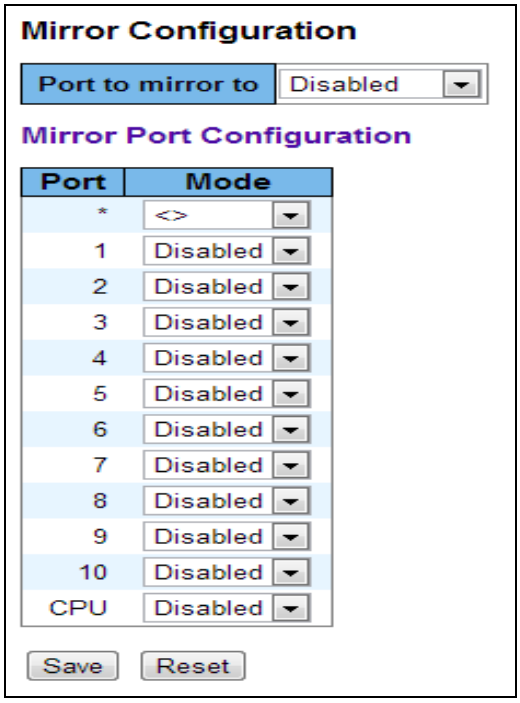
[Refresh]: Click to refresh the page immediately.

[Clear]: Clears the counters for the selected port.

5.5.3 MIRRORING

Configure port Mirroring on this page.

To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.



Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Mode**	Select mirror mode. **Rx only** Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. **Tx only** Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored. **Disabled** Neither frames transmitted nor frames received are mirrored. **Enabled** Frames received and frames transmitted are mirrored on the mirror port. **Note**: For a given port, a frame is only transmitted once. It is therefore not possible to mirror mirror port Tx frames. Because of this, mode for the selected mirror port is limited to **Disabled** or **Rx only**.

Buttons

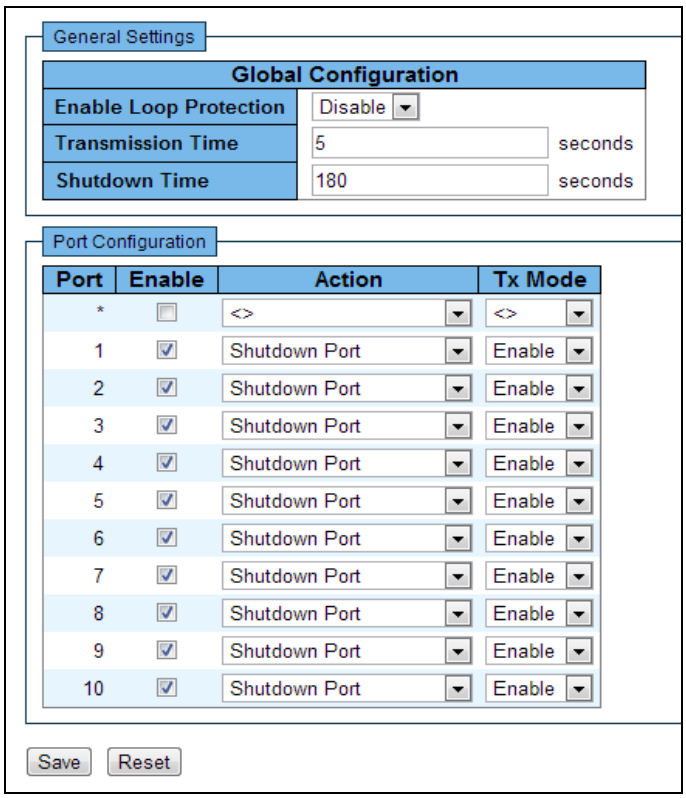
[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

5.5.4 LOOP PROTECTION

5.5.4.1 Configuration

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.



Object	Description
• **Enable Loop Protection**	Controls whether loop protections is enabled (as a whole).

• **Transmission Time**	The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.
• **Shutdown Time**	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).
• **Port**	The switch port number of the port.
• **Enable**	Controls whether loop protection is enabled on this switch port.
• **Action**	Configures the action performed when a loop is detected on a port. Valid values are **Shutdown Port**, **Shutdown Port and Log** or **Log Only**.
• **Tx Mode**	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.6.4.2 Status

This page displays the loop protection port status the ports of the switch.

Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

Object	Description

• **Port**	The switch port number of the logical port.
• **Action**	The currently configured port action.
• **Transmit**	The currently configured port transmit mode.
• **Loops**	The number of loops detected on this port.
• **Status**	The current loop protection status of the port.
• **Loop**	Whether a loop is currently detected on the port.
• **Time of Last Loop**	The time of the last loop event detected.

Buttons

Auto-refresh ☐ : Check this box to enable an automatic refresh of the page at regular intervals.

Refresh: Click to refresh the page immediately.

5.5.5 LIMIT CONTROL

This page allows you to configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port.

Port Security Limit Control Configuration

System Configuration

Mode	Disabled
Aging Enabled	☐
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen

Save Reset

Object	Description
• **Mode**	Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
• **Aging Enabled**	If checked, secured MAC addresses are subject to aging as discussed under Aging Period .
• **Aging Period**	If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds.
• **Port**	The port number to which the configuration below

	applies.
• **Mode**	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
• **Limit**	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
• **Action**	If Limit is reached, the switch can take one of the following actions: **None**: Do not allow more than Limit MAC addresses on the port, but take no further action. **Trap**: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded. **Shutdown**: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Boot the switch, 2) Disable and re-enable Limit Control on the port or the switch,

	3) Click the Reopen button. **Trap & Shutdown**: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.
• **State**	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: **Disabled**: Limit Control is either globally disabled or disabled on the port. **Ready**: The limit is not yet reached. This can be shown for all actions. **Limit Reached**: Indicates that the limit is reached on this port. This state can only be shown if Action is set to **None** or **Trap**. **Shutdown**: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to **Shutdown** or **Trap & Shutdown**.
• **Re-open Button**	If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to **Shutdown** in the Action section. Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values..

Refresh: Click to refresh the page. Note that non-committed changes will be lost.

5.5.6 ACL

5.5.6.1 Configuration

■ 5.5.6.1.1 port

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2 Port 3	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	444942
2	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	4396
10	0	Permit	Disabled	Disabled Port 1 Port 2 Port 3	Disabled	Disabled	Disabled	Enabled	0

Save Reset

Object	Description
● **Port**	The logical port for the settings contained in the same row.
● **Policy ID**	Select the policy to apply to this port. The allowed values

	are **0** through **255**. The default value is 0.
• **Action**	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
• **Rate Limiter ID**	Select which rate limiter to apply on this port. The allowed values are **Disabled** or the values **1** through **16**. The default value is "Disabled".
• **Port Redirect**	Select which port frames are redirected on. The allowed values are **Disabled** or a specific port number and it can't be set when action is permitted. The default value is "Disabled".
• **Mirror**	Specify the mirror operation of this port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled".
• **Logging**	Specify the logging operation of this port. The allowed values are: **Enabled**: Frames received on the port are stored in the System Log. **Disabled**: Frames received on the port are not logged. The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.
• **Shutdown**	Specify the port shut down operation of this port. The allowed values are: **Enabled**: If a frame is received on the port, the port will be disabled. **Disabled**: Port shut down is disabled. The default value is "Disabled".
• **State**	Specify the port state of this port. The allowed values are: **Enabled**: To reopen ports by changing the volatile port configuration of the ACL user module. **Disabled**: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".

● **Counter**	Counts the number of frames that match this ACE.

Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

[Refresh]: Click to refresh the page;

[Clear]: Click to clear the counters.

■ 5.5.6.1.2 Rate Limiters

Configure the rate limiter for the ACL of the switch.

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

[Save] [Reset]

Object	Description

• **Rate Limiter ID**	The rate limiter ID for the settings contained in the same row.
• **Rate**	The allowed values are: **0-3276700** in pps or **0, 100, 200, 300, ..., 1000000** in kbps.
• **Unit**	Specify the rate unit. The allowed values are: **pps**: packets per second. **kbps**: Kbits per second.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.5.6.1.3 Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is **256** on each switch.

Access Control List Configuration

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
								⊕

Object	Description
• **Ingress Port**	Indicates the ingress port of the ACE. Possible values are: **All**: The ACE will match all ingress port. **Port**: The ACE will match a specific ingress port.
• **Policy / Bitmask**	Indicates the policy number and bitmask of the ACE.
• **Frame Type**	Indicates the frame type of the ACE. Possible values are: **Any**: The ACE will match any frame type. **EType**: The ACE will match Ethernet Type frames. Note

	that an Ethernet Type based ACE will not get matched by IP and ARP frames. **ARP**: The ACE will match ARP/RARP frames. **IPv4**: The ACE will match all IPv4 frames. **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. **IPv6**: The ACE will match all IPv6 standard frames.
• **Action**	Indicates the forwarding action of the ACE. **Permit**: Frames matching the ACE may be forwarded and learned. **Deny**: Frames matching the ACE are dropped. **Filter**: Frames matching the ACE are filtered.
• **Rate Limiter**	Indicates the rate limiter number of the ACE. The allowed range is **1** to **16**. When **Disabled** is displayed, the rate limiter operation is disabled.
• **Port Redirect**	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are **Disabled** or a specific port number. When **Disabled** is displayed, the port redirect operation is disabled.
• **Mirror**	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled".
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.

• **Modification Buttons**	You can modify each ACE (Access Control Entry) in the table using the following buttons: ⊕: Inserts a new ACE before the current row. ⓔ: Edits the ACE row. ⬆: Moves the ACE up the list. ⬇: Moves the ACE down the list. ⊗: Deletes the ACE. ⊕: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

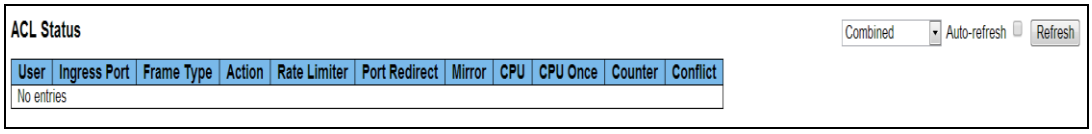
Refresh: Click to refresh the page;

Clear: Click to clear the counters.

Remove All: Click to remove all ACEs.

5.5.6.2 Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is **256** on each switch.



Object	Description

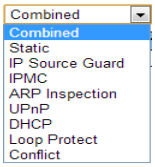
• **User**	Indicates the ACL user.
• **Ingress Port**	Indicates the ingress port of the ACE. Possible values are: **All**: The ACE will match all ingress port. **Port**: The ACE will match a specific ingress port.
• **Frame Type**	Indicates the frame type of the ACE. Possible values are: **Any**: The ACE will match any frame type. **EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. **ARP**: The ACE will match ARP/RARP frames. **IPv4**: The ACE will match all IPv4 frames. **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. **IPv6**: The ACE will match all IPv6 standard frames.
• **Action**	Indicates the forwarding action of the ACE. **Permit**: Frames matching the ACE may be forwarded and learned. **Deny**: Frames matching the ACE are dropped. **Filter**: Frames matching the ACE are filtered.
• **Rate Limiter**	Indicates the rate limiter number of the ACE. The allowed range is **1** to **16**. When **Disabled** is displayed, the rate limiter operation is disabled.
• **Port Redirect**	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are **Disabled** or a specific port number. When **Disabled** is displayed, the port redirect operation is disabled.

• **Mirror**	Specify the mirror operation of this port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled".
• **CPU**	Forward packet that matched the specific ACE to CPU.
• **CPU Once**	Forward first packet that matched the specific ACE to CPU.
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.
• **Conflict**	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

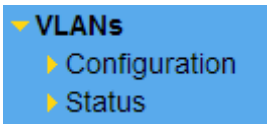
Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.



: The select box determines which ACL user is affected by clicking the buttons.

5.6 VLANS



Indicate general setting detail of switch and configure.

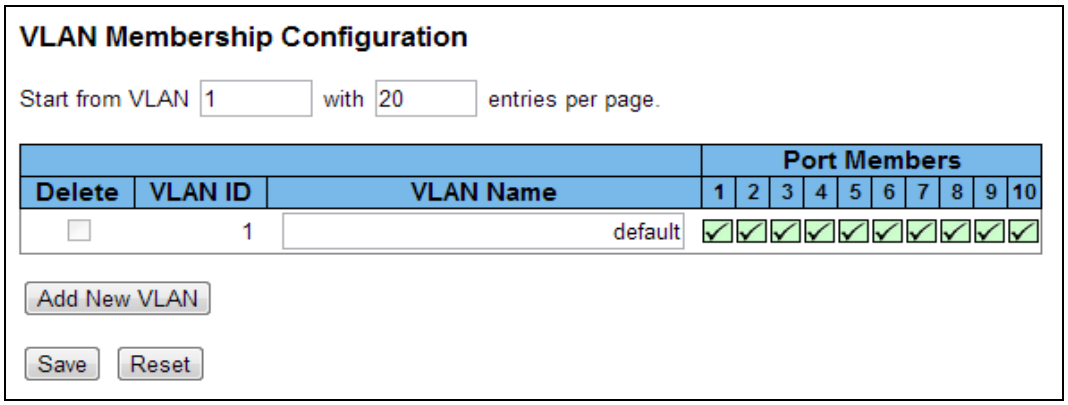
In VLANs, there are two chapters. In these chapters provide VLANs information as below.

■ **Configuration**	Set VLAN, PVLAN.
■ **Status**	Check VLAN, PVLAN.

5.6.1 CONFIGURATION

5.6.1.1 VLAN Membership

The VLAN membership configuration for the switch can be monitored and modified here. Up to 4096 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.



object	Description
● **Delete**	To delete a VLAN entry, check this box. The entry will be deleted during the next Save.
● **VLAN ID**	Indicates the ID of this particular VLAN.
● **VLAN Name**	Indicates the name of the VLAN. Maximum length of the VLAN Name String is 32. VLAN Name can be null. If it is not null, it must contain alphabets or numbers. At least one alphabet must be present in a non-null VLAN name. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.

• **Port Members**	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box as ✓ To include a port in a forbidden port list, check the box as shown ✗ To remove or exclude the port from the VLAN, make sure the box is unchecked as shown ▼ By default, no ports are members, and for every new VLAN entry all boxes are unchecked.
• **Add New VLAN**	Click [Add New VLAN] to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled when you click on "Save". The [Delete] button can be used to undo the addition of new

Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

[Refresh]: Refreshes the displayed table starting from the "VLAN ID" input fields.

[<<]: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

[>>]: Updates the table, starting with the entry after the last entry currently displayed.

5.6.1.2 Ports

This page is used for configuring the switch port VLAN.

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN Mode	Port VLAN ID	Tx Tag
*	<>		<>	<>	1	<>
1	Unaware		All	Specific	1	Untag_pvid
2	Unaware		All	Specific	1	Untag_pvid
3	Unaware		All	Specific	1	Untag_pvid
4	Unaware		All	Specific	1	Untag_pvid
5	Unaware		All	Specific	1	Untag_pvid
6	Unaware		All	Specific	1	Untag_pvid
7	Unaware		All	Specific	1	Untag_pvid
8	Unaware		All	Specific	1	Untag_pvid
9	Unaware		All	Specific	1	Untag_pvid
10	Unaware		All	Specific	1	Untag_pvid

Save Reset

object	Description
• **Ethertype for Custom S-ports**	This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports.
• **Port**	This is the logical port number of this row.
• **Port Type**	Port can be one of the following types: Unaware, Customer port(C-port), Service port(S-port), Custom Service port(S-custom-port) If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.
• **Ingress Filtering**	Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).
• **Frame Type**	Determines whether the port accepts all frames or only

	tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.
• **Port VLAN Mode**	Configures the Port VLAN Mode. The allowed values are **None** or **Specific**. This parameter affects VLAN ingress and egress processing. If **None** is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches. Tx tag should be set to Untag_pvid when this mode is used. If **Specific** (the default value) is selected, a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.
• **Port VLAN ID**	Configures the VLAN identifier for the port. The allowed values are from 1 through 4095. The default value is 1. Note: The port must be a member of the same VLAN as the Port VLAN ID.
• **Tx Tag**	Determines egress tagging of a port. Untag_pvid - All VLANs except the configured PVID will be tagged. Tag_all - All VLANs are tagged. Untag_all - All VLANs are untagged.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Save : Click to save changes.

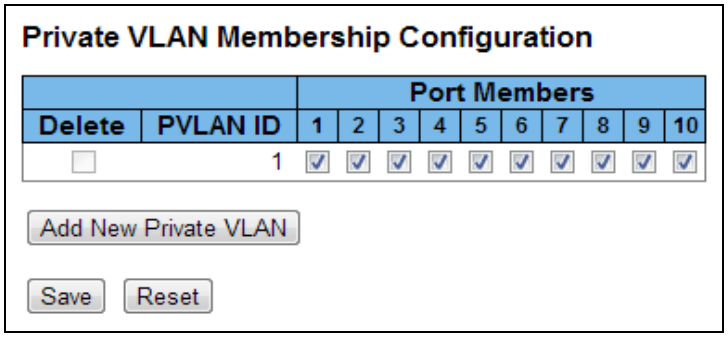
[Reset]: Click to undo any changes made locally and revert to previously saved values.

[Refresh]: Click to refresh the page immediately.

5.6.1.3 Private VLANs

■ 5.6.1.3.1 PVLAN Membership

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.



object	Description
● **Delete**	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
● **Private VLAN ID**	Indicates the ID of this particular private VLAN.
● **Port Members**	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
● **Add New Private VLAN**	Click [Add New Private VLAN] to add a new private VLAN ID. An empty row is added to the table, and the private

	VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click "Save". The [Delete] button can be used to undo the addition of new Private VLANs.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

[Save]: Click to save changes.

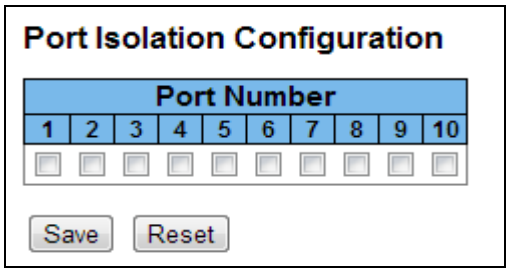
[Reset]: Click to undo any changes made locally and revert to previously saved values.

[Refresh]: Click to refresh the page immediately.

5.6.1.3.2 Port Isolation

This page is used for enabling or disabling port isolation on ports in a Private VLAN.

A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.



object	Description
• Port Numbers	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page immediately.

5.6.1.4 VCL

■ 5.6.1.4.1 MAC-based VLAN

The MAC-based VLAN enties can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

MAC-based VLAN Membership Configuration

			Port Members									
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10
Currently no entries present												

Add New Entry

Save Reset

object	Description
• **Delete**	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
• **MAC Address**	Indicates the MAC address.
• **VLAN ID**	Indicates the VLAN ID.
• **Port Members**	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
• **Add New Entry**	Click [Add New Entry] to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095. The MAC-based VLAN entry is enabled when you click on "Save". A MAC-based VLAN without any port members will be deleted when you click "Save". The [Delete] button can be used to undo the addition of new MAC-based VLANs. The maximum possible MAC-based VLAN entries are limited to 256.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

Refresh: Refreshes the displayed table.

<< : Updates the table starting from the first entry in the MAC-based VLAN Table.

>> : Updates the table, starting with the entry after the last entry currently displayed.

5.6.1.4.2 Protocol-based VLAN

5.6.1.4.2.1 Protocol to Group

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switch .

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
No Group entry found!			

Add New Entry

Save Reset

object	Description
• **Delete**	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
• **Frame Type**	Frame Type can have one of the following values: 1. Ethernet 2. LLC 3. SNAP Note: On changing the Frame type field, valid value of

	the following text field will vary depending on the new frame type you selected.
• **Value**	Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu. Below is the criteria for three different Frame Types: **1. For Ethernet**: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff **2. For LLC**: Valid value in this case is comprised of two different sub-values. a. **DSAP**: 1-byte long string (0x00-0xff) b. **SSAP**: 1-byte long string (0x00-0xff) **3. For SNAP**: Valid value in this case also is comprised of two different sub-values. a. **OUI**: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. b. **PID**: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.
• **Group Name**	A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). **Note**: special character and underscore(_) are not allowed.

• **Add New Entry**	Click [Add New Entry] to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed. The button can be used to undo the addition of new entry. The [Delete] maximum possible Protocol to Group mappings are limited to 128.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

[Refresh]: Click to refresh the page immediately.

• 5.6.1.4.2.1.2 Group to VLAN

This page allows you to map a already configured Group Name to a VLAN for the switch .

Group Name to VLAN mapping Table

			Port Members								
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10
No Group entries												

[Add New Entry]

[Save] [Reset]

object	Description

• **Delete**	To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save.
• **Group Name**	A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.
• **VLAN ID**	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
• **Port Members**	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
• **Add New Entry**	Click [Add New Entry] to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The [Delete] button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page immediately.

5.6.1.4.3 IP Subnet-based Vlan

The IP subnet-based VLAN enties can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

IP Subnet-based VLAN Membership Configuration

					Port Members									
Delete	VCE ID	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10
Currently no entries present														

Add New Entry

Save Reset

object	Description
• **Delete**	To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
• **VCE ID**	Indicates the index of the entry. It is user configurable. It's value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.
• **IP Address**	Indicates the IP address.
• **Mask Length**	Indicates the network mask length.
• **VLAN ID**	Indicates the VLAN ID. VLAN ID can be changed for the existing entries.
• **Port Members**	A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make

	sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
• **Add New Entry**	Click [Add New Entry] to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095. The IP subnet-based VLAN entry is enabled when you click on "Save". The [Delete] button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

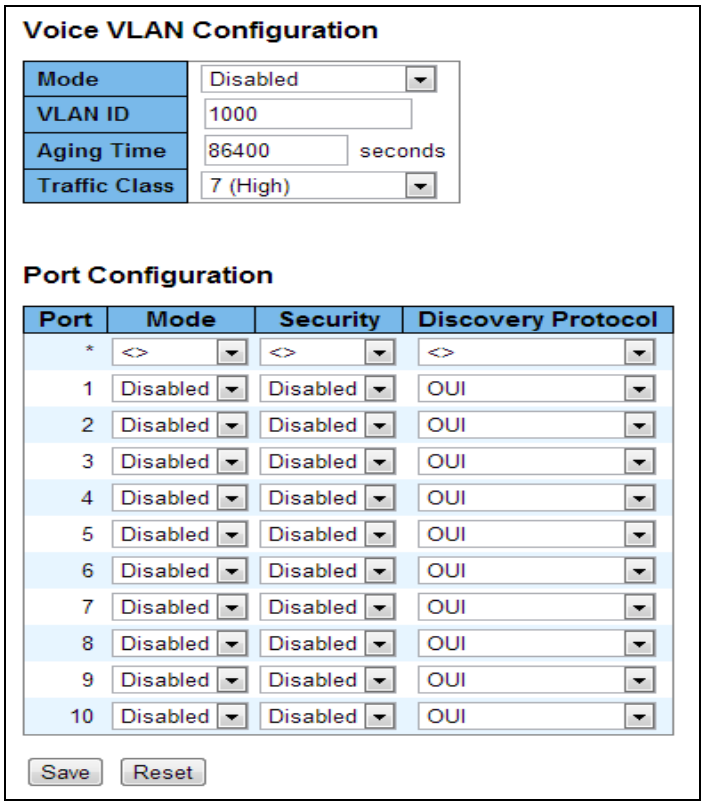
[Refresh]: Refreshes the displayed table.

5.6.1.5 Voice VLAN

■ 5.6.1.5.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the

switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.



object	Description
• **Mode**	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: **Enabled**: Enable Voice VLAN mode operation. **Disabled**: Disable Voice VLAN mode operation.
• **VLAN ID**	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
• **Aging Time**	Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other

	cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.
• **Traffic Class**	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.
• **Port Mode**	Indicates the Voice VLAN port mode. Possible port modes are: **Disabled**: Disjoin from Voice VLAN. **Auto**: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. **Forced**: Force join to Voice VLAN.
• **Port Security**	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are: **Enabled**: Enable Voice VLAN security mode operation. **Disabled**: Disable Voice VLAN security mode operation.
• **Port Discovery Protocol**	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are: **OUI**: Detect telephony device by OUI address. **LLDP**: Detect telephony device by LLDP. **Both**: Both OUI and LLDP.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.6.1.5.2 OUI

Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process.

Voice VLAN OUI Table

Delete	Telephony OUI	Description
☐	00-01-e3	Siemens AG phones
☐	00-03-6b	Cisco phones
☐	00-0f-e2	H3C phones
☐	00-60-b9	Philips and NEC AG phones
☐	00-d0-1e	Pingtel phones
☐	00-e0-75	Polycom phones
☐	00-e0-bb	3Com phones

Add New Entry

Save Reset

object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Telephony OUI**	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
• **Description**	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Buttons

Add New Entry: Click to add a new access management entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.6.2 STATUS

5.6.2.1 VLAN Membership

This page provides an overview of membership status of VLAN users.

object	Description
• **VLAN ID**	VLAN ID for which the Port members are displayed.
• **Port Members**	A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, an image ✓ will be displayed. If a port is included in a Forbidden port list, an image ✕ will be displayed.

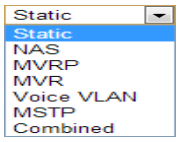
Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Use the button to start over.

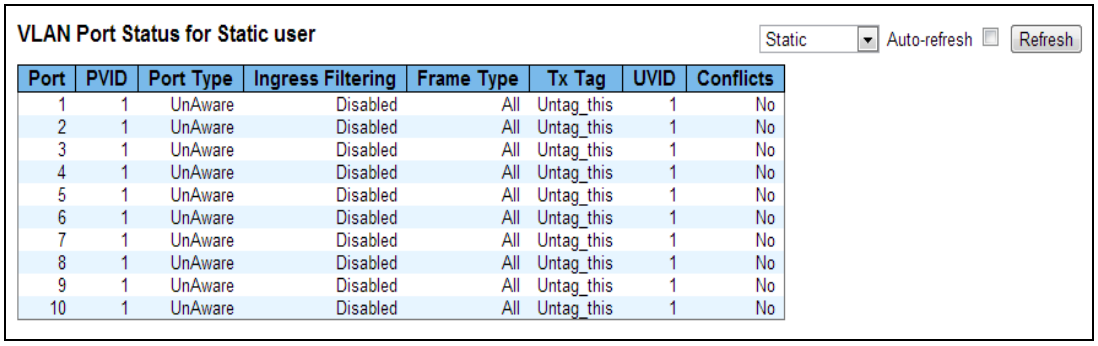
>>: The button will use the last entry of the currently displayed VLAN entry as a basis for the next lookup.



: Select VLAN Users from this drop down list.

5.6.2.2 VLAN Port

This page provides VLAN Port Status.



VLAN Port Status for Static user

Static | Auto-refresh | Refresh

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No
5	1	UnAware	Disabled	All	Untag_this	1	No
6	1	UnAware	Disabled	All	Untag_this	1	No
7	1	UnAware	Disabled	All	Untag_this	1	No
8	1	UnAware	Disabled	All	Untag_this	1	No
9	1	UnAware	Disabled	All	Untag_this	1	No
10	1	UnAware	Disabled	All	Untag_this	1	No

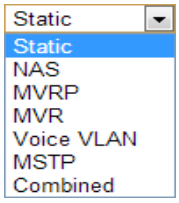
object	Description
• **Port**	The logical port for the settings contained in the same row.
• **PVID**	Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.
• **Port Type**	Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port. If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.
• **Ingress Filtering**	Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

• **Frame Type**	Shows whether the port accepts all frrrames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
• **Tx Tag**	Shows egress filtering frame status whether tagged or untagged.
• **UVID**	Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behaviour at the egress side.
• **Conflicts**	Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur: Functional Conflicts between features. Conflicts due to hardware limitation. Direct conflict between user modules.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

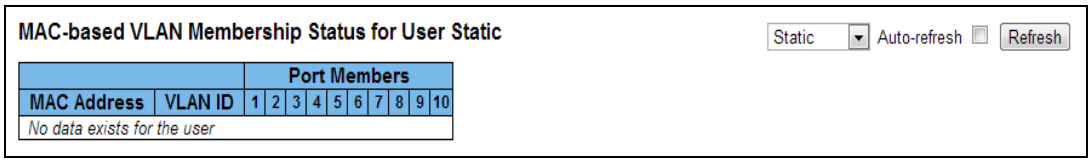


: Select VLAN Users from this drop down list.

5.6.2.3 VCL

■ 5.6.2.3.1 MAC-based VLAN

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users.



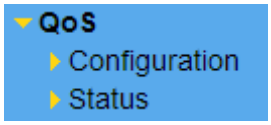
object	Description
• **MAC Address**	Indicates the MAC address.
• **VLAN ID**	Indicates the VLAN ID.
• **Port Members**	Port members of the MAC-based VLAN entry.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table.

5.7 QOS



Indicate general setting detail of switch and configure.

In QOS there are two chapters. In these chapters provide QOS information as below.

■ **Configuration**	Set Qos.
■ **Status**	Check Qos.

5.7.1 CONFIGURATION

5.7.1.1 Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports.

QoS Ingress Port Classification

Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<>	<>	<>	<>		
1	0	0	0	0	Disabled	
2	0	0	0	0	Disabled	
3	0	0	0	0	Disabled	
4	0	0	0	0	Disabled	
5	0	0	0	0	Disabled	
6	0	0	0	0	Disabled	
7	0	0	0	0	Disabled	
8	0	0	0	0	Disabled	
9	0	0	0	0	Disabled	
10	0	0	0	0	Disabled	

Save Reset

object	Description
• **Port**	The port number for which the configuration below applies.
• **QoS class**	Controls the default QoS class. All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a QoS class that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default QoS class. The classified QoS class can be overruled by a QCL entry. Note: If the default QoS class has been dynamically changed, then the actual default QoS class is shown in parentheses after the configured default QoS class.

• **DP level**	Controls the default Drop Precedence Level. All frames are classified to a DP level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level. The classified DP level can be overruled by a QCL entry.
• **PCP**	Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
• **DEI**	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
• **Tag Class**	Shows the classification mode for tagged frames on this port. Disabled: Use default QoS class and DP level for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping. Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default QoS class and DP level.
• **DSCP Based**	Click to Enable DSCP Based QoS Ingress Port Classification.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.7.1.2 Port Policing

This page allows you to configure the Policer settings for all switch ports.

QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	☐	500	<>	☐
1	☐	500	kbps	☐
2	☐	500	kbps	☐
3	☐	500	kbps	☐
4	☐	500	kbps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐
9	☐	500	kbps	☐
10	☐	500	kbps	☐

Save Reset

object	Description
• **Port**	The port number for which the configuration below applies.
• **Enabled**	Controls whether the policer is enabled on this switch port.
• **Rate**	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the

	"Unit" is "Mbps" or "kfps".
• **Unit**	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".
• **Flow Control**	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

5.7.1.3 Queue Policing

This page allows you to configure the Queue Policer settings for all switch ports.

QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐

[Save] [Reset]

object	Description
• **Port**	The port number for which the configuration below applies.

• **Enabled (E)**	Controls whether the queue policer is enabled on this switch port.
• **Rate**	Controls the rate for the queue policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps". This field is only shown if at least one of the queue policers are enabled.
• **Unit**	Controls the unit of measure for the queue policer rate as kbps or Mbps. The default value is "kbps". This field is only shown if at least one of the queue policers are enabled.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.7.1.4 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

QoS Egress Port Schedulers

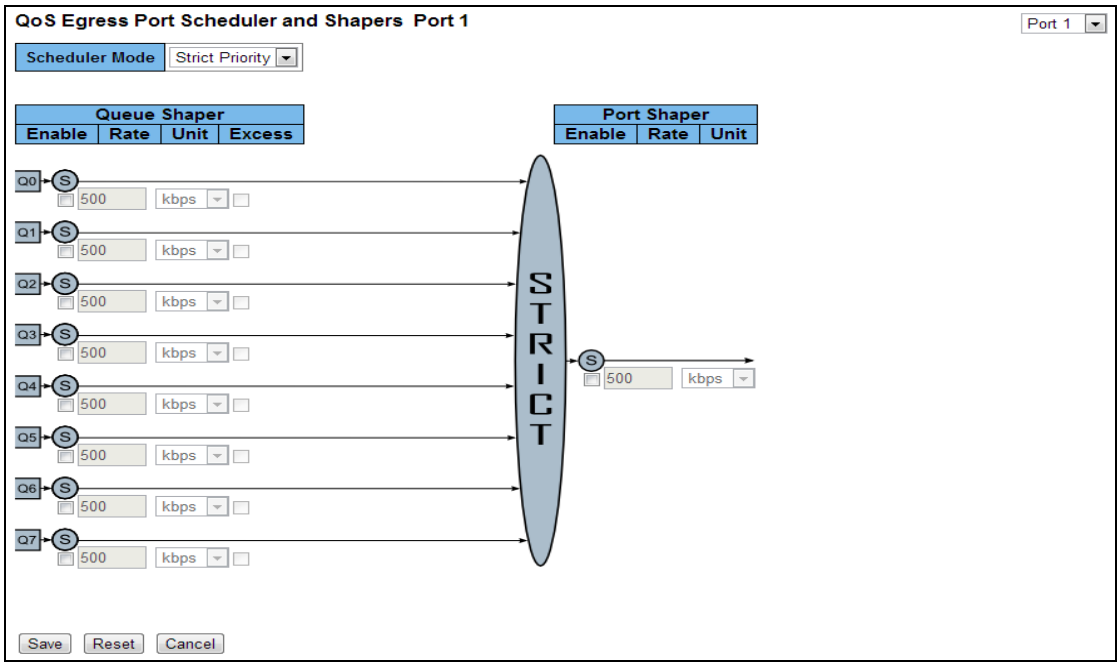
Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-

object	Description
• **Port**	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
• **Mode**	Shows the scheduling mode for this port.
• **Weight**	Shows the weight for this queue and port.

5.7.1.4.1 Port Scheduler and Shapers Port

Click a port No. to configure.

This page allows you to configure the Scheduler and Shapers for a specific port.



	object	Description
•	**Scheduler Mode**	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
•	**Queue Shaper Enable**	Controls whether the queue shaper is enabled for this queue on this switch port.
•	**Queue Shaper Rate**	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
•	**Queue Shaper Unit**	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
•	**Queue Shaper Excess**	Controls whether the queue is allowed to use excess bandwidth.
•	**Queue Scheduler Weight**	Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
•	**Queue Scheduler Percent**	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

• **Port Shaper Enable**	Controls whether the port shaper is enabled for this switch port.
• **Port Shaper Rate**	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
• **Port Shaper Unit**	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

[Cancel]: Click to undo any changes made locally and return to the previous page.

5.7.1.5 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

QoS Egress Port Shapers

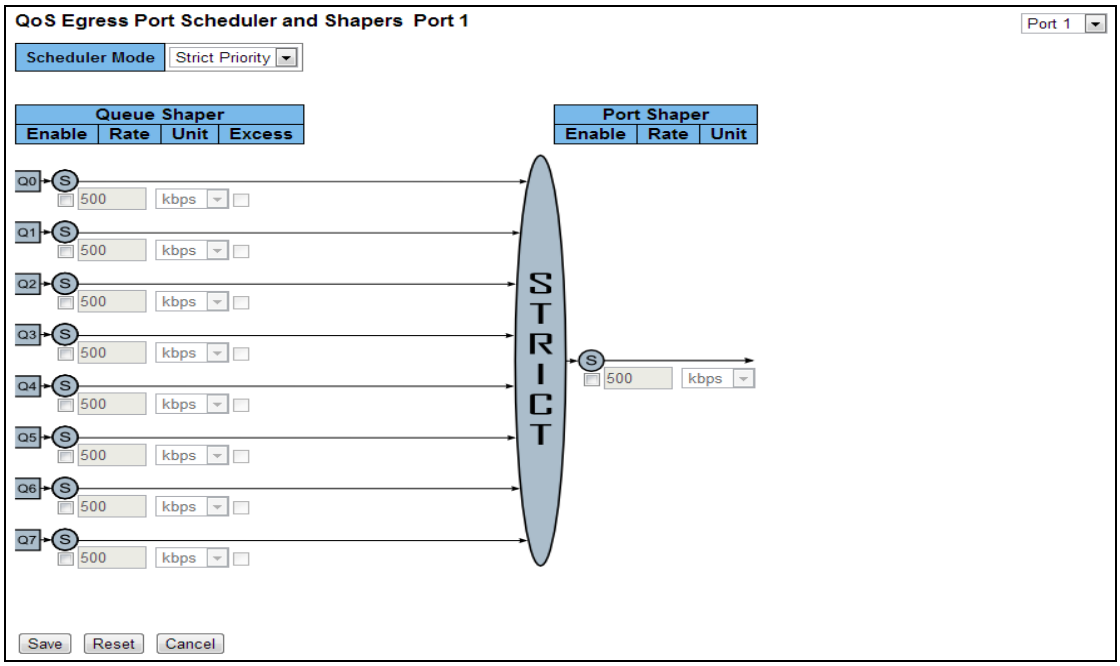
Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

object	Description
• **Port**	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.
• **Shapers**	Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".
• **Port**	Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

5.7.1.5.1 QoS Egress Port Scheduler and Shapers Port

Click a port No. to configure.

This page allows you to configure the Scheduler and Shapers for a specific port.



object	Description
• **Scheduler Mode**	Controls whether the scheduler mode is "Strict Priority"

	or "Weighted" on this switch port.
• **Queue Shaper Enable**	Controls whether the queue shaper is enabled for this queue on this switch port.
• **Queue Shaper Rate**	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
• **Queue Shaper Unit**	Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
• **Queue Shaper Excess**	Controls whether the queue is allowed to use excess bandwidth.
• **Queue Scheduler Weight**	Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
• **Queue Scheduler Percent**	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
• **Port Shaper Enable**	Controls whether the port shaper is enabled for this switch port.
• **Port Shaper Rate**	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
• **Port Shaper Unit**	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to undo any changes made locally and return to the previous page.

5.7.1.6 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified

object	Description
• **Port**	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.
• **Mode**	Shows the tag remarking mode for this port. **Classified**: Use classified PCP/DEI values. **Default**: Use default PCP/DEI values. **Mapped**: Use mapped versions of QoS class and DP level.

5.7.1.6.1 QoS Egress Port Tag Remarking Port

Click a port No. to configure.

The QoS Egress Port Tag Remarking for a specific port are configured on this page.

	object	Description
•	**Mode**	Controls the tag remarking mode for this port. **Classified**: Use classified PCP/DEI values. **Default**: Use default PCP/DEI values. **Mapped**: Use mapped versions of QoS class and DP level.
•	**PCP/DEI Configuration**	Controls the default PCP and DEI values used when the mode is set to **Default**.
•	**(QoS class, DP level) to (PCP, DEI) Mapping**	Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to **Mapped**.

Buttons

Save: Click to save changes

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to undo any changes made locally and return to the previous page.

5.7.1.7 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☐	Disable	Disable
3	☐	Disable	Disable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable
7	☐	Disable	Disable
8	☐	Disable	Disable
9	☐	Disable	Disable
10	☐	Disable	Disable

Save Reset

object	Description
• **Port**	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
• **Translate**	To Enable the Ingress Translation click the checkbox.
• **Ingress**	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: **1. Translate** **2. Classify**
• **Classify**	Classification for a port have 4 different values. **Disable**: No Ingress DSCP Classification. **DSCP=0**: Classify if incoming (or translated if enabled) DSCP is 0. **Selected**: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation

	window for the specific DSCP. **All**: Classify all DSCP.
• **Egress**	Port Egress Rewriting can be one of - **Disable**: No Egress rewrite. **Enable**: Rewrite enabled without remapping. **Remap DP Unaware**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. **Remap DP Aware**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

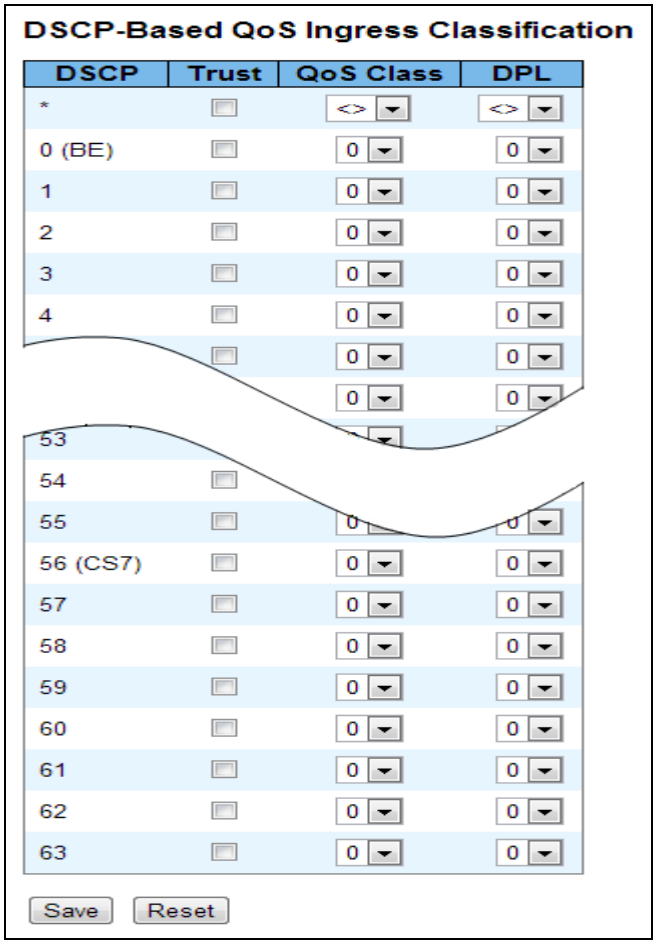
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.7.1.8 DSCP-Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.



object	Description
• **DSCP**	Maximum number of supported DSCP values are 64.
• **Trust**	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
• **QoS Class**	QoS class value can be any of (0-7)
• **DPL**	Drop Precedence Level (0-1)

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.7.1.9 DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>		<>	<>
0 (BE)	0 (BE)		0 (BE)	0 (BE)
1	1		1	1
2	2		2	2
3	3		3	3
4	4		4	4
5	5		5	5
6	6		6	6
7	7		7	7
8 (CS1)	8 (CS1)		8 (CS1)	8 (CS1)
[illegible]	[illegible]		9	9
[illegible]	[illegible]		10 (AF11)	10 (AF1[illegible]
[illegible]	53		11	[illegible]
54	54		[illegible]	[illegible]
55	55		[illegible]	[illegible]
56 (CS7)	56 (CS7)		[illegible]	[illegible] (CS7)
57	57		57	57
58	58		58	58
59	59		59	59
60	60		60	60
61	61		61	61
62	62		62	62
63	63		63	63

Save Reset

object	Description

• **DSCP**	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
• **Ingress**	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation - **1. Translate** **2. Classify**
• **Translate**	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
• **Classify**	Click to enable Classification at Ingress side.
• **Egress**	There are the following configurable parameters for Egress side - **1. Remap DP0** Controls the remapping for frames with DP level 0. **2. Remap DP1** Controls the remapping for frames with DP level 1.
• **Remap DP0**	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
• **Remap DP1**	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.7.1.10 DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.

DSCP Classification

QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)
5	0	0 (BE)
5	1	0 (BE)
6	0	0 (BE)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

Save Reset

	object	Description
•	**QoS Class**	Actual QoS class.
•	**DPL**	Actual Drop Precedence Level.
•	**DSCP**	Select the classified DSCP value (0-63).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.7.1.11 QoS Control List

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

Click on the lowest plus sign to add a new QCE to the list.

QoS Control List Configuration

QCE#	Port	Frame Type	SMAC	DMAC	VID	PCP	DEI	Action			
								Class	DPL	DSCP	
											⊕

object	Description
• **QCE#**	Indicates the index of QCE.
• **Port**	Indicates the list of ports configured with the QCE.
• **Frame Type**	Indicates the type of frame to look for incoming frames. Possible frame types are: **Any**: The QCE will match all frame type. **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. **LLC**: Only (LLC) frames are allowed. **SNAP**: Only (SNAP) frames are allowed. **IPv4**: The QCE will match only IPV4 frames. **IPv6**: The QCE will match only IPV6 frames.
• **SMAC**	Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.
• **DMAC**	Specify the type of Destination MAC addresses for incoming frame. Possible values are: **Any**: All types of Destination MAC addresses are allowed. **Unicast**: Only Unicast MAC addresses are allowed. **Multicast**: Only Multicast MAC addresses are allowed. **Broadcast**: Only Broadcast MAC addresses are allowed. The default value is 'Any'.

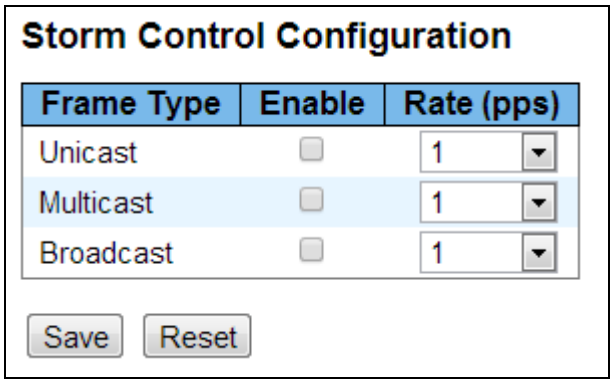
• **VID**	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
• **PCP**	Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
• **DEI**	Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.
• **Action**	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. **Class**: Classified QoS class. **DPL**: Classified Drop Precedence Level. **DSCP**: Classified DSCP value.
• **Modification Buttons**	You can modify each QCE (QoS Control Entry) in the table using the following buttons: Inserts a new QCE before the current row. Edits the QCE. Moves the QCE up the list. Moves the QCE down the list. Deletes the QCE. The lowest plus sign adds a new entry at the bottom of the QCE listings.

5.7.1.12 Storm Control

Storm control for the switch is configured on this page.

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch.



object	Description
• **Frame Type**	The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.
• **Enable**	Enable or disable the storm control status for the given frame type.
• **Rate**	The rate unit is packets per second (pps). Valid values are: **1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K.**

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.7.2 STATUS

5.7.2.1 QoS Statistics

This page provides statistics for the different queues for all switch ports.

Queuing Counters Auto-refresh Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	903408306	18674	0	0	0	0	0	0	0	0	0	0	0	0	0	7186
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	18676	56908786	0	0	0	0	0	0	0	0	0	0	0	0	0	2
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

object	Description
• **Port**	The logical port for the settings contained in the same row.
• **QN**	There are 8 QoS queues per port. Q0 is the lowest priority queue.
• **Rx/Tx**	The number of received and transmitted packets per queue.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

5.7.2.2 QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware

limitations. The maximum number of QCEs is 256 on each switch.

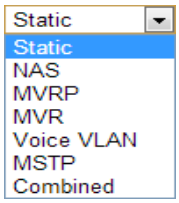
QoS Control List Status Combined Auto-refresh Resolve Conflict Refresh

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DPL	DSCP	
No entries							

object	Description
• **User**	Indicates the QCL user.
• **QCE#**	Indicates the index of QCE.
• **Frame Type**	Indicates the type of frame to look for incoming frames. Possible frame types are: **Any**: The QCE will match all frame type. **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. **LLC**: Only (LLC) frames are allowed. **SNAP**: Only (SNAP) frames are allowed. **IPv4**: The QCE will match only IPV4 frames. **IPv6**: The QCE will match only IPV6 frames.
• **Port**	Indicates the list of ports configured with the QCE.
• **Action**	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. **Class**: Classified QoS class; if a frame matches the QCE it will be put in the queue. **DPL**: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. **DSCP**: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

• **Conflict**	Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons



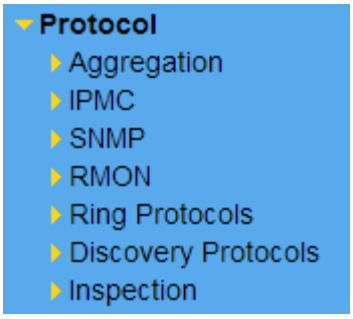
: Select the QCL status from this drop down list.

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Resolve Conflict: Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

Refresh: Click to refresh the page.

5.8 PROTOCOL



Indicate general setting detail of switch and configure.

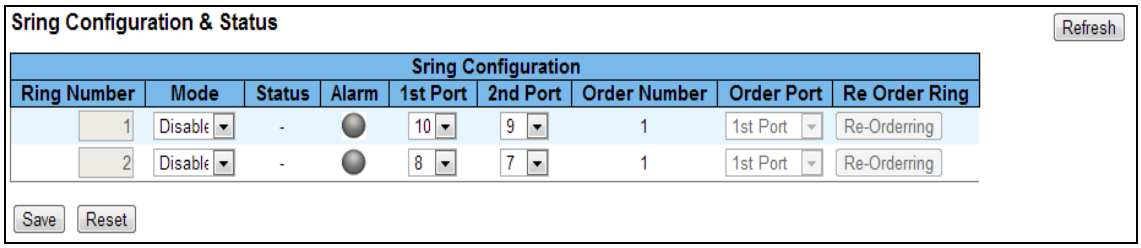
In PROTOCOL, there are three chapters. In these chapters provide PROTOCOL information as below.

■ **Ring Protocols**	Check the status of Ring protocol. It can set devices as ring type using STP, RSTP and MSTP.
■ **Aggregation**	Set and check Static, LACP
■ **IPMC**	Set and check IGMP Snooping, MLD Snooping, MVR
■ **SNMP**	Receive change of network device through SNMP setting, Trap setting for network management system.
■ **RMON**	Set or check RMON(Statistics, History, Alarm, Event).
■ **Discovery Protocols**	Can adjust bandwidth to set LLDP, UPnP.
■ **Inspection**	Set DHCP, IP Source Guard, ARP Inspections and sFlow to avoid an attack from other devices.

5.8.1 RING PROTOCOLS

5.8.1.1 S-RING

This page can set S-ring.



object	Description
● **Ring Number**	Ring number

• **Mode**	Use or nonuse of s-ring, Show S-ring mode. Disabled : Nonuse of s-ring Slave : Set Slave mode of S-ring. Master : Set Master mode of S-ring
• **Status**	Show the status of S-ring. (Master mode only) Open : In case of it is not ring type. Ring : In case of it is ring type.
• **Alarm**	Show the status of S-ring using pictures. : Disable or slave : In case of it is not ring type. : In case of it is ring type.
• **1st Port**	Set a port to configure S-ring. (s-ring #1 port)
• **2nd Port**	Set a port to configure S-ring. (s-ring #2 port)
• **Order Number**	Show Order Number of Ring. Order Ring : Assign ring number to catch type of configuration easily.
• **Order Port**	Master mode only. Set a port to assign Order Number in S-ring ports.
• **Re Order Ring**	Master mode only. It assigns the Order Number as Order Port setting. (Notice : Users must click 'save → Re Order Ring' buttons. If not, Order Number is not assigned.)

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

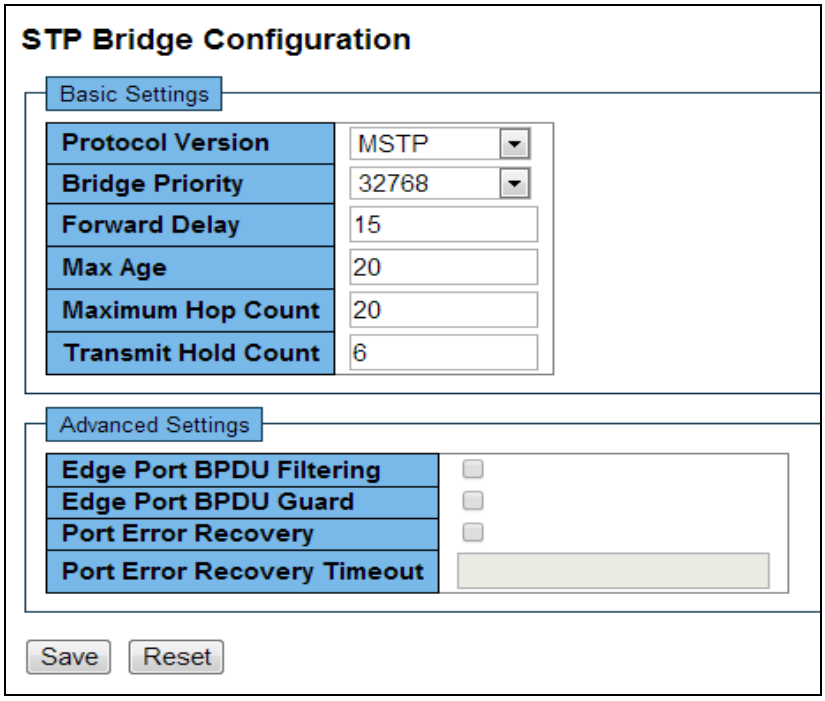
Refresh: Click to refresh the page.

5.8.1.2 Spanning Tree

■ 5.8.1.2.1 Configuration

● 5.8.1.2.1.1 Bridge Settings

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch.



object	Description
● **Protocol Version**	The MSTP / RSTP / STP protocol version setting. Valid values are **STP, RSTP** and **MSTP**.
● **Bridge Priority**	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For **MSTP** operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

• **Forward Delay**	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
• **Max Age**	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.
• **Maximum Hop Count**	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
• **Transmit Hold Count**	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
• **Edge Port BPDU Filtering**	Control whether a port explicitly configured as **Edge** will transmit and receive BPDUs.
• **Edge Port BPDU Guard**	Control whether a port explicitly configured as **Edge** will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
• **Port Error Recovery**	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
• **Port Error Recovery Timeout**	The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

[Save]: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

- ### 5.8.1.2.1.2 CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.

This page contains settings for physical and aggregated ports.

STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
-	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
*	☐	<>		<>	<>	☐	☐	☐	☐	<>
1	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
2	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
3	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
4	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
5	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
6	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
7	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
8	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
9	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
10	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto

Save Reset

object	Description
• **Port**	The switch port number of the logical STP port.
• **STP Enabled**	Controls whether STP is enabled on this switch port.
• **Path Cost**	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the

	physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
• **AdminEdge**	Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).
• **AutoEdge**	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
• **Restricted Role**	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
• **Restricted TCN**	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region,

	possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
• **BPDU Guard**	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
• **Point-to-Point**	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

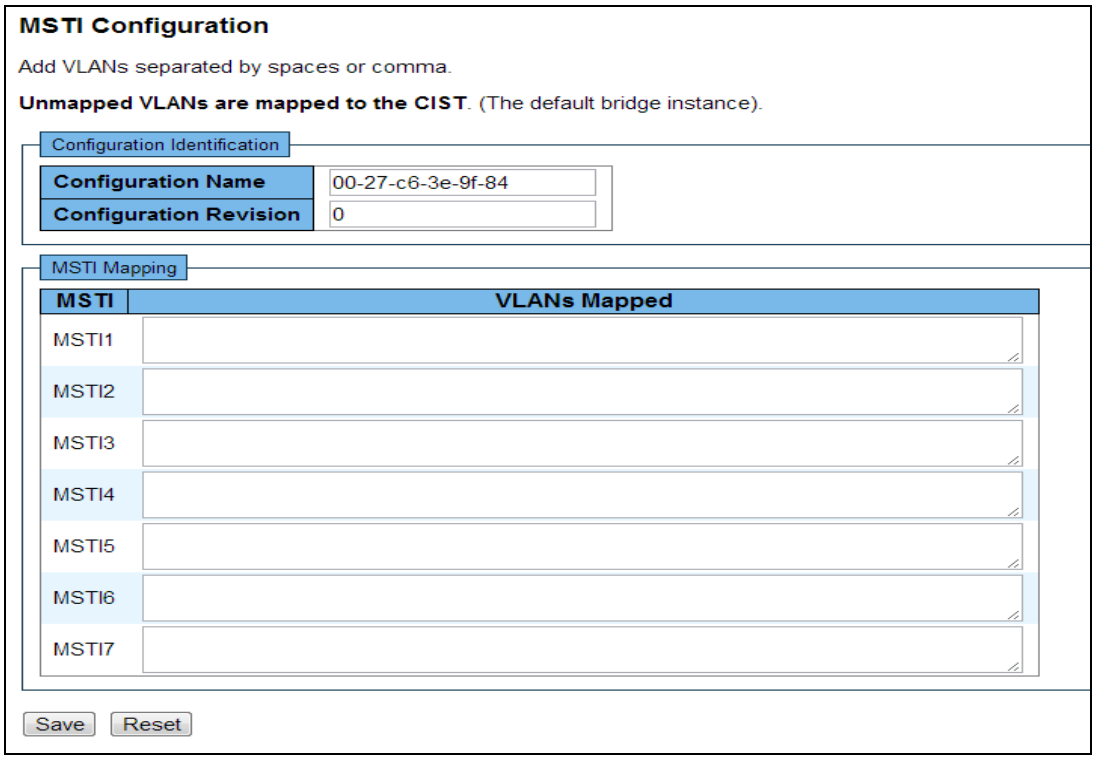
Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

• 5.8.1.2.1.3 MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



object	Description
• **Configuration Name**	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.
• **Configuration Revision**	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
• **MSTI**	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
• **VLANs Mapped**	The list of VLANs mapped to the MSTI. The VLANs can be given as a single (**xx**, xx being between 1 and 4094) VLAN, or a range (**xx-yy**), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

Example: **2,5,20-40**.

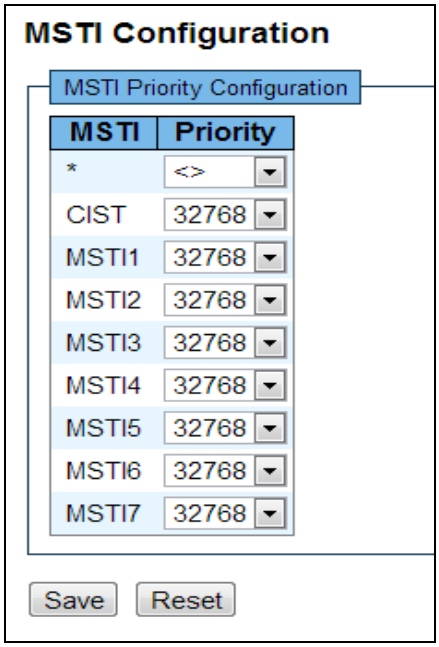
Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

5.8.1.2.1.4 MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



object	Description
• **MSTI**	The bridge instance. The CIST is the default instance, which is always active.
• **Priority**	Controls the bridge priority. Lower numeric values have

	better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

Save: Click to save changes.

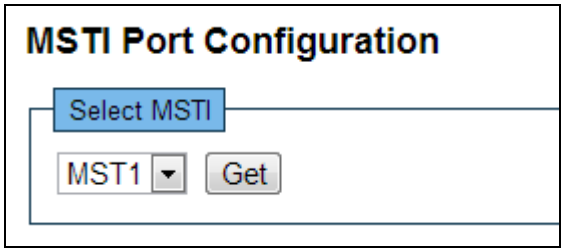
Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.1.2.1.5 MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports.



object	Description
• **Port**	The switch port number of the corresponding STP CIST (and MSTI) port.
• **Path Cost**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended

	values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

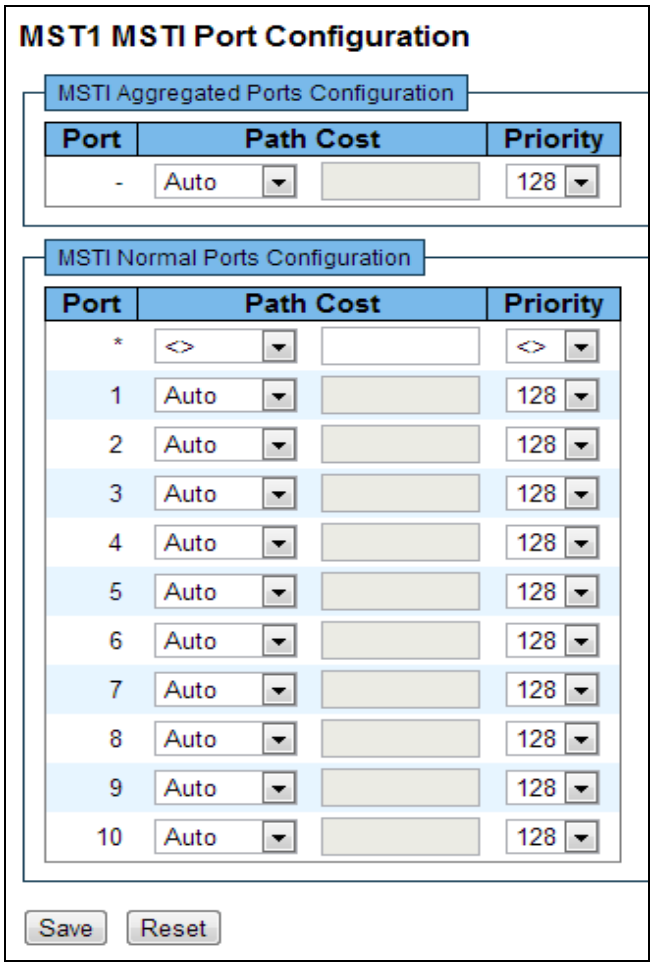
Get : Click to retrieve settings for a specific MSTI.

Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

5.8.1.1.1.5.1 MSTI Port Configuration

When click 'Get' button, the next page will be displayed for MSTI setting.



object	Description
• **Port**	The switch port number of the corresponding STP CIST (and MSTI) port.
• **Path Cost**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.1.2.2 Status

5.8.1.2.2.1 Bridge Status

This page provides a status overview of all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

STP Bridges Auto-refresh Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-27-C6-3E-9F-84	32768.00-27-C6-3E-9F-84	-	0	Steady	-

object	Description
• **MSTI**	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
• **Bridge ID**	The Bridge ID of this Bridge instance.
• **Root ID**	The Bridge ID of the currently elected root bridge.
• **Root Port**	The switch port currently assigned the root port role.
• **Root Cost**	Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
• **Topology Flag**	The current state of the Topology Change Flag of this Bridge instance.
• **Topology**	The time since last Topology Change occurred.

Change Last

Buttons

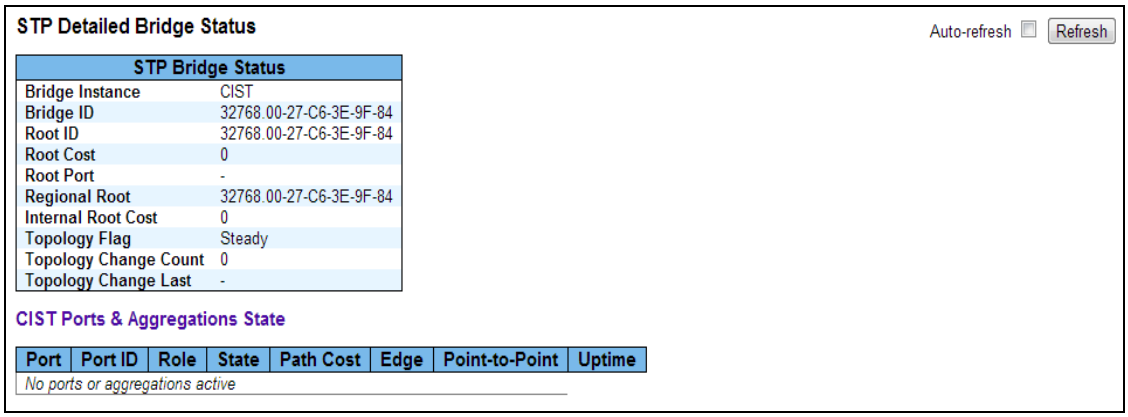
Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

5.8.1.1.2.1.1 STP Detailed Bridge Status

Users can check the next page if click MSTI link.

It shows detailed information of STP.



STP Detailed Bridge Status

Auto-refresh ☐ Refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-27-C6-3E-9F-84
Root ID	32768.00-27-C6-3E-9F-84
Root Cost	0
Root Port	-
Regional Root	32768.00-27-C6-3E-9F-84
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
No ports or aggregations active							

object	Description
• **Bridge Instance**	The Bridge instance - **CIST, MST1**, ...
• **Bridge ID**	The Bridge ID of this Bridge instance.
• **Root ID**	The Bridge ID of the currently elected root bridge.
• **Root Port**	The switch port currently assigned the root port role.
• **Root Cost**	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the

	least cost path to the Root Bridge.
• **Regional Root**	The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only).
• **Internal Root Cost**	The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only).
• **Topology Flag**	The current state of the Topology Change Flag of this Bridge instance.
• **Topology Change Count**	The number of times where the topology change flag has been set (during a one-second interval).
• **Topology Change Last**	The time passed since the Topology Flag was last set.
• **Port**	The switch port number of the logical STP port.
• **Port ID**	The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.
• **Role**	The current STP port role. The port role can be one of the following values: **AlternatePort BackupPort RootPort DesignatedPort.**
• **State**	The current STP port state. The port state can be one of the following values: **Discarding Learning Forwarding.**
• **Path Cost**	The current STP port path cost. This will either be a value computed from the **Auto** setting, or any explicitly configured value.
• **Edge**	The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.
• **Point-to-Point**	The current STP port point-to-point flag. A point-to-point

	port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.
• **Uptime**	The time since the bridge port was last initialized.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

• 5.8.1.2.2.2 Port Status

This page displays the STP CIST port status for physical ports of the switch.

STP Port Status

Auto-refresh ☐ Refresh

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-

	object	Description
•	**Port**	The switch port number of the logical STP port.
•	**CIST Role**	The current STP port role of the CIST port. The port role can be one of the following values: **AlternatePort**

	BackupPort RootPort DesignatedPort Disabled.
• **CIST State**	The current STP port state of the CIST port. The port state can be one of the following values: **Discarding Learning Forwarding.**
• **Uptime**	The time since the bridge port was last initialized.

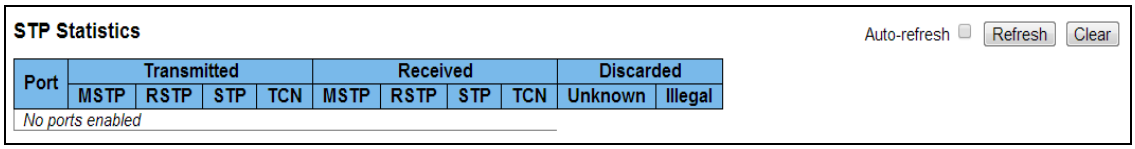
Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

• 5.8.1.2.2.3 Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.



	object	Description
•	**Port**	The switch port number of the logical STP port.
•	**MSTP**	The number of MSTP BPDU's received/transmitted on the port.
•	**RSTP**	The number of RSTP BPDU's received/transmitted on the port.
•	**STP**	The number of legacy STP Configuration BPDU's received/transmitted on the port.
•	**TCN**	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

● **Discarded Unknown**	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
● **Discarded Illegal**	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Click to reset the counters.

5.8.1.3 ERPS

■ 5.8.1.3.1 MEP

The Maintenance Entity Point instances are configured here.

Maintenance Entity Point Refresh

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm

Add New MEP Save Reset

object	Description
● **Delete**	This box is used to mark a MEP for deletion in next Save operation.
● **Instance**	The ID of the MEP. Click on the ID of a MEP to enter the configuration page.
● **Domain**	**Port**: This is a MEP in the Port Domain. 'Flow Instance' is a Port. **Esp**: Future use

	Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC **Mpls**: Future use
• **Mode**	**MEP**: This is a Maintenance Entity End Point. **MIP**: This is a Maintenance Entity Intermediate Point.
• **Direction**	**Ingress**: This is a Ingress (down) MEP - monitoring ingress traffic on 'Residence Port'. **Egress**: This is a Egress (up) MEP - monitoring egress traffic on 'Residence Port'.
• **Residence Port**	The port where MEP is monitoring - see 'Direction'.
• **Level**	The MEG level of this MEP.
• **Flow Instance**	The MEP is related to this flow - See 'Domain'.
• **Tagged VID**	**Port MEP**: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
• **This MAC**	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
• **Alarm**	There is an active alarm on the MEP.

Buttons

Add New MEP : Click to add a new MEP entry.

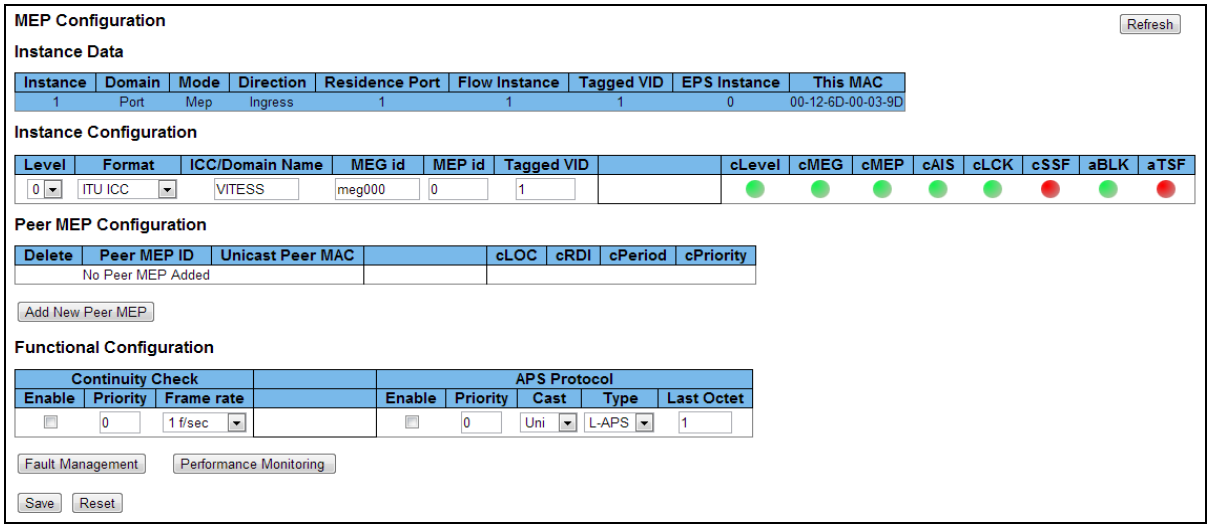
Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.1.3.1.1 MEP Configuration

This page allows the user to inspect and configure the current MEP Instance.



object	Description
• **MEP Instance**	The ID of the MEP.
• **Domain**	See help on MEP create WEB.
• **Mode**	See help on MEP create WEB.
• **Direction**	See help on MEP create WEB.
• **Residence Port**	See help on MEP create WEB.
• **Flow Instance**	See help on MEP create WEB.
• **Tagged VID**	See help on MEP create WEB.
• **This MAC**	See help on MEP create WEB.
• **EVC Policy ID**	This is relevant for a Caracal EVC Egress-MEP and Jaguar MEP. This is the Policy number of the relevant ECE. **Jaguar**: Policy ID is used to assure that received OAM PDU is able to hit a IS2 entry. If this value is '0' IS2 rules will be created on clasified VID. If this is NOT '0' IS2 rules will be created on this Policy (PAG). This must be equal to ECE Policy Number if OAM PDU will hit the ECE IS0. This is the case if an ECE is create with 'tag_type' as 'any' **Caracal**: Policy ID that the generated TST frames will get as IS1 action. Can be the same as any ECE Policy

	Number, enabling it to hit the same ACL and thereby the sam EVC policer.
• **EVC QoS**	This is only relevant for a EVC MEP. This is the Qos of the EVC and used for getting QoS counters for Loss Measurement.
• **Level**	See help on MEP create WEB.
• **Format**	This is the configuration of the two possible Maintenance Association Identifier formats. **ITU ICC**: This is defined by ITU. 'ICC' can be max. 6 char. 'MEG id' can be max. 7 char. **IEEE String**: This is defined by IEEE. 'Domain Name' can be max. 8 char. 'MEG id' can be max. 8 char.
• **ICC/Domain Name**	This is either ITU ICC (MEG ID value[1-6]) or IEEE Maintenance Domain Name - depending on 'Format'. See 'Format'.
• **MEG Id**	This is either ITU UMC (MEG ID value[7-13]) or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this can be max. 7 char. If only 6 char. is entered the MEG ID value[13] will become NULL.
• **MEP Id**	This value will become the transmitted two byte CCM MEP ID.
• **Tagged VID**	This value will be the VID of a TAG added to the OAM PDU.
• **VOE**	This will attemt to utilize VOE HW for MEP implementation. Not all platforms support VOE.
• **cLevel**	Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.
• **cMEG**	Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.
• **cMEP**	Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.
• **cAIS**	Fault Cause indicating that AIS PDU is received.

• **cLCK**	Fault Cause indicating that LCK PDU is received.
• **cSSF**	Fault Cause indicating that server layer is indicating Signal Fail.
• **aBLK**	The consequent action of blocking service frames in this flow is active.
• **aTSF**	The consequent action of indicating Trail Signal Fail towards protection is active.
• **Delete**	This box is used to mark a Peer MEP for deletion in next Save operation.
• **Peer MEP ID**	This value will become an expected MEP ID in a received CCM - see 'cMEP'.
• **Unicast Peer MAC**	This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.
• **cLOC**	Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.
• **cRDI**	Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.
• **cPeriod**	Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.
• **cPriority**	Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.
• **Enable**	Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.
• **Priority**	The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.
• **Frame rate**	Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses:

	* The transmission rate of the CCM PDU. * Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'. * Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'. Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.
• **Enable**	Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.
• **Priority**	The priority to be inserted as PCP bits in TAG (if any).
• **Cast**	Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.
• **Type**	**R-APS**: APS PDU is transmitted as R-APS - this is for ERPS. **L-APS**: APS PDU is transmitted as L-APS - this is for ELPS.
• **Last Octet**	This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

Buttons

Add New Peer MEP : Click to add a new peer MEP.

Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC		cLOC	cRDI	cPeriod	cPriority
	No Peer MEP Added						
Delete	0	00-00-00-00-00-00					

Add New Peer MEP

Fault Management : Click to go to Fault Management page.

Performance Monitoring : Click to go to Performance Monitor page.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.1.3.1.2.1 Fault Management – Instance 1

This page allows the user to inspect and configure the Fault Management of the current MEP Instance.

Fault Management - Instance 1 Refresh

Loop Back

Enable	Dei	Priority	Cast	Peer MEP	Unicast MAC	To Send	Size	Interval
☐	☐	0	Uni	0	00-00-00-00-00-00	10	100	10

Loop Back State

Transaction ID	Transmitted	Reply MAC	Received	Out Of Order
No Replies				

Link Trace

Enable	Priority	Peer MEP	Unicast MAC	Time To Live
☐	0	0	00-00-00-00-00-00	1

Link Trace State

Transaction ID	Time To Live	Mode	Direction	Relayed	Last MAC	Next MAC
No Transactions						

Test Signal

Tx	Rx	Dei	Priority	Peer MEP	Rate	Size	Pattern	Sequence Number
☐	☐	☐	0	0	1	64	All Zero	☐

Test Signal State

TX frame count	RX frame count	RX rate	Test time	Clear
0	0	0	0	☐

Client Configuration

Domain	Level	Flow									
Evc	0	0	0	0	0	0	0	0	0	0	0

AIS

Enable	Priority	Frame Rate	Protection
☐	0	1 f/sec	☐

LOCK

Enable	Priority	Frame Rate
☐	0	1 f/sec

Back

Save Reset

object	Description
• **Enable**	Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end.
• **Dei**	The DEI to be inserted as PCP bits in TAG (if any).
• **Priority**	The priority to be inserted as PCP bits in TAG (if any).
• **Cast**	Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop

	Back is possible.
• **Peer MEP**	This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
• **Unicast MAC**	This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP.
• **To Send**	The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behaviour). This is HW based LBM/LBR and Requires VOE.
• **Size**	The number of bytes in the LBM PDU Data Pattern TLV.
• **Interval**	The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1us. in case 'To Send' == 0 (max 10.000)",
• **Transaction ID**	The transaction id of the first LBM transmitted. For each LBM transmitted the transaction id in the PDU is incremented.
• **Transmitted**	The total number of LBM PDU transmitted.
• **Reply MAC**	The MAC of the replying MEP/MIP. In case of multi-cast LBM, replies can be received from all peer MEP in the group. This MAC is not shown in case of 'To Send' == 0.
• **Received**	The total number of LBR PDU received from this 'Reply MAC'.
• **Out Of Order**	The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.
• **Enable**	Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.
• **Priority**	The priority to be inserted as PCP bits in TAG (if any).
• **Peer MEP**	This is only used if the 'Unicast MAC' is configured to all

	zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
• **Unicast MAC**	This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.
• **Time To Live**	This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero.
• **Transaction ID**	The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.
• **Time To Live**	This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.
• **Mode**	Indicating if is was a MEP/MIP sending this LTR.
• **Direction**	Indicating if MEP/MIP sending this LTR is ingress/egress.
• **Relayed**	Indicating if MEP/MIP sending this LTR has relayed/forwarded the LTM.
• **Last MAC**	The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.
• **Next MAC**	The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.
• **Enable**	Test Signal based on transmitting TST PDU can be enabled/disabled.
• **Dei**	The DEI to be inserted as PCP bits in TAG (if any).
• **Priority**	The priority to be inserted as PCP bits in TAG (if any).
• **Peer MEP**	The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.
• **Rate**	The TST frame transmission bit rate - in Mega bits pr. second. Limit on Caracal is 400 Mbps. Limit on Serval is 1Gbps.

• **Size**	The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes). Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. The transmitting frame rate will be adjusted according to the actually transmitted frame size to obtain correct transmission bit rate.
• **Pattern**	The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern. Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes The TST PDU needs to be 46 bytes so a pattern of 46-12=34 bytes will be added. **All Zero**: Pattern will be '00000000' **All One**: Pattern will be '11111111' **10101010**: Pattern will be '10101010'
• **TX frame count**	The number of transmitted TST frames since last 'Clear'.
• **RX frame count**	The number of received TST frames since last 'Clear'.
• **RX rate**	The current received TST frame bit rate in 100 Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'
• **Test time**	The number of seconds passed since first TST frame received after last 'Clear'.
• **Clear**	This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving

	first TST frame.
• **Domain**	The domain of the client layer. Must be EVC.
• **Level**	Client layer level - meaning that PDU transmitted in client layer flows will be on this level.
• **Flow**	Client layer flow instance numbers - max. 10. Must only be configured in case of Port MEP.
• **Enable**	Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled.
• **Prio**	On Caracal this priority is used in sink direction (client layer). On Serval, for each client EVC, the highest COS-ID (ECE Class) is used.
• **Frame Rate**	Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.:
• **Protection**	Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.
• **Enable**	Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled.
• **Prio**	The priority to be inserted in MEP source direction. On Caracal, this priority is also used in sink direction (client layer). On Serval, for each client EVC, the highest COS-ID (ECE Class) is used.
• **Frame Rate**	Selecting the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.:

Buttons

Back : Click to go back to this MEP instance main page.

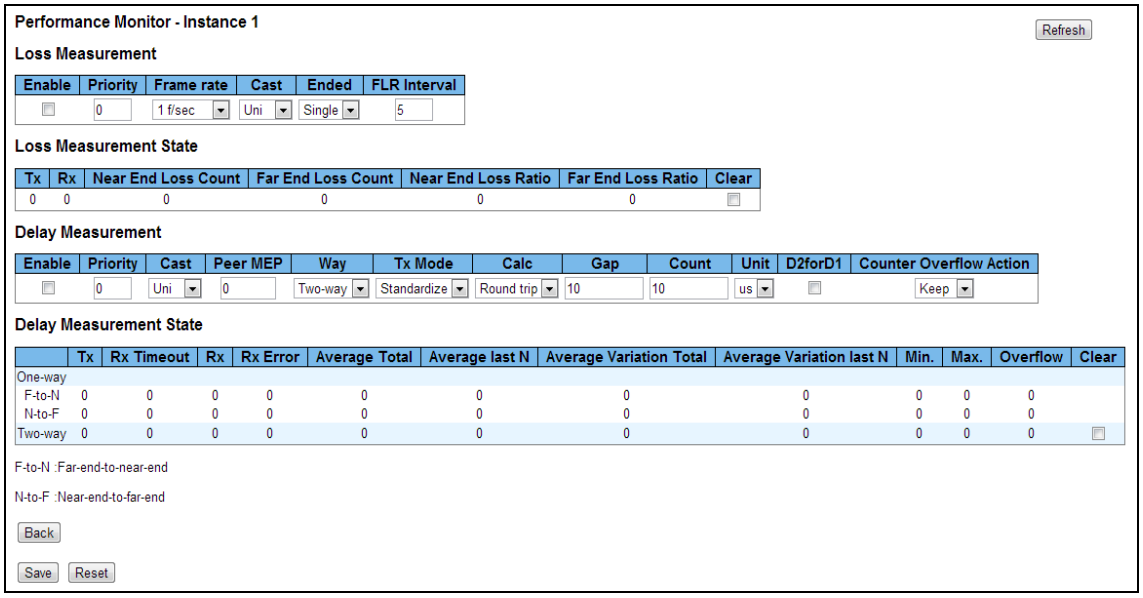
Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.1.3.1.3 performance Monitor –Instance 1

This page allows the user to inspect and configure the performance monitor of the current MEP Instance.



object	Description
• **Enable**	Loss Measurement based on transmitting/receiving CCM or LMM/LMR PDU can be enabled/disabled - see 'Ended'. This is only valid with one Peer MEP configured.
• **Priority**	The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.
• **Frame rate**	Selecting the frame rate of CCM/LMM PDU. This is the inverse of transmission period as described in Y.1731. Selecting 300f/sec or 100f/sec is not valid. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.
• **Cast**	Selection of CCM or LMM PDU transmitted unicast or

	multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.
• **Ended**	**Single**: Single ended Loss Measurement implemented on LMM/LMR. **Dual**: Dual ended Loss Measurement implemented on SW based CCM.
• **FLR Interval**	This is the interval in seconds where the Frame Loss Ratio is calculated.
• **Near End Loss Count**	The accumulated near end frame loss count - since last 'clear'.
• **Far End Loss Count**	The accumulated far end frame loss count - since last 'clear'.
• **Near End Loss Ratio**	The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.
• **Far End Loss Ratio**	The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.
• **Clear**	Set of this check and save will clear the accumulated counters and restart ratio calculation.
• **Enable**	Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.
• **Priority**	The priority to be inserted as PCP bits in TAG (if any).
• **Cast**	Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'.
• **Peer MEP**	This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

• **Way**	**One-Way**: One-Way Delay Measurement implemented on 1DM. **Two-Way**: Two-Way Delay Measurement implemented on DMM/DMR.
• **Tx Mode**	**Standardize**: Y.1731 standardize way to transmit 1DM/DMR. **Proprietary**: Vitesse proprietary way with follow-up packets to transmit 1DM/DMR.
• **Calc**	This is only used if the 'Way' is configured to Two-way. **Round trip**: The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf **Flow**: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay=(RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)
• **Gap**	The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.
• **Count**	The number of last records to calculate. The range is 10 to 2000.
• **Unit**	The time resolution.
• **D2forD1**	Enable to use DMM/DMR packet to calculate one-way DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calcualted. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.
• **Counter Overflow Action**	The action to counter when overflow happens.
• **Tx**	The accumulated transmit count - since last 'clear'.
• **Rx Timeout**	The accumulated receive timeout count for two-way only - since last 'clear'.

• **Rx**	The accumulated receive count - since last 'clear'.
• **Rx Error**	The accumulated receive error count - since last 'clear'. The frame delay is larger than 1 second(timeout).
• **Average Total**	The average delay - since last 'clear'. The unit is microsecond.
• **Average last N**	The average delay of the last n packets - since last 'clear'. The unit is microsecond.
• **Average Variation Total**	The average delay variation - since last 'clear'. The unit is microsecond.
• **Average Variation last N**	The average delay variation of the last n packets - since last 'clear'. The unit is microsecond.
• **Min.**	The minimum delay - since last 'clear'. The unit is microsecond.
• **Max.**	The maximum delay - since last 'clear'. The unit is microsecond.
• **Overflowr**	The number of counter overflow - since last 'clear'.
• **Clear**	Set of this check and save will clear the accumulated counters.
• **Far-end-to-near-end one-way delay**	The one-way delay is from remote devieces to the local devices. Here are the conditions to calculate this delay. 1. 1DM received. 2. DMM received with D2forD1 eanbled. 3. DMR received with D2forD1 eanbled.
• **Nar-end-to-near-end one-way delay**	The one-way delay is from the local devices to remote devieces. The only case to calculate this delay is below. DMR received with D2forD1 eanbled.

Buttons

Back : Click to go back to this MEP instance main page.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.1.3.2 ERPS

The Ethernet Ring Protection Switch instances are configured here.

Ethernet Ring Protection Switching Refresh

Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm

Add New Protection Group Save Reset

	object	Description
•	**Delete**	This box is used to mark an ERPS for deletion in next Save operation.
•	**Protection group ID**	The ID of the created Protection group. Click on the ID of an Protection group to enter the configuration page.
•	**Port 0**	This will create a Port 0 of the switch in the ring.
•	**Port 1**	This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance
•	**Port 0 SF MEP**	The Port 0 Signal Fail reporting MEP.
•	**Port 1 SF MEP**	The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.
•	**Port 0 APS MEP**	Type of Protecting ring. It can be either major ring or sub-ring.
•	**Port 1 APS MEP**	The Port 1 APS PDU handling MEP. As only one APS MEP

	is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.
• **Ring Type**	Type of Protecting ring. It can be either major ring or sub-ring.
• **Interconnected Node**	Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.
• **Virtual Channel**	Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.
• **Major Ring ID**	Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.
• **Alarm**	There is an active alarm on the ERPS.

Buttons

Add New Protection Group : Click to add a new Protection group entry.

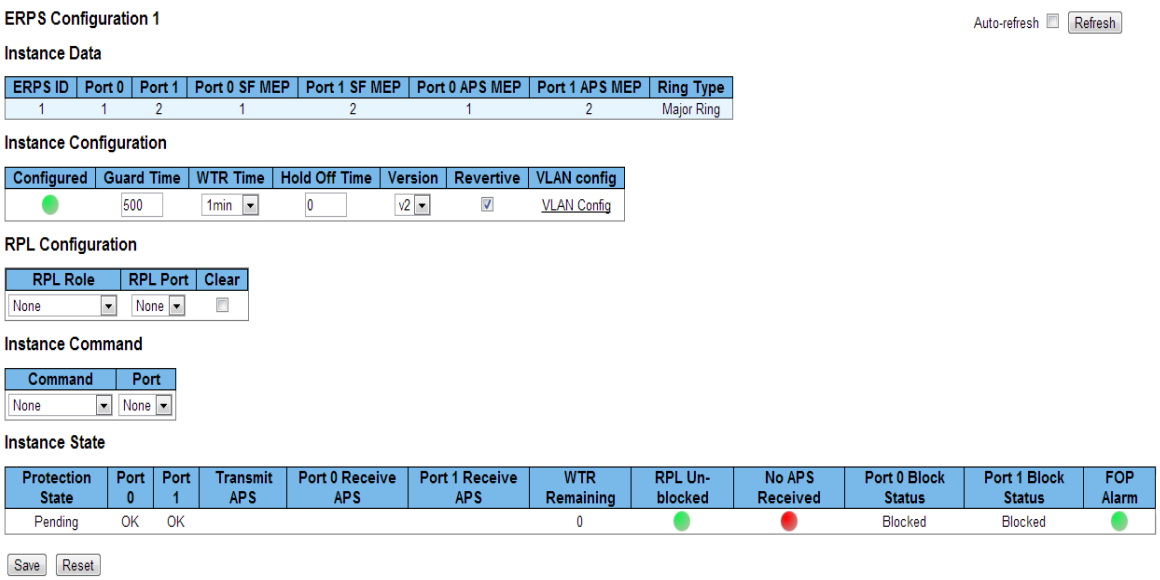
Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.1.3.2.1 ERPS configuration1

This page allows the user to inspect and configure the current ERPS Instance.



	object	Description
•	**ERPS ID**	The ID of the Protection group.
•	**Port 0**	See help on ERPS create WEB.
•	**Port 1**	See help on ERPS create WEB.
•	**Port 0 SF MEP**	See help on ERPS create WEB.
•	**Port 1 SF MEP**	See help on ERPS create WEB.
•	**Port 0 APS MEP**	See help on ERPS create WEB.
•	**Port 1 APS MEP**	See help on ERPS create WEB.
•	**Ring Type**	Type of Protecting ring. It can be either major ring or sub-ring.
•	**Configured**	**Red**: This ERPS is only created and has not yet been configured - is not active. **Green**: This ERPS is configured - is active.
•	**Guard Time**	Guard timeout value to be used to prevent ring nodes

	from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms
• **WTR Time**	The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.
• **Hold Off Time**	The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms
• **Version**	ERPS Protocol Version - v1 or v2
• **Revertive**	In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
• **VLAN config**	VLAN configuration of the Protection Group. Click on the "VLAN Config" link to confure VLANs for this protection group.
• **RPL Role**	It can be either RPL owner or RPL Neighbour.
• **RPL Port**	This allows to select the east port or west port as the RPL block.
• **Clear**	If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.
• **Topology Change**	Clicking this checkbox indicates that the topology changes in the sub-ring are propagated in the major ring.
• **Command**	Administrative command. A port can be administratively configured to be in either manual switch or forced switch

	state.
• **Forced Switch**	Forced Switch command forces a block on the ring port where the command is issued.
• **Manual Switch**	In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.
• **Clear**	The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).
• **Port**	Port selection - Port0 or Port1 of the protection Group on which the command is applied.
• **Protection State**	ERPS state according to State Transition Tables in G.8032.
• **Port 0**	**OK**: State of East port is ok **SF**: State of East port is Signal Fail
• **Port 1**	**OK**: State of West port is ok **SF**: State of West port is Signal Fail
• **Transmit APS**	The transmitted APS according to State Transition Tables in G.8032.
• **Port 0 Receive APS**	The received APS on Port 0 according to State Transition Tables in G.8032.
• **Port 1 Receive APS**	The received APS on Port 1 according to State Transition Tables in G.8032.
• **WTR Remaining**	Remaining WTR timeout in milliseconds.
• **RPL Un-blocked**	APS is received on the working flow.
• **No APS Received**	RAPS PDU is not received from the other end.
• **Port 0 Block Status**	Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
• **Port 1 Block Status**	Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
• **FOP Alarm**	Failure of Protocol Defect(FOP) status. If FOP is detected,

red LED glows; else green LED glows.

Buttons

[Refresh]: Click to refresh the page immediately.

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

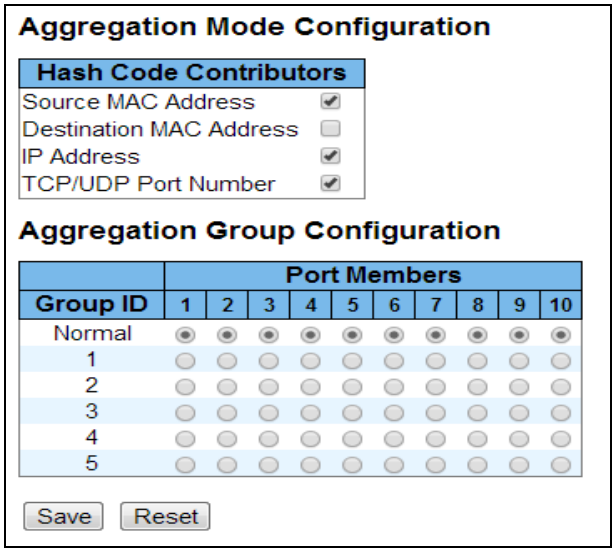
[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

5.8.2 AGGREGATION

5.8.2.1 Static

This page is used to configure the Aggregation hash mode and the aggregation group.



object	Description

• **Source MAC Address**	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
• **Destination MAC Address**	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
• **IP Address**	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
• **TCP/UDP Port Number**	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.
• **Group ID**	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
• **Port Members**	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

5.8.2.2 LACP

■ 5.8.2.2.1 configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well.

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768
9	☐	Auto		Active	Fast	32768
10	☐	Auto		Active	Fast	32768

Save Reset

object	Description
● **Port**	The switch port number.
● **LACP Enabled**	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.
● **Key**	The Key value incurred by the port, range 1-65535 . The **Auto** setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the **Specific** setting, a user-defined value can be entered. Ports with the same Key value can participate in

	the same aggregation group, while ports with different keys cannot.
• **Role**	The **Role** shows the LACP activity status. The **Active** will transmit LACP packets each second, while **Passive** will wait for a LACP packet from a partner (speak if spoken to).
• **Timeout**	The **Timeout** controls the period between BPDU transmissions. **Fast** will transmit LACP packets each second, while **Slow** will wait for 30 seconds before sending a LACP packet.
• **Prio**	The **Prio** controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

■ 5.8.2.2.2 Status

• 5.8.2.2.2.1 System Status

This page provides a status overview for all LACP instances.

LACP System Status Auto-refresh Refresh

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

object	Description
• **AGGR ID**	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
• **Partner System ID**	The system ID (MAC address) of the aggregation partner.
• **Partner Key**	The Key that the partner has assigned to this aggregation ID.
• **Partner Prio**	The time since this aggregation changed.
• **Last changed**	The time since this aggregation changed.
• **Local Ports**	Shows which ports are a part of this aggregation for this switch.

Buttons

Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

• 5.8.2.2.2.2 Port Status

This page provides a status overview for LACP status for all ports.

LACP Status Auto-refresh ☐ Refresh

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-

object	Description

• **Port**	The switch port number.
• **LACP**	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
• **Key**	The key assigned to this port. Only ports with the same key can aggregate together.
• **AGGR ID**	The Aggregation ID assigned to this aggregation group.
• **Partner System ID**	The partner's System ID (MAC address).
• **Partner Port**	The partner's port number connected to this port.
• **Partner Prio**	The partner's port priority.

Buttons

Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

Refresh : Click to refresh the page immediately.

• 5.8.2.2.2.3 Port Statistics

This page provides an overview for LACP statistics for all ports.

LACP Statistics Auto-refresh ☐ Refresh Clear

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

object	Description
• **Port**	The switch port number.
• **LACP Received**	Shows how many LACP frames have been received at each port.
• **LACP Transmitted**	Shows how many LACP frames have been sent from each port.
• **Discarded**	Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

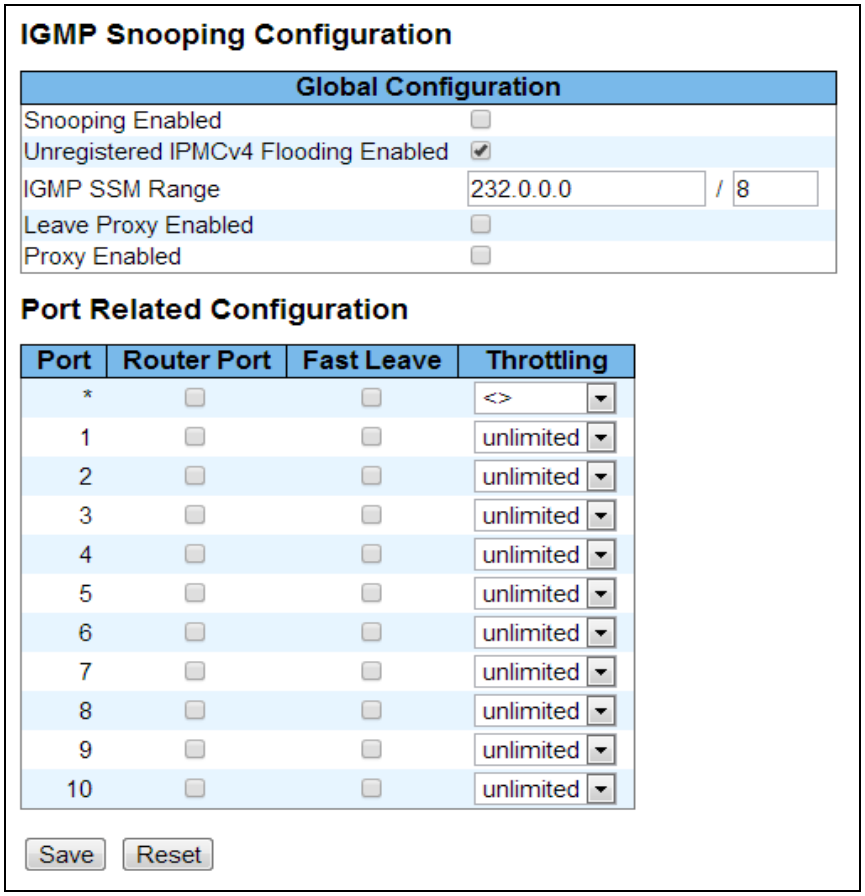
5.8.3 IPMC

5.8.3.1 IGMP Snooping

■ 5.8.3.1.1 Configuration

• 5.8.3.1.1.1 Basic Configuration

This page provides IGMP Snooping related configuration.



	object	Description
•	**Snooping Enabled**	Enable the Global IGMP Snooping.
•	**Unregistered IPMCv4 Flooding Enabled**	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.
•	**IGMP SSM Range**	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
•	**Leave Proxy Enabled**	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

• **Proxy Enabled**	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
• **Router Port**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
• **Fast Leave**	Enable the fast leave on the port.
• **Throttling**	Enable to limit the number of multicast groups to which a switch port can belong.

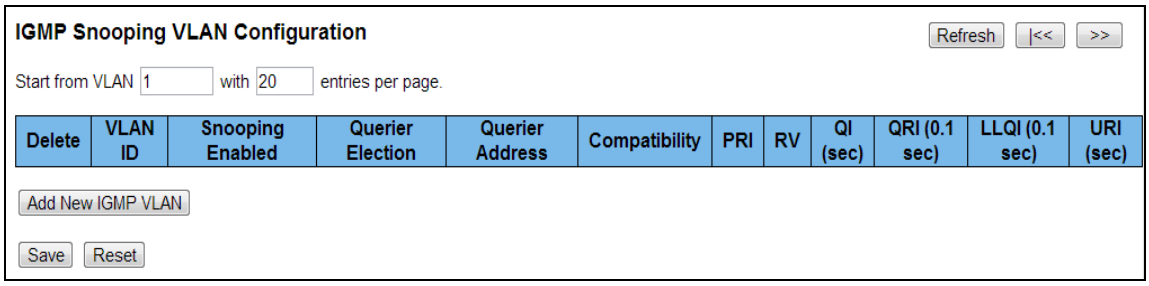
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

• 5.8.3.1.1.2 VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.



object	Description
• **Delete**	Check to delete the entry. The designated entry will be deleted during the next save.
• **VLAN ID**	The VLAN ID of the entry.
• **IGMP Snooping Enabled**	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
• **Querier Election**	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
• **Querier Address**	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
• **Compatibility**	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is **IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3**, default compatibility value is IGMP-Auto.
• **PRI**	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is **0** (best effort) to **7** (highest), default interface priority value is 0.
• **RV**	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is **1** to **255**, default robustness

	variable value is 2.
• **QI**	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is **1** to **31744** seconds, default query interval is 125 seconds.
• **QRI**	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is **0** to **31744** in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
• **LLQI**	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is **0** to **31744** in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).
• **URI**	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is **0** to **31744** seconds, default unsolicited report interval is 1 second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

<< : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

>> : Updates the table, starting with the entry after the last entry currently displayed.

Add New IGMP VLAN: Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

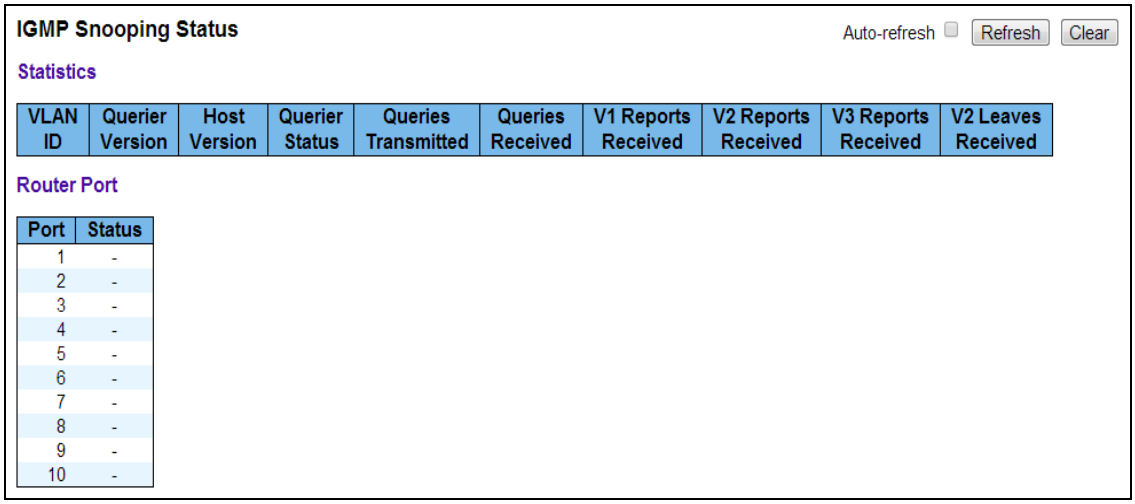
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.3.1.2 Status

5.8.3.1.2.1 Status

This page provides IGMP Snooping status.



object	Description
• VLAN ID	The VLAN ID of the entry.
• Querier Version	Working Querier Version currently.

• **Host Version**	Working Host Version currently.
• **Querier Status**	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
• **Queries Transmitted**	The number of Transmitted Queries.
• **Queries Received**	The number of Received Queries.
• **V1 Reports Received**	The number of Received V1 Reports.
• **V2 Reports Received**	The number of Received V2 Reports.
• **V3 Reports Received**	The number of Received V3 Reports.
• **V2 Leaves Received**	The number of Received V2 Leaves.
• **Router Port**	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
• **Port**	Switch port number.
• **Status**	Indicate whether specific port is a router port or not.

Buttons

Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

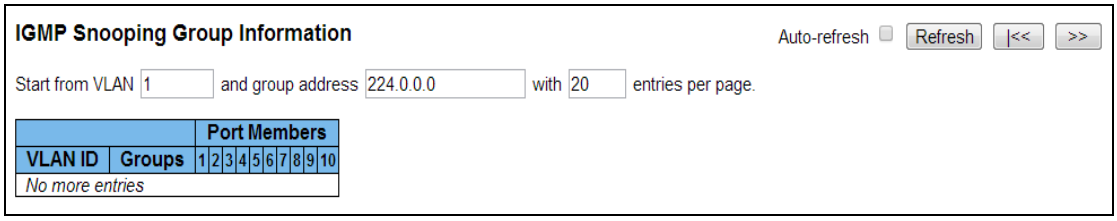
Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

5.8.3.1.2.2 Groups Information

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by

group.



object	Description
• VLAN ID	VLAN ID of the group.
• Group	Group address of the group displayed.
• Port Members	Ports under this group.

Buttons

Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

<<: Updates the table, starting with the first entry in the IGMP Group Table.

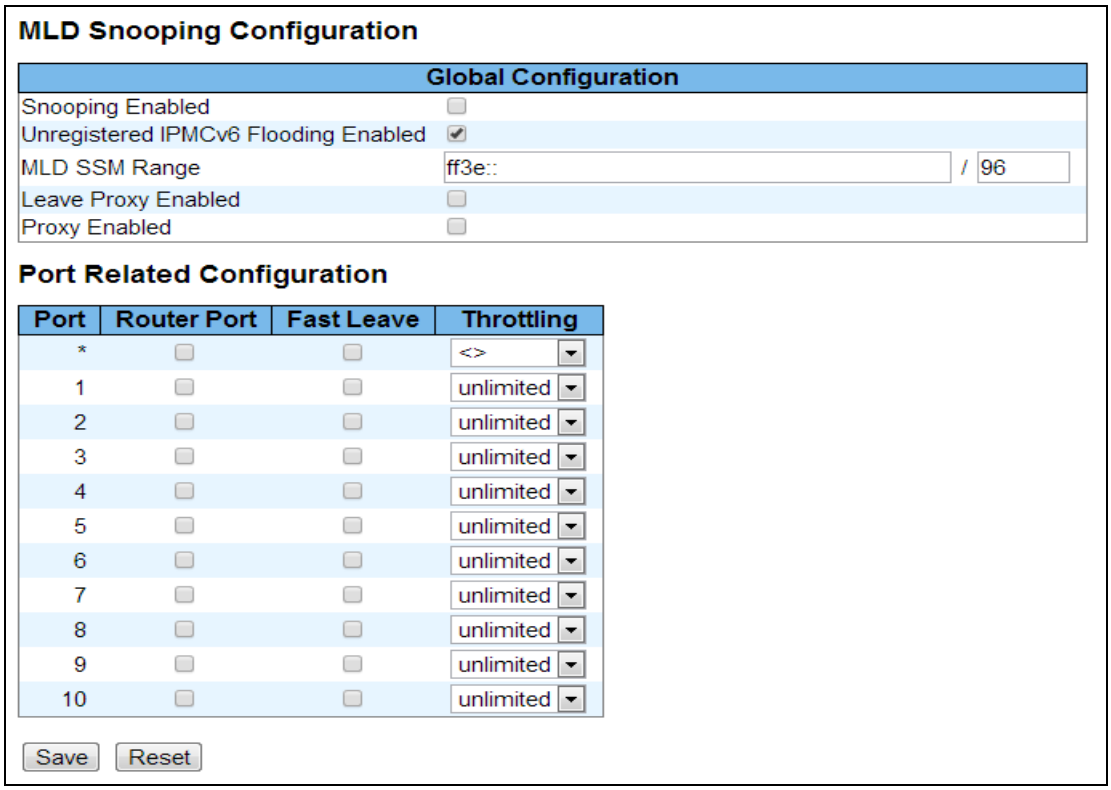
>>: Updates the table, starting with the entry after the last entry currently displayed.

5.8.3.2 MLD Snooping

5.8.3.2.1 Configuration

5.8.3.2.1.1 Basic Configuration

This page provides MLD Snooping related configuration.



	object	Description
•	**Snooping Enabled**	Enable the Global MLD Snooping.
•	**Unregistered IPMCv6 Flooding Enabled**	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.
•	**MLD SSM Range**	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
•	**Leave**	Enable MLD Leave Proxy. This feature can be used to

	Proxy Enabled	avoid forwarding unnecessary leave messages to the router side.
•	**Proxy Enabled**	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
•	**Router Port**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
•	**Fast Leave**	Enable the fast leave on the port.
•	**Throttling**	Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

• 5.8.3.2.1.2 VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

MLD Snooping VLAN Configuration Refresh |<< >>

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)

Add New MLD VLAN

Save Reset

object	Description
• **Delete**	Check to delete the entry. The designated entry will be deleted during the next save.
• **VLAN ID**	The VLAN ID of the entry.
• **MLD Snooping Enabled**	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
• **Querier Election**	Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier. Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.
• **Compatibility**	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is **MLD-Auto, Forced MLDv1, Forced MLDv2**, default compatibility value is MLD-Auto.
• **PRI**	Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is **0** (best effort) to **7** (highest), default interface priority value is 0.
• **RV**	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is **1** to **255**, default robustness variable value is 2.

• **QI**	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is **1** to **31744** seconds, default query interval is 125 seconds.
• **QRI**	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is **0** to **31744** in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).
• **LLQI**	Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is **0** to **31744** in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).
• **URI**	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is **0** to **31744** seconds, default unsolicited report interval is 1 second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

[<<]: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

[>>]: Updates the table, starting with the entry after the last entry currently displayed.

[Add New MLD VLAN]: Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.

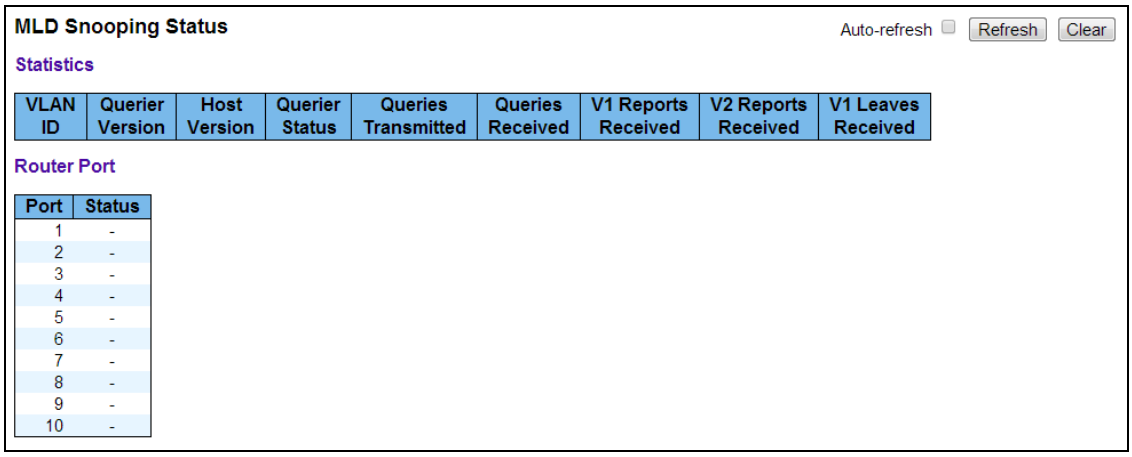
[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

■ 5.8.3.2.2 Status

● 5.8.3.2.2.1 Status

This page provides MLD Snooping status.



object	Description

• **VLAN ID**	The VLAN ID of the entry.
• **Querier Version**	Working Querier Version currently.
• **Host Version**	Working Host Version currently.
• **Querier Status**	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
• **Queries Transmitted**	The number of Transmitted Queries.
• **Queries Received**	The number of Received Queries.
• **V1 Reports Received**	The number of Received V1 Reports.
• **V2 Reports Received**	The number of Received V2 Reports.
• **V1 Leaves Received**	The number of Received V1 Leaves.
• **Router Port**	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
• **Port**	Switch port number.
• **Status**	Indicate whether specific port is a router port or not.

Buttons

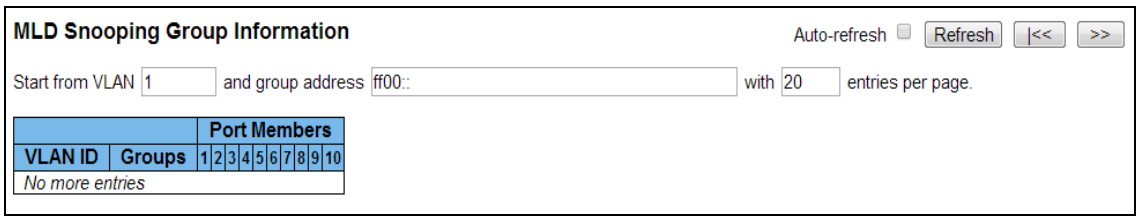
Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

Refresh : Click to refresh the page immediately.

Clear: Clears all Statistics counters.

5.8.3.2.2.2 Groups Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.



object	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port Members	Ports under this group.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

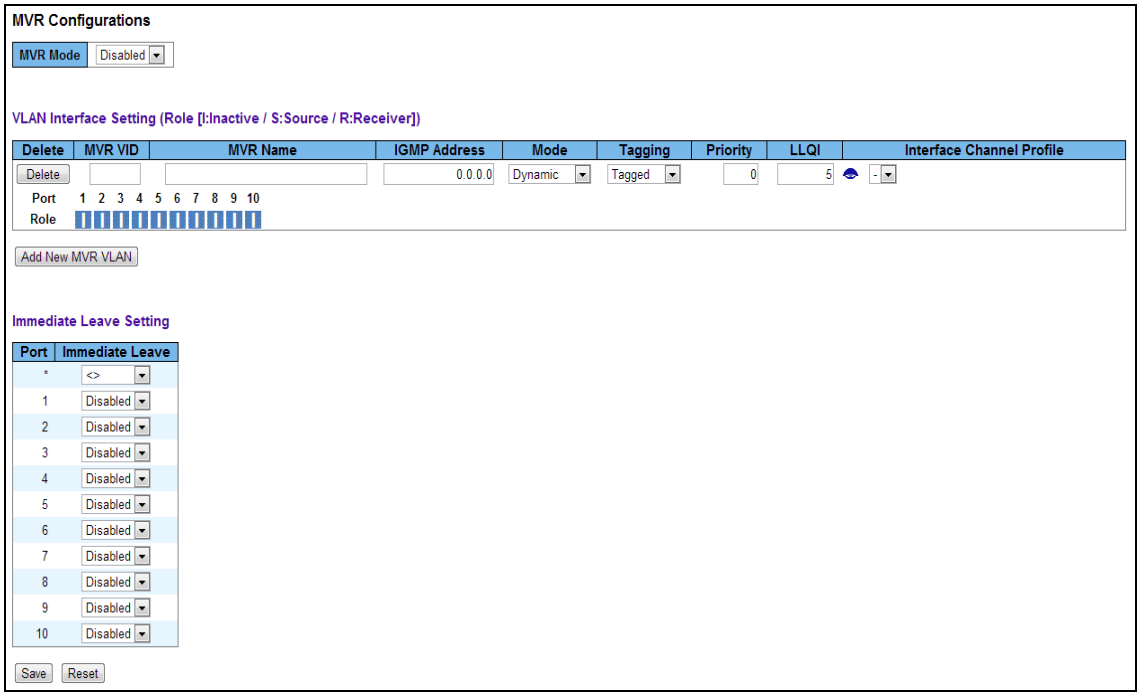
<<: Updates the table, starting with the first entry in the MLD Group Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5.8.3.3 MVR

■ 5.8.3.3.1 Configuration

This page provides MVR related configurations.



object	Description
● **MVR Mode**	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.
● **Delete**	Check to delete the entry. The designated entry will be deleted during the next save.
● **MVR VID**	Specify the Multicast VLAN ID. Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

• **MVR Name**	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
• **IGMP Address**	Define the IPv4 address as source address used in IP header for IGMP control frames. When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
• **Mode**	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
• **Tagging**	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
• **Priority**	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
• **LLQI**	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
• **Interface Channel Profile**	When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view

	button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.
• **Profile Management Button**	You can inspect the rules of the designated profile by using the following button: : List the rules associated with the designated profile.
• **Port**	The logical port for the settings.
• **Port Role**	Configure an MVR port of the designated MVR VLAN as one of the following roles. **Inactive**: The designated port does not participate MVR operations. **Source**: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. **Receiver**: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. **Be Caution**: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver The default Role is Inactive.
• **Immediate Leave**	Enable the fast leave on the port.

Buttons

Add New MVR VLAN: Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save".

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.3.3.2 Statistics

This page provides MVR Statistics information.

MVR Statistics Auto-refresh Refresh Clear

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
No more entries						

object	Description
• **VLAN ID**	The Multicast VLAN ID.
• **IGMP/MLD Queries Received**	The number of Received Queries for IGMP and MLD, respectively.
• **IGMP/MLD Queries Transmitted**	The number of Transmitted Queries for IGMP and MLD, respectively.
• **IGMPv1 Joins Received**	The number of Received IGMPv1 Join's.
• **IGMPv2/MLDv1 Report's Received**	The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.
• **IGMPv3/MLDv2 Report's Received**	The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.
• **IGMPv2/MLDv1 Leave's Received**	The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

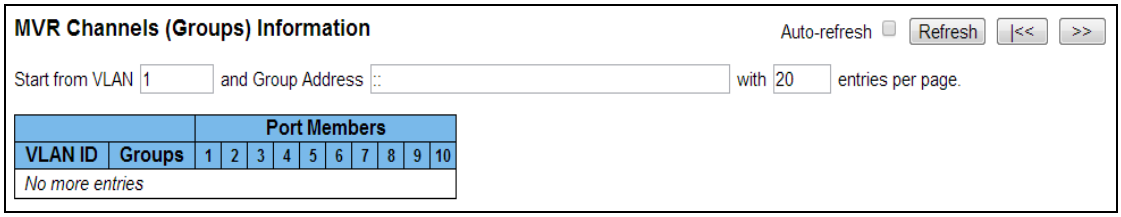
Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

■ 5.8.3.3.3 MVR Channel Groups

Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.



object	Description
● **VLAN ID**	VLAN ID of the group.
● **Groups**	Group ID of the group displayed.
● **Port Members**	Ports under this group.t

Buttons

Auto-refresh ☐ : Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

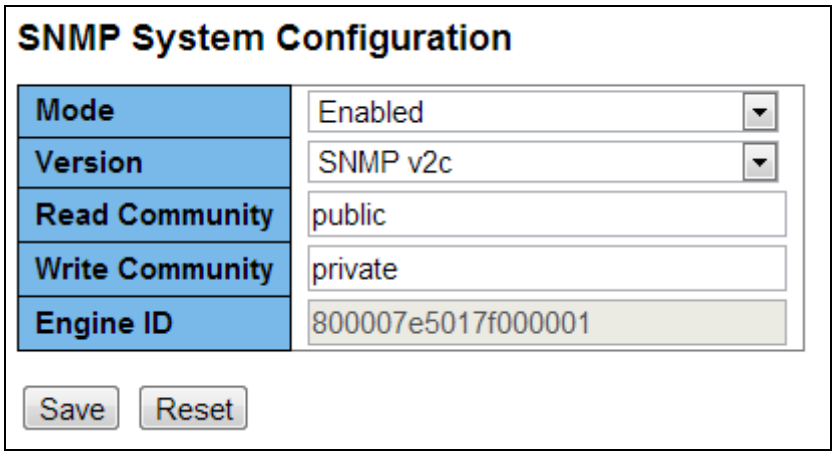
<<: Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5.8.4 SNMP

5.8.4.1 System

Configure SNMP on this page.



object	Description
• **Mode**	Indicates the SNMP mode operation. Possible modes are: **Enabled**: Enable SNMP mode operation. **Disabled**: Disable SNMP mode operation.
• **Version**	Indicates the SNMP supported version. Possible versions are: **SNMP v1**: Set SNMP supported version 1. **SNMP v2c**: Set SNMP supported version 2c. **SNMP v3**: Set SNMP supported version 3.
• **Read Community**	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
• **Write Community**	Indicates the community write access string to permit

	access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
• **Engine ID**	Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

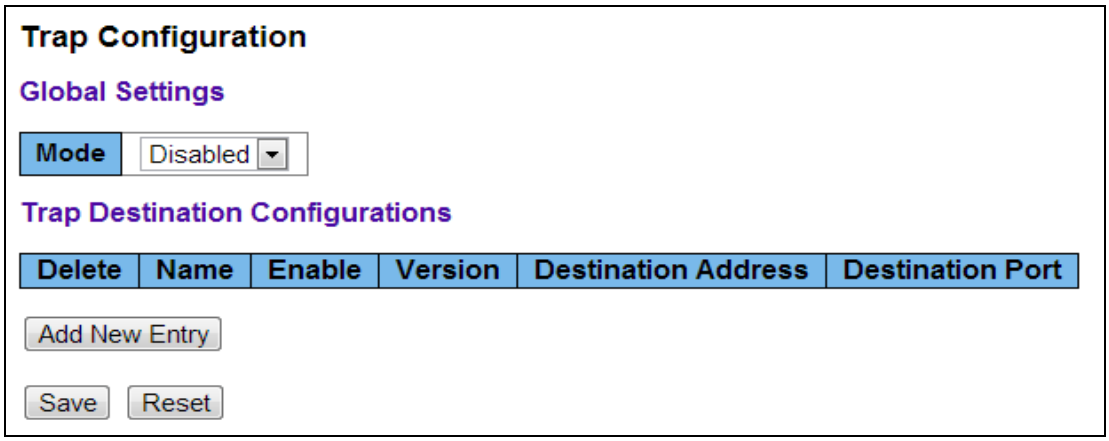
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.4.2 Trap

Configure SNMP trap on this page.



object	Description
• **Mode**	Indicates the trap mode operation. Possible modes are: **Enabled**: Enable SNMP trap mode operation. **Disabled**: Disable SNMP trap mode operation.
• **Name**	Indicates the trap Configuration's name. Indicates the trap destination's name.
• **Enable**	Indicates the trap destination mode operation. Possible modes are: **Enabled**: Enable SNMP trap mode operation. **Disabled**: Disable SNMP trap mode operation.
• **Version**	Indicates the SNMP trap supported version. Possible versions are: **SNMPv1**: Set SNMP trap supported version 1. **SNMPv2c**: Set SNMP trap supported version 2c. **SNMPv3**: Set SNMP trap supported version 3.
• **Trap Community**	Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.
• **Destination Address**	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character

	must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
• **Destination port**	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

Buttons

Add New Entry : Click to add a new user.

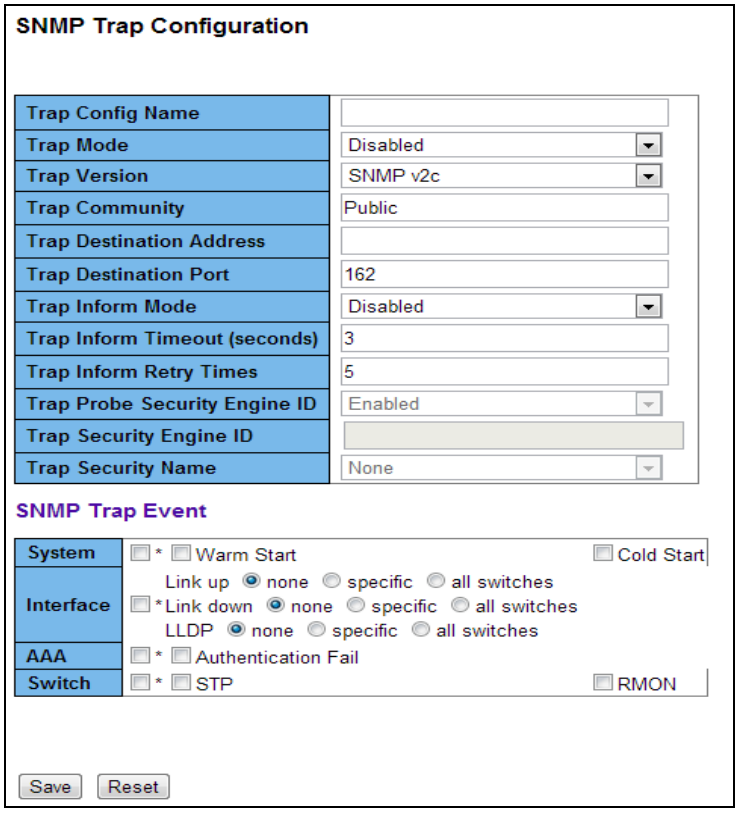
Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

5.8.4.2.1 SNMP Trap Configuration

When push 'Add New Entry' button, Trap setting page will be displayed.

Configure trap detailed configuration on this page.



object	Description
• **Trap Config Name**	Indicates which trap Configuration's name for configureing.
• **Enable**	Indicates the SNMP mode operation. Possible modes are: **Enabled**: Enable SNMP mode operation. **Disabled**: Disable SNMP mode operation.
• **Version**	Indicates the SNMP supported version. Possible versions are: **SNMP v1**: Set SNMP supported version 1. **SNMP v2c**: Set SNMP supported version 2c. **SNMP v3**: Set SNMP supported version 3.
• **Destination Address**	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character

	must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
• **Destination port**	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.
• **Trap Inform Mode**	Indicates the SNMP trap inform mode operation. Possible modes are: **Enabled**: Enable SNMP trap inform mode operation. **Disabled**: Disable SNMP trap inform mode operation.
• **Trap Inform Timeout (seconds)**	Indicates the SNMP trap inform timeout. The allowed range is **0** to **2147**.
• **Trap Inform Retry Times**	Indicates the SNMP trap inform retry times. The allowed range is **0** to **255**.
• **Trap Probe Security Engine ID**	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: **Enabled**: Enable SNMP trap probe security engine ID mode of operation. **Disabled**: Disable SNMP trap probe security engine ID mode of operation.
• **Trap Security Engine ID**	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format)

	with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
• **Trap Security Name**	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.
• **System**	Enable/disable that the Interface group's traps. Possible traps are: **Warm Start**: Enable/disable Warm Start trap. **Cold Start**: Enable/disable Cold Start trap.
• **Interface**	Indicates that the Interface group's traps. Possible traps are: Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: **Warm Start**: Enable SNMP trap authentication failure. **Link Up**: Enable/disable Link up trap. **Link Down**: Enable/disable Link down trap. **LLDP**: Enable/disable LLDP trap.
• **AAA**	Indicates that the AAA group's traps. Possible traps are: **Authentication Fail** : Enable/disable SNMP trap authentication failure trap.
• **Switch**	Indicates that the Switch group's traps. Possible traps are: **STP**: Enable/disable STP trap. **RMON**: Enable/disable RMON trap.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.4.3 Communities

Configure SNMPv3 community table on this page. The entry index key is **Community**.

SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
☐	public	0.0.0.0	0.0.0.0
☐	private	0.0.0.0	0.0.0.0

Add New Entry Save Reset

object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Community**	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
• **Source IP**	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
• **Source Mask**	Indicates the SNMP access source address mask.

Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.4.4 Users

Configure SNMPv3 user table on this page. The entry index keys are **Engine ID** and **User Name**.

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Add New Entry Save Reset

object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Engine ID**	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
• **User Name**	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are:

	NoAuth, NoPriv: No authentication and no privacy. **Auth, NoPriv**: Authentication and no privacy. **Auth, Priv**: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.
• **Authentication Protocol**	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: **None**: No authentication protocol. **MD5**: An optional flag to indicate that this user uses MD5 authentication protocol. **SHA**: An optional flag to indicate that this user uses SHA authentication protocol. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
• **Authentication Password**	A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.
• **Privacy Protocol**	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: **None**: No privacy protocol. **DES**: An optional flag to indicate that this user uses DES authentication protocol. **AES**: An optional flag to indicate that this user uses AES authentication protocol.
• **Privacy Password**	A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add New Entry : Click to add a new user entry.

Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

5.8.4.5 Groups

Configure SNMPv3 group table on this page. The entry index keys are **Security Model** and **Security Name**.

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group

Add New Entry Save Reset

object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Security Model**	Indicates the security model that this entry should belong to. Possible security models are: **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based Security Model (USM).
• **Security Name**	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to

	126.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

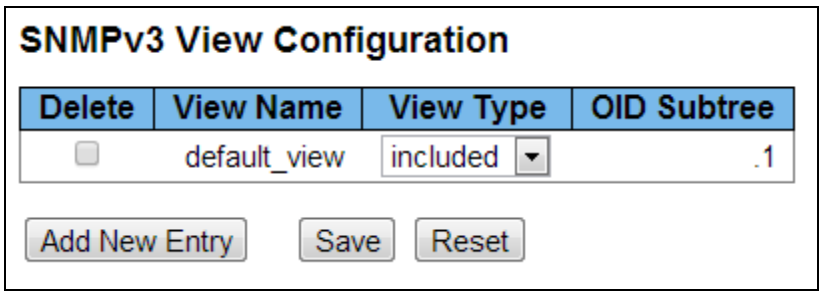
Add New Entry: Click to add a new group entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.8.4.6 Views

Configure SNMPv3 view table on this page. The entry index keys are **View Name** and **OID Subtree**.



object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **View Name**	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

• **View Type**	Indicates the view type that this entry should belong to. Possible view types are: **included**: An optional flag to indicate that this view subtree should be included. **excluded**: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.
• **OID Subtree**	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

Add New Entry : Click to add a new view entry.

Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

5.8.4.7 Access

Configure SNMPv3 access table on this page. The entry index keys are **Group Name, Security Model** and **Security Level**.

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view	None
☐	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

Add New Entry Save Reset

object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
• **Security Model**	Indicates the security model that this entry should belong to. Possible security models are: **any**: Any security model accepted(v1|v2c|usm). **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based Security Model (USM).
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are: **NoAuth, NoPriv**: No authentication and no privacy. **Auth, NoPriv**: Authentication and no privacy. **Auth, Priv**: Authentication and privacy.
• **Read View Name**	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
• **Write View Name**	The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add New Entry : Click to add a new access entry..

Save : Click to save changes.

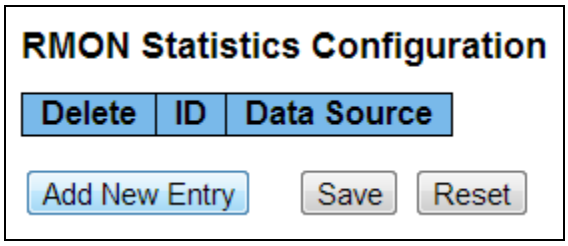
Reset : Click to undo any changes made locally and revert to previously saved values.

5.8.5 RMON

5.8.5.1 Configuration

5.8.5.1.1 Statistics

Configure RMON Statistics table on this page. The entry index key is **ID**.



object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Data Source**	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons

Add New Entry : Click to add a new community entry.

Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

5.8.5.1.2 History

Configure RMON History table on this page. The entry index key is **ID**.

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted

Add New Entry Save Reset

object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Data Source**	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.
• **Interval**	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
• **Buckets**	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from

	1 to 3600, default value is 50.
• **Buckets Granted**	The number of data shall be saved in the RMON.

Buttons

Add New Entry : Click to add a new community entry.

Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

■ 5.8.5.1.3 Alarm

Configure RMON Alarm table on this page. The entry index key is **ID**.

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index

Add New Entry Save Reset

object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Interval**	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
• **Variable**	Indicates the particular variable to be sampled, the possible variables are: **InOctets**: The total number of octets received on the

	interface, including framing characters. **InUcastPkts**: The number of uni-cast packets delivered to a higher-layer protocol. **InNUcastPkts**: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. **InDiscards**: The number of inbound packets that are discarded even the packets are normal. **InErrors**: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. **InUnknownProtos**: the number of the inbound packets that were discarded because of the unknown or un-support protocol. **OutOctets**: The number of octets transmitted out of the interface , including framing characters. **OutUcastPkts**: The number of uni-cast packets that request to transmit. **OutNUcastPkts**: The number of broad-cast and multi-cast packets that request to transmit. **OutDiscards**: The number of outbound packets that are discarded event the packets is normal. **OutErrors**: The The number of outbound packets that could not be transmitted because of errors. **OutQLen**: The length of the output packet queue (in packets).
• **Sample Type**	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: **Absolute**: Get the sample directly. **Delta**: Calculate the difference between samples (default).
• **Value**	The value of the statistic during the last sampling period.
• **Startup Alarm**	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

	RisingTrigger alarm when the first value is larger than the rising threshold. **Falling**Trigger alarm when the first value is less than the falling threshold. **RisingOrFallingTrigger** alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
• **Rising Threshold**	Rising threshold value (-2147483648-2147483647).
• **Rising Index**	Rising event index (1-65535).
• **Falling Threshold**	Falling threshold value (-2147483648-2147483647)
• **Falling Index**	Falling event index (1-65535).

Buttons

Add New Entry : Click to add a new community entry.

Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

5.8.5.1.4 Event

Configure RMON Event table on this page. The entry index key is **ID**.

RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time

Add New Entry Save Reset

object	Description

• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Desc**	Indicates this event, the string length is from 0 to 127, default is a null string.
• **Type**	Indicates the notification of the event, the possible types are: **none**: The total number of octets received on the interface, including framing characters. **log** The number of uni-cast packets delivered to a higher-layer protocol. **snmptrap**: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. **logandtrap**: The number of inbound packets that are discarded even the packets are normal.
• **Community**	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".
• **Event Last Time**	Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

Add New Entry : Click to add a new community entry.

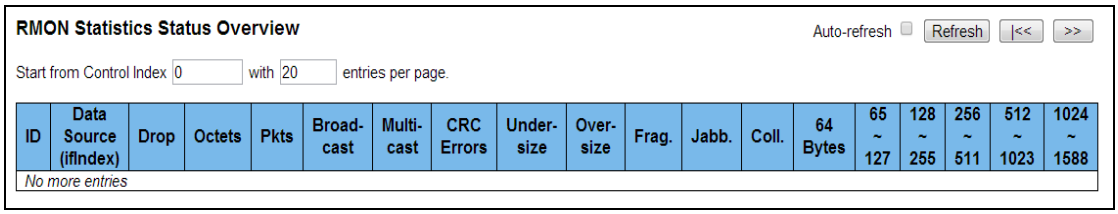
Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

5.8.5.2 Status

5.8.5.2.1 Statistics

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.



object	Description
• ID	Indicates the index of Statistics entry.
• Data Source(ifIndex)	The port ID which wants to be monitored.
• Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
• Octets	The total number of octets of data (including those in bad packets) received on the network.
• Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• Broad-cast	The total number of good packets received that were directed to the broadcast address.
• Multi-cast	The total number of good packets received that were directed to a multicast address.
• CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of

	between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
• **Under-size**	The total number of packets received that were less than 64 octets.
• **Over-size**	The total number of packets received that were longer than 1518 octets.
• **Frag**	The number of frames which size is less than 64 octets received with invalid CRC.
• **Jabb**	The number of frames which size is larger than 64 octets received with invalid CRC.
• **Coll.**	The best estimate of the total number of collisions on this Ethernet segment.
• **64 Byte**	The total number of packets (including bad packets) received that were 64 octets in length.
• **65~127**	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
• **128~255**	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
• **256~511**	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
• **512~1023**	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
• **1024~1588**	The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

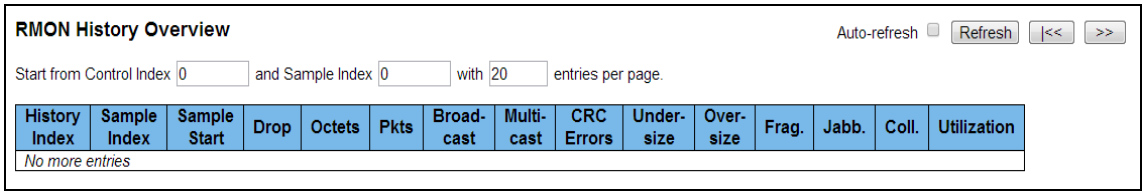
Refresh: Click to refresh the page immediately.

|<< : Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

>> : Updates the table, starting with the entry after the last entry currently displayed.

5.8.5.2.2 History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.



object	Description
• **History Index**	Indicates the index of History control entry.
• **Sample Index**	Indicates the index of the data entry associated with the control entry.
• **Sample Start**	The value of sysUpTime at the start of the interval over which this sample was measured.
• **Drop**	The total number of events in which packets were dropped by the probe due to lack of resources.
• **Octets**	The total number of octets of data (including those in bad packets) received on the network.
• **Pkts**	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

• **Broadcast**	The total number of good packets received that were directed to the broadcast address.
• **Multicast**	The total number of good packets received that were directed to a multicast address.
• **CRCErrors**	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
• **Undersize**	The total number of packets received that were less than 64 octets.
• **Oversize**	The total number of packets received that were longer than 1518 octets.
• **Frag.**	The number of frames which size is less than 64 octets received with invalid CRC.
• **Jabb.**	The number of frames which size is larger than 64 octets received with invalid CRC.
• **Coll.**	The best estimate of the total number of collisions on this Ethernet segment.
• **Utilization**	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

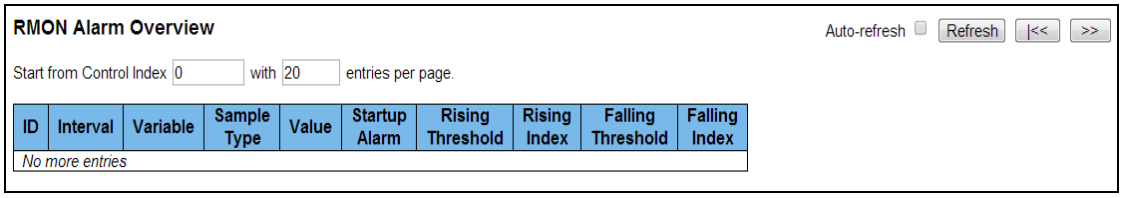
[Refresh]: Click to refresh the page immediately.

[<<]: Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index

[>>]: Updates the table, starting with the entry after the last entry currently displayed.

5.8.5.2.3 Alarm

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.



object	Description
● **ID**	Indicates the index of Alarm control entry.
● **Interval**	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
● **Variable**	Indicates the particular variable to be sampled
● **Sample Type**	The method of sampling the selected variable and calculating the value to be compared against the thresholds. The method of sampling the selected variable and calculating the value to be compared against the thresholds.
● **Value**	The value of the statistic during the last sampling period.
● **Startup Alarm**	The alarm that may be sent when this entry is first set to valid.
● **Rising Threshold**	Rising threshold value.
● **Rising Index**	Rising event index.
● **Falling Threshold**	Falling threshold value.
● **Falling Index**	Falling event index.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

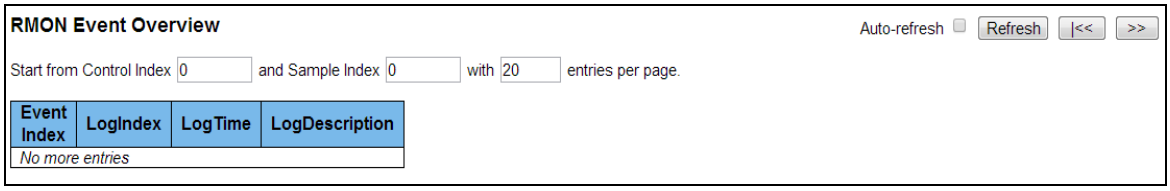
Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5.8.5.2.4 Event

This page provides an overview of RMON Event table entries.Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table table.



object	Description
• **Event Index**	Indicates the index of the event entry.
• **Log Index**	Indicates the index of the log entry.
• **LogTIme**	Indicates Event log time
• **LogDescription**	Indicates the Event description.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

<< : Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.

>> : Updates the table, starting with the entry after the last entry currently displayed.

5.8.6 DISCOVERY PROTOCOLS

5.8.6.1 LLDP

■ 5.8.6.1.1 Configuration

● 5.8.6.1.1.1 LLDP

This page allows the user to inspect and configure the current LLDP port settings.

LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Port Configuration

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☐	☐	☐	☐	☐
1	Disabled	☐	☑	☑	☑	☑	☑
2	Disabled	☐	☑	☑	☑	☑	☑
3	Disabled	☐	☑	☑	☑	☑	☑
4	Disabled	☐	☑	☑	☑	☑	☑
5	Disabled	☐	☑	☑	☑	☑	☑
6	Disabled	☐	☑	☑	☑	☑	☑
7	Disabled	☐	☑	☑	☑	☑	☑
8	Disabled	☐	☑	☑	☑	☑	☑
9	Disabled	☐	☑	☑	☑	☑	☑
10	Disabled	☐	☑	☑	☑	☑	☑

Save Reset

object	Description
• **Tx Interval**	The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.
• **Tx Hold**	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.
• **Tx Delay**	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192

	seconds.
• **Tx Reinit**	When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.
• **Port**	The switch port number of the logical LLDP port.
• **Mode**	Select LLDP mode. **Rx only** The switch will not send out LLDP information, but LLDP information from neighbour units is analyzed. **Tx only** The switch will drop LLDP information received from neighbours, but will send out LLDP information. **Disabled** The switch will not send out LLDP information, and will drop LLDP information received from neighbours. **Enabled** The switch will send out LLDP information, and will analyze LLDP information received from neighbours.
• **CDP Aware**	Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbours' table as shown below.CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbours table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field. Both the

	CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbours' table. If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbour devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch. Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.
• **Port Descr**	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
• **Sys Name**	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
• **Sys Descr**	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
• **Sys Capa**	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.
• **Mgmt Addr**	Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

• 5.8.6.1.1.2 LLDP-MED

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4

Coordinates Location

Latitude	0	°	North	Longitude	0	°	East	Altitude	0	Meters	Map Datum	WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighbourhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service	

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Add New Policy

Save Reset

object	Description
• **Fast start repeat count**	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.
• **Latitude**	Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.
• **Longitude**	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.

	It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.
• **Altitude**	Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). **Meters**: Representing meters of Altitude defined by the vertical datum specified. **Floors**: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
• **Map Datum**	The Map Datum is used for the coordinates given in these options: **WGS84**: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. **NAD83/NAVD88**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). **NAD83/MLLW**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.
• **Country code**	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
• **State**	National subdivisions (state, canton, region, province, prefecture).
• **County**	County, parish, gun (Japan), district.

• **City**	City, township, shi (Japan) - Example: Copenhagen.
• **City district**	City division, borough, city district, ward, chou (Japan).
• **Block (Neighbourhood)**	Neighbourhood, block.
• **Street**	Street - Example: Poppelvej.
• **Leading street direction**	Leading street direction - Example: N.
• **Trailing street suffix**	Trailing street suffix - Example: SW.
• **Street suffix**	Street suffix - Example: Ave, Platz.
• **House no.**	House number - Example: 21.
• **suffix**	House number suffix - Example: A, 1/2.
• **Landmark**	Landmark or vanity address - Example: Columbia University.
• **Additional location info**	Additional location info - Example: South Wing.
• **Name**	Name (residence and office occupant) - Example: Flemming Jahn.
• **Zip code**	Postal/zip code - Example: 2791.
• **Building**	Building (structure) - Example: Low Library.
• **Apartment**	Unit (Apartment, suite) - Example: Apt 42.
• **Floor**	Floor - Example: 4.
• **Room no.**	Room number - Example: 450F.
• **Place type**	Place type - Example: Office.
• **Postal community name**	Postal community name - Example: Leonia.
• **P.O. Box**	Post office box (P.O. BOX) - Example: 12345.
• **Additional code**	Additional code - Example: 1320300003.

• **Emergency Call Service**	Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.
• **Delete**	Check to delete the policy. It will be deleted during the next save.
• **Policy ID**	ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.
• **Application Type**	Intended use of the application types: **1. Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. **2. Voice Signalling (conditional)** - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. **3. Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. **4. Guest Voice Signalling (conditional)** - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy. **5. Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops.

	This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. **6. Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. **7. Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. **8. Video Signalling (conditional)** - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
• **Tag**	Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format

	also includes priority tagged frames as defined by IEEE 802.1Q-2003.
• **VLAN ID**	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.
• **L2 Priority**	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
• **DSCP**	DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
• **Add New Policy**	Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save". The number of policies supported is 32
• **Port**	The port number to which the configuration applies.
• **Policy Id**	The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons

[Add New Policy]: Click to add a new policy.

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

5.8.6.1.2 Status

5.8.6.1.2.1 Neighbours

This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. The columns hold the following information:

LLDP Neighbour Information Auto-refresh Refresh

LLDP Remote Device Summary						
Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbour information found						

object	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbour's LLDP frames.
Port ID	The Port ID is the identification of the neighbour port.
Port Description	Port Description is the port description advertised by the neighbour unit.
System Name	System Name is the name advertised by the neighbour unit.
System Capabilities	System Capabilities describes the neighbour unit's capabilities. The possible capabilities are: **1. Other** **2. Repeater** **3. Bridge** **4. WLAN Access Point** **5. Router** **6. Telephone** **7. DOCSIS cable device** **8. Station only**

	9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
• **Management Address**	Management Address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbour's IP address.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

• 5.8.6.1.2.2 LLDP-MED Neighbours

This page provides a status overview of all LLDP-MED neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

LLDP-MED Neighbour Information Auto-refresh ☐ Refresh

Local Port
No LLDP-MED neighbour information found

object	Description
• **Port**	The port on which the LLDP frame was received.
• **Device Type**	LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

• **LLDP-MED Capabilities**	LLDP-MED Capabilities describes the neighbour unit's LLDP-MED capabilities. The possible capabilities are: 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE 5. Extended Power via MDI - PD 6. Inventory 7. Reserved
• **Application Type**	Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below. **1. Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. **2. Voice Signalling** - for use in network topologies that require a different policy for the voice signalling than for the voice media. **3. Guest Voice** - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. **4. Guest Voice Signalling** - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. **5. Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. **6. Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. **7. Streaming Video** - for use by broadcast or multicast

	based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. **8. Video Signalling** - for use in network topologies that require a separate policy for the video signalling than for the video media.
• **Policy**	Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown Unknown: The network policy for the specified application type is currently unknown. Defined: The network policy is defined.
• **TAG**	TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged. Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. Tagged: The device is using the IEEE 802.1Q tagged frame format.
• **VLAN ID**	VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
• **Priority**	Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
• **DSCP**	DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as

	defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
• **Auto-negotiation**	Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.
• **Auto-negotiation status**	Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
• **Auto-negotiation Capabilities**	Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh : Click to refresh the page.

• 5.8.6.1.2.3 EEE

This page provides an overview of EEE information exchanged by LLDP.

LLDP Neighbors EEE Information Auto-refresh ☐ Refresh

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
No LLDP EEE information found								

object	Description
• **Local Port**	The port on which LLDP frames are received or transmitted.
• **Tx Tw**	The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.

• **Rx Tw**	The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.
• **Fallback Receive Tw**	The link partner's fallback receive Tw. A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.
• **Echo Tx Tw**	The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.
• **Echo Rx Tw**	The link partner's Echo Rx Tw value.
• **Resolved Tx Tw**	The resolved Tx Tw for this link. Note : NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).
• **Resolved Rx Tw**	The resolved Rx Tw for this link. Note : NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

• **EEE in Sync**	Shows whether the switch and the link partner have agreed on wake times. Red - Switch and link partner have not agreed on wakeup times. Green - Switch and link partner have agreed on wakeup times.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

• 5.8.6.1.2.4 Port Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch.

LLDP Global Counters

Auto-refresh ☐ Refresh Clear

Global Counters	
Neighbour entries were last changed	1970-01-01T00:00:00+00:00 (82941 secs. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics Local Counters

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

object	Description
• **Neighbour entries were last changed**	Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
• **Total Neighbours Entries Added**	Shows the number of new entries added since switch reboot.
• **Total Neighbours Entries Deleted**	Shows the number of new entries deleted since switch reboot.
• **Total Neighbours Entries Dropped**	Shows the number of LLDP frames dropped due to the entry table being full.
• **Total Neighbours Entries Aged Out**	Shows the number of entries deleted due to Time-To-Live expiring.
• **Local Port**	The port on which LLDP frames are received or transmitted.
• **Tx Frames**	The number of LLDP frames transmitted on the port.
• **Rx Frames**	The number of LLDP frames received on the port.
• **Rx Errors**	The number of received LLDP frames containing some kind of error.
• **Frames Discarded**	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.
• **TLVs Discarded**	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
• **TLVs Unrecognized**	The number of well-formed TLVs, but with an unknown type value.

• **Discarded**	The number of organizationally received TLVs.
• **Age-Outs**	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Buttons

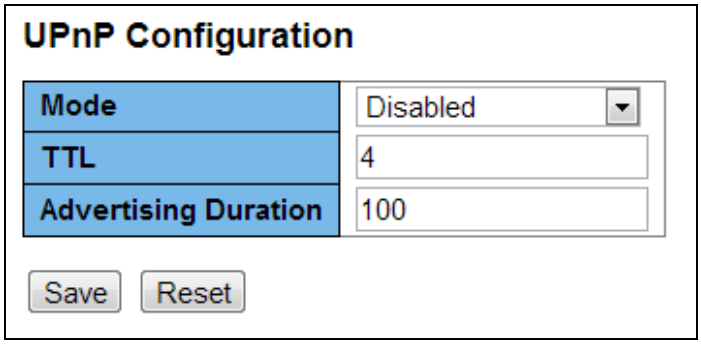
Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

[Refresh]: Click to refresh the page.

[Clear]: Clears the local counters. All counters (including global counters) are cleared upon reboot.

5.8.6.2 UPnP

Configure UPnP on this page.



object	Description
• **Mode**	Indicates the UPnP operation mode. Possible modes are: **Enabled**: Enable UPnP mode operation. **Disabled**: Disable UPnP mode operation.

	When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.
• **TTL**	The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.
• **Advertising Duration**	The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

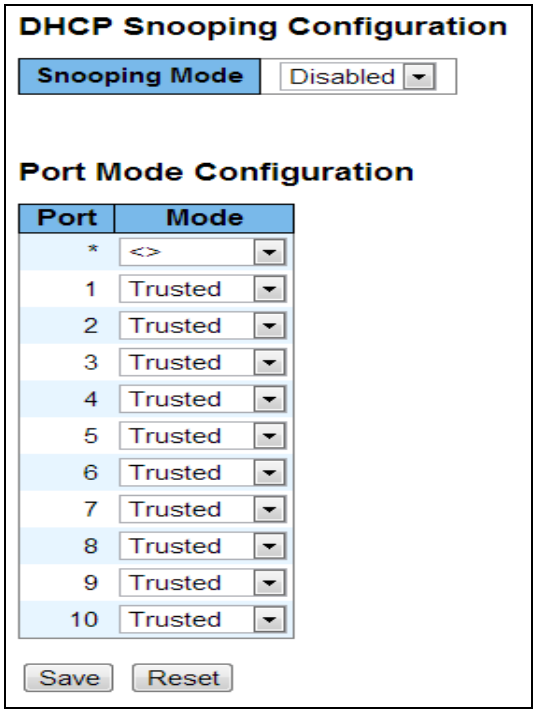
5.8.7 INSPECTION

5.8.7.1 DHCP

■ 5.8.7.1.1 Snooping

5.8.7.1.1.1 Configuration

Configure DHCP Snooping on this page.



object	Description
• **Snooping Mode**	Indicates the DHCP snooping mode operation. Possible modes are: **Enabled**: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports. **Disabled**: Disable DHCP snooping mode operation.
• **Port Mode Configuration**	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted source of the DHCP messages. **Untrusted**: Configures the port as untrusted source of the DHCP messages.

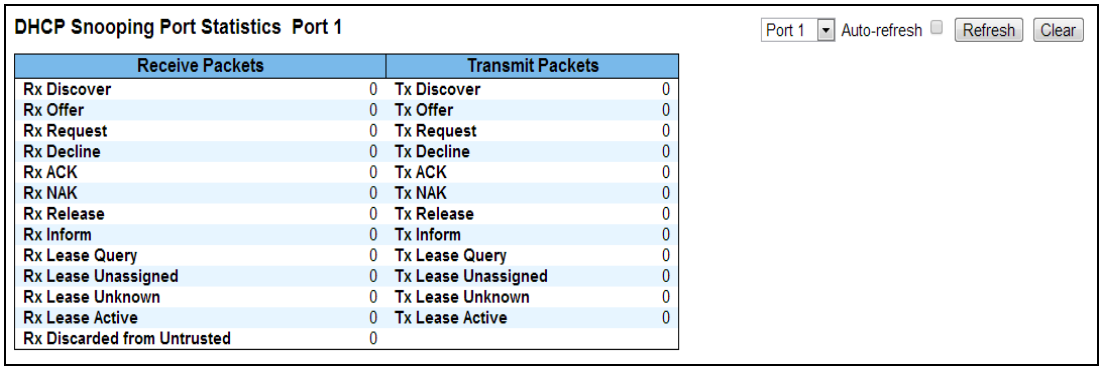
Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

5.8.7.1.1.2 Statistics

This page provides statistics for DHCP snooping. The statistics doesn't count the DHCP packets for system DHCP client or DHCP relay mode is enabled.



DHCP Snooping Port Statistics Port 1

Port 1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded from Untrusted	0		

object	Description
• Rx / Tx Discover	The number of discover (option 53 with value 1) packets received and transmitted.
• Rx / Tx Offer	The number of offer (option 53 with value 2) packets received and transmitted.
• Rx / Tx Request	The number of request (option 53 with value 3) packets received and transmitted.
• Rx / Tx Decline	The number of decline (option 53 with value 4) packets received and transmitted.
• Rx / Tx ACK	The number of ACK (option 53 with value 5) packets received and transmitted.
• Rx / Tx NAK	The number of NAK (option 53 with value 6) packets received and transmitted.

• **Rx / Tx Release**	The number of release (option 53 with value 7) packets received and transmitted.
• **Rx / Tx Inform**	The number of inform (option 53 with value 8) packets received and transmitted.
• **Rx / Tx Lease Query**	The number of lease query (option 53 with value 10) packets received and transmitted.
• **Rx / Tx Lease Unassigned**	The number of lease unassigned (option 53 with value 11) packets received and transmitted.
• **Rx / Tx Lease Unknown**	The number of lease unknown (option 53 with value 12) packets received and transmitted.
• **Rx / Tx Lease Active**	The number of lease active (option 53 with value 13) packets received and transmitted.
• **Rx Discarded from Untrusted**	The number of discarded packet that are coming from untrusted port.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

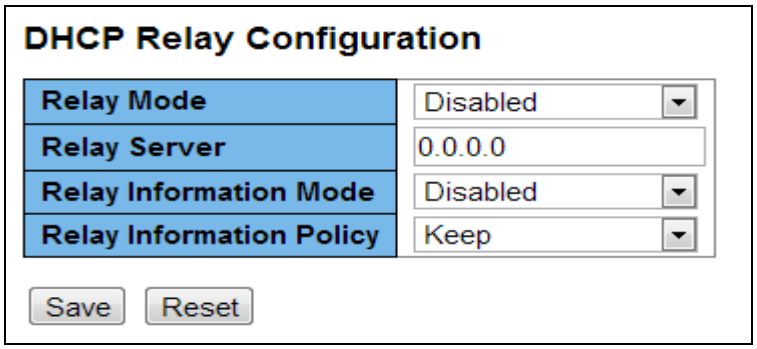
[Refresh]: Click to refresh the page immediately.

[Clear]: Clears the counters for the selected port.

■ 5.8.7.1.2 Relay

• 5.8.7.1.2.1 Configuration

Configure DHCP Relay on this page.



object	Description
• **Relay Mode**	Indicates the DHCP relay mode operation. Possible modes are: **Enabled**: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations. **Disabled**: Disable DHCP relay mode operation.
• **Relay Server**	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain.
• **Relay Information Mode**	Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address. Possible modes are:

	Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled. **Disabled**: Disable DHCP relay information mode operation.
• **Relay Information Policy**	Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are: **Replace**: Replace the original relay information when a DHCP message that already contains it is received. **Keep**: Keep the original relay information when a DHCP message that already contains it is received. **Drop**: Drop the package when a DHCP message that already contains relay information is received.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

• 5.8.7.1.2.2 Statistics

This page provides statistics for DHCP relay.

DHCP Relay Statistics Auto-refresh Refresh Clear

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

object	Description
• **Transmit to Server**	The number of packets that are relayed from client to server.
• **Transmit Error**	The number of packets that resulted in errors while being sent to clients.
• **Receive from Server**	The number of packets received from server.
• **Receive Missing Agent Option**	The number of packets received without agent information options.
• **Receive Missing Circuit ID**	The number of packets received with the Circuit ID option missing.
• **Receive Missing Remote ID**	The number of packets received with the Remote ID option missing.
• **Receive Bad Circuit ID**	The number of packets whose Circuit ID option did not match known circuit ID.
• **Receive Bad Remote ID**	The number of packets whose Remote ID option did not match known Remote ID.
• **Transmit to Client**	The number of relayed packets from server to client.
• **Transmit Error**	The number of packets that resulted in error while being sent to servers.
• **Receive from Client**	The number of received packets from server.
• **Receive Agent Option**	The number of received packets with relay agent information option.
• **Replace Agent Option**	The number of packets which were replaced with relay agent information option.

• **Keep Agent Option**	The number of packets whose relay agent information was retained.
• **Drop Agent Option**	The number of packets that were dropped which were received with relay agent information.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

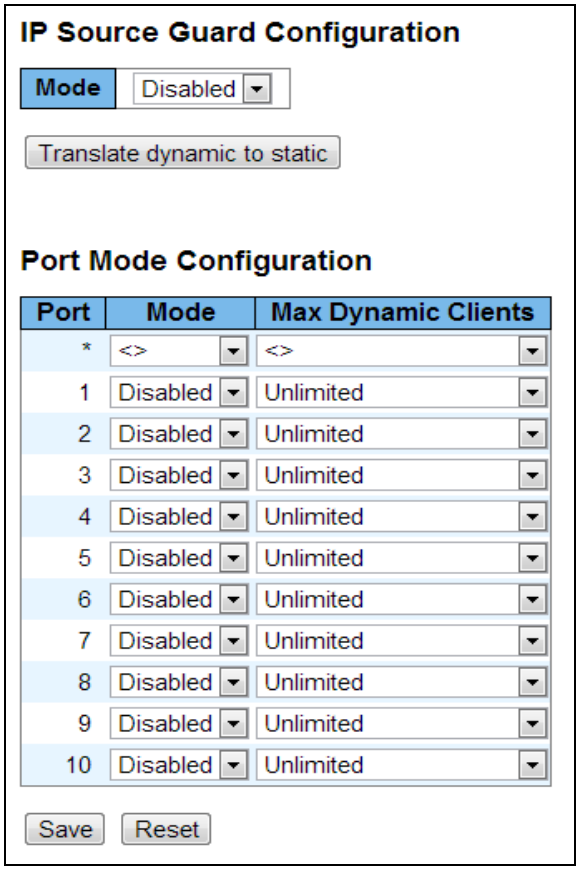
Clear: Clear all statistics.

5.8.7.2 IP Source Guard

■ 5.8.7.2.1 Configuration

• 5.8.7.2.1.1 Configuration

This page provides IP Source Guard related configuration.



object	Description
• **Mode of IP Source Guard Configuration**	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
• **Port Mode Configuration**	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.
• **Max Dynamic Clients**	Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

[Translate dynamic to static]: Click to translate all dynamic entries to static entries.

5.8.7.2.1.2 Static Table

Add a static IP source guard table a new entry page.

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address

[Add New Entry]

[Save] [Reset]

object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings.
VLAN ID	The vlan id for the settings.
IP Address	Allowed Source IP address.
MAC address	Allowed Source MAC address.

Buttons

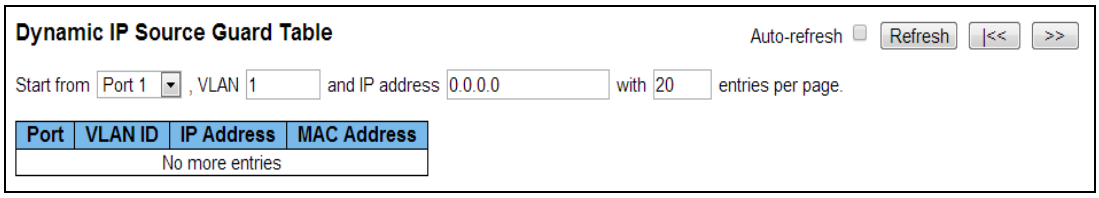
[Add New Entry]: Click to add a new entry to the Static IP Source Guard table.

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

■ 5.8.7.2.2 Status

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.



	용어	설명
●	**Port**	Switch Port Number for which the entries are displayed.
●	**VLAN ID**	VLAN-ID in which the IP traffic is permitted.
●	**IP Address**	User IP address of the entry.
●	**MAC Address**	Source MAC address.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

[Refresh]: Refreshes the displayed table starting from the input fields.

[Clear]: Flushes all dynamic entries.

[|<<]: Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

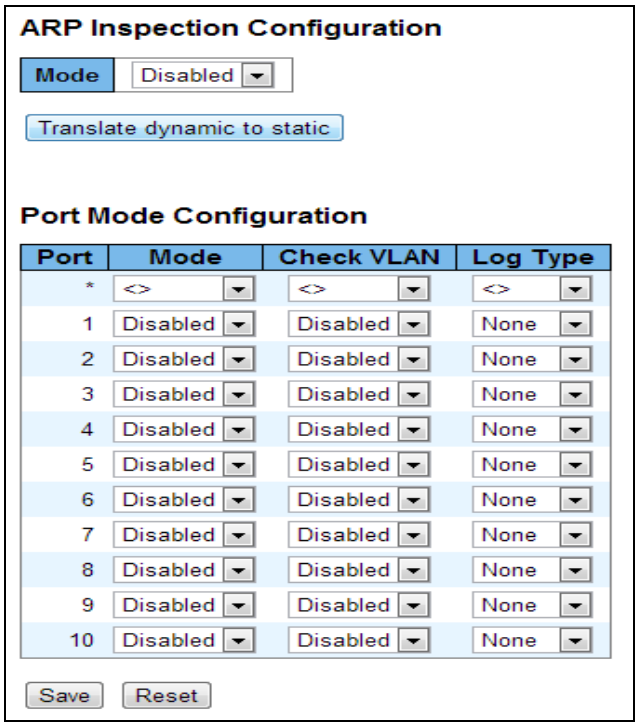
[>>]: Updates the table, starting with the entry after the last entry currently displayed.

5.8.7.3 ARP Inspection

■ 5.8.7.3.1 Configuration

● 5.8.7.3.1 Port Configuration

This page provides ARP Inspection related configuration.



	object	Description
●	**Mode of ARP Inspection Configuration**	Enable the Global ARP Inspection or disable the Global ARP Inspection.
●	**Port Mode Configuration**	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

	Enabled: Enable ARP Inspection operation. **Disabled**: Disable ARP Inspection operation. If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are: **Enabled**: Enable check VLAN operation. **Disabled**: Disable check VLAN operation. Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are: **None**: Log nothing. **Deny**: Log denied entries. **Permit**: Log permitted entries. **ALL**: Log all entries.

Buttons

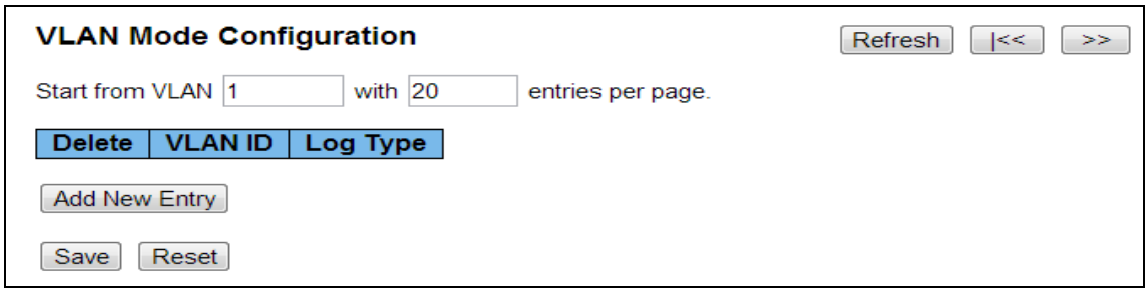
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Translate dynamic to static: Click to translate all dynamic entries to static entries.

5.8.7.3.2 VLAN Configuration

This page provides ARP Inspection related configuration.



object	Description
• VLAN Mode Configuration	Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting. Possible types are: **None**: Log nothing. **Deny**: Log denied entries. **Permit**: Log permitted entries. **ALL**: Log all entries.

Buttons

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

k<: Updates the table starting from the first entry in the ARP Inspection VLAN table.

[>>]: Updates the table, starting with the entry after the last entry currently displayed.

[Add New Entry]: Click to add a new VLAN to the ARP Inspection VLAN table.

5.8.7.3.3 Static Table

Add new item in this page is static ARP Inspection Table.

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address

[Add New Entry]

[Save] [Reset]

object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings.
VLAN ID	The vlan id for the settings.
MAC Address	Allowed Source MAC address in ARP request packets.
IP Address	Allowed Source IP address in ARP request packets.

Buttons

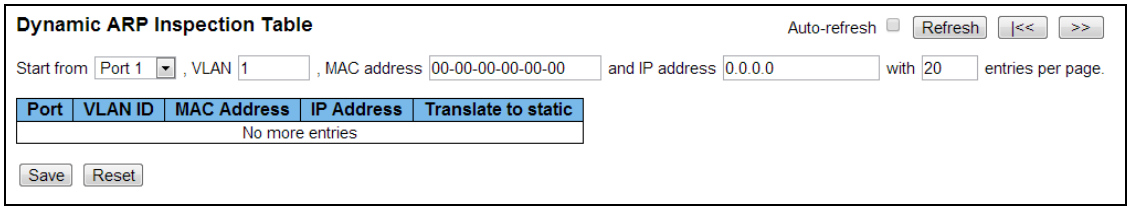
[Add New Entry]: Click to add a new entry to the Static ARP Inspection table.

[Save]: Click to save changes.

[Reset]: Click to undo any changes made locally and revert to previously saved values.

5.8.7.3.4 Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.



object	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the ARP traffic is permitted.
MAC Address	User MAC address of the entry.
IP Address	User IP address of the entry.
Translate to static	Select the checkbox to translate the entry to static entry.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

Save: Click to save changes.

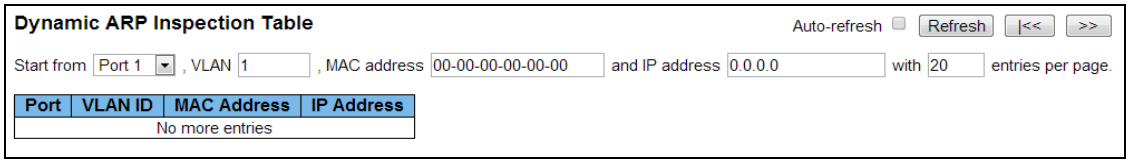
Reset: Click to undo any changes made locally and revert to previously saved values.

|<<: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

5.8.7.3.2 Status

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.



object	Description
• **Port**	Switch Port Number for which the entries are displayed.
• **VLAN ID**	VLAN-ID in which the ARP traffic is permitted.
• **MAC Address**	User MAC address of the entry.
• **IP Address**	User IP address of the entry.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

Clear: Flushes all dynamic entries.

<<: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

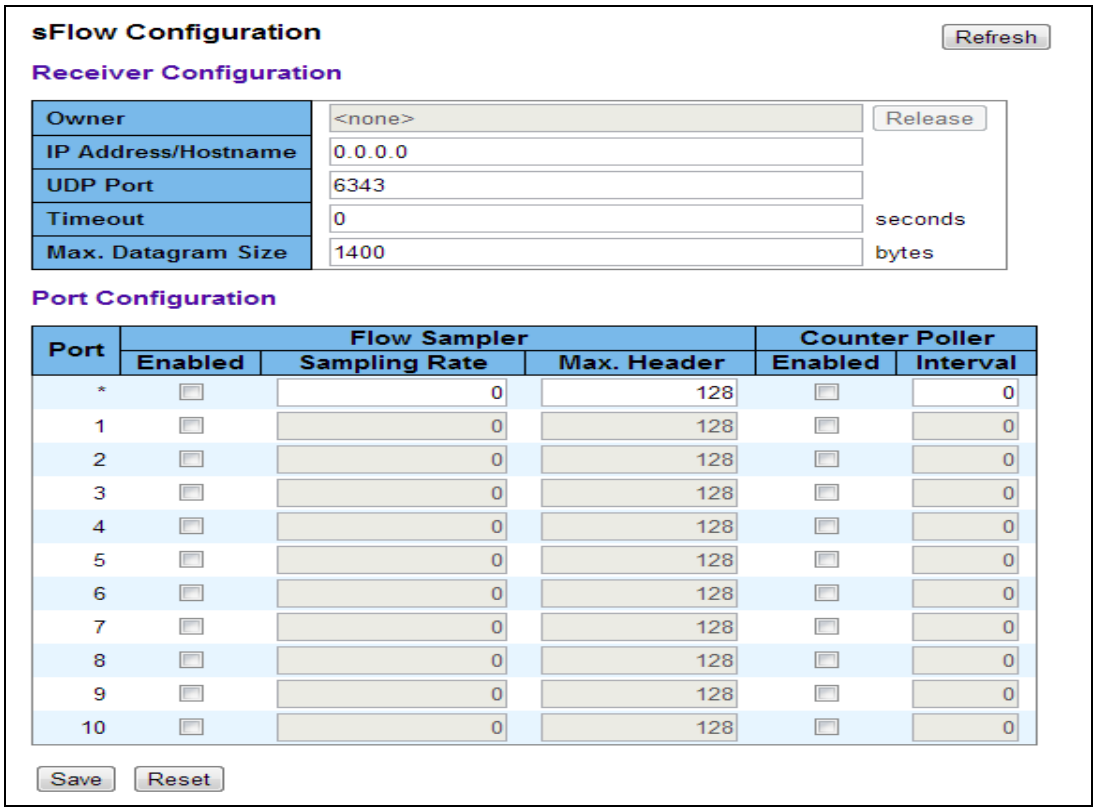
>>: Updates the table, starting with the entry after the last entry currently displayed.

5.8.7.4 sFlow

■ 5.8.7.4.1 Configuration

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.



object	Description
● Owner	Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of

	the current sFlow configuration and assumes values as follows: • If sFlow is currently unconfigured/unclaimed, Owner contains **<none>.** • If sFlow is currently configured through Web or CLI, Owner contains **<Configured through local management>.** • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.
• **IP Address/ Hostname**	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.
• **UDP Port**	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
• **Timeout**	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.
• **Datagram Size**	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.
• **Port**	The port number for which the configuration below applies.
• **Flow Sampler Enabled**	Enables/disables flow sampling on this port.
• **Flow Sampler Sampling Rate**	The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported

	sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.
• **Flow Sampler Max.**	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.
• **Counter Poller Enabled**	Enables/disables counter polling on this port.
• **Counter Poller Interval**	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.

Buttons

Refresh: Click to refresh the page. Note that unsaved changes will be lost.

Save: Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

Reset: Click to undo any changes made locally and revert to previously saved values.

Release: See description under Owner.

5.8.7.4.2 Status

This page shows receiver and per-port sFlow statistics.

sFlow Statistics

Auto-refresh ☐ Refresh Clear Receiver Clear Ports

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Rx Flow Samples	Tx Flow Samples	Counter Samples
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0

object	Description
• **Owner**	This field shows the current owner of the sFlow configuration. It assumes one of three values as follows: • If sFlow is currently unconfigured/unclaimed, Owner contains **<none>.** • If sFlow is currently configured through Web or CLI, Owner contains **<Configured through local management>**. • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
• **IP Address /Hostname**	The IP address or hostname of the sFlow receiver.
• **Timeout**	The number of seconds remaining before sampling stops and the current sFlow owner is released.
• **Tx Successes**	The number of UDP datagrams successfully sent to the sFlow receiver.
• **Tx Errors**	The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web

	page (Diagnostics → Ping/Ping6).
• **Flow Samples**	The total number of flow samples sent to the sFlow receiver.
• **Counter Samples**	The total number of counter samples sent to the sFlow receiver.
• **Port**	The port number for which the following statistics applies.
• **Rx and Tx Flow Samples**	The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.
• **Counter Samples**	The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons

Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

[Refresh]: Click to refresh the page.

[Clear Receiver]: Clears the sFlow receiver counters.

[Clear Ports]: Clears the per-port counters.

5.9 DIAGNOSTICS

- Diagnostics
  - Ping
  - Ping6
  - VeriPHY

Indicate general setting detail of switch and configure.

In Diagnostics, there are three chapters. In these chapters provide Diagnostics information as below.

■ **Ping**	Check the ping which flows out through ICMP packet. (In case of IP address is IPv4)
■ **Ping6**	Check the ping which flows out through ICMP packet. (In case of IP address is IPv6)
■ **VeriPHY**	Diagnose cable of ports using diagnostic program.

5.9.1 PING(IPV4, IPV6)

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press **Start**, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space(the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

ICMP Ping Output

```
PING server 192.168.20.191, 56 bytes of data.
64 bytes from 192.168.20.191: icmp_seq=0, time=0ms
64 bytes from 192.168.20.191: icmp_seq=1, time=0ms
64 bytes from 192.168.20.191: icmp_seq=2, time=0ms
64 bytes from 192.168.20.191: icmp_seq=3, time=0ms
64 bytes from 192.168.20.191: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues. After you press **Start**, ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

ICMPv6 Ping Output

```
PING6 server fe80::6d97:3c26:5e84:731, 56 bytes of data.
64 bytes from fe80::6d97:3c26:5e84:731: icmp_seq=0, time=0ms
64 bytes from fe80::6d97:3c26:5e84:731: icmp_seq=1, time=0ms
64 bytes from fe80::6d97:3c26:5e84:731: icmp_seq=2, time=0ms
64 bytes from fe80::6d97:3c26:5e84:731: icmp_seq=3, time=0ms
64 bytes from fe80::6d97:3c26:5e84:731: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

New Ping

You can configure the following properties of the issued ICMP packets:

Object	Description
• **IP Address**	The destination IP Address.
• **Ping Length**	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
• **Ping Count**	The count of the ICMP packet. Values range from 1 time to 60 times.
• **Ping Interval**	The interval of the ICMP packet. Values range from 1 second to 30 seconds.

Buttons

Start: Click to start transmitting ICMP packets.

New Ping: Click to re-start diagnostics with PING.

5.9.2 VERIPHY

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

VeriPHY Cable Diagnostics

Port All

Start

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--

Object	Description
• **Port**	The port where you are requesting VeriPHY Cable Diagnostics.
• **Cable Status**	**Port**: Port number. **Pair**: The status of the cable pair. OK - Correctly terminated pair Open - Open pair Short - Shorted pair Short A - Cross-pair short to pair A Short B - Cross-pair short to pair B Short C - Cross-pair short to pair C Short D - Cross-pair short to pair D Cross A - Abnormal cross-pair coupling with pair A Cross B - Abnormal cross-pair coupling with pair B Cross C - Abnormal cross-pair coupling with pair C Cross D - Abnormal cross-pair coupling with pair D **Length**: The length (in meters) of the cable pair. The resolution is

3 meters

Buttons

Start : Act up diagnostic program. (It takes 5 ~ 15 seconds.)

5.10 MAINTENANCE

- Maintenance
  - Restart Device
  - Factory Defaults
  - Software
  - Configuration

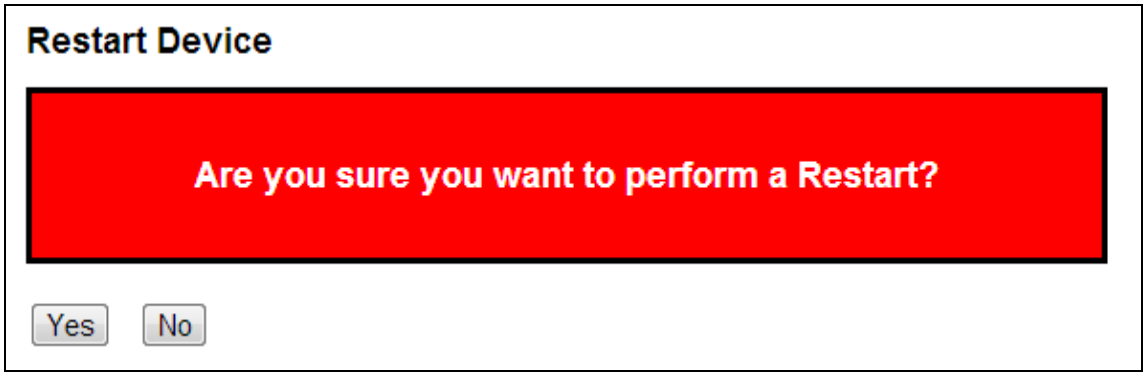
Indicate general setting detail of switch and configure.

In Maintenance, there are four chapters. In these chapters provide Maintenance information as below.

■ **Restart Device**	Restart a device.
■ **Factory Defaults**	Return to factory defaults
■ **Software**	Update firmware of the device.
■ **Configuration**	Save or upload setting information of the device to bring the information.

5.10.1 RESTART DEVICE

You can restart the switch on this page. After restart, the switch will boot normally.



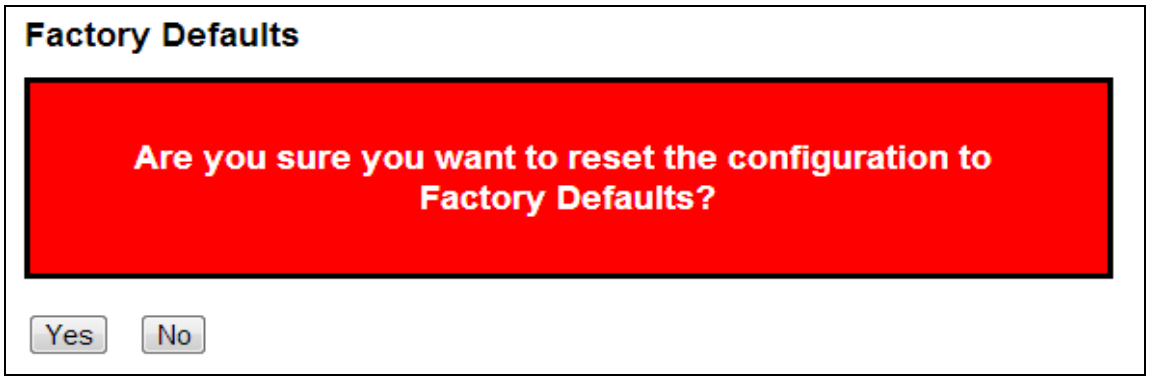
Yes : Click to restart device.

No : Click to return to the Port State page without restarting.

5.10.2 FACTORY DEFAULTS

You can reset the configuration of the switch on this page. Only the IP configuration is retained.

The new configuration is available immediately, which means that no restart is necessary.



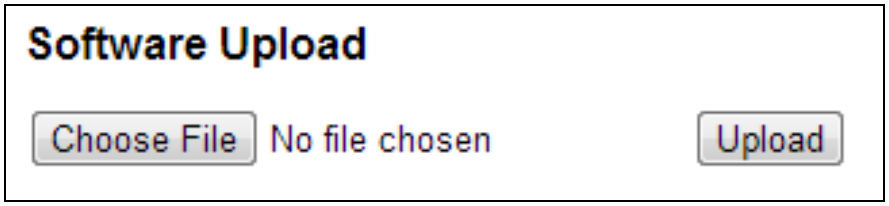
Yes : Click to reset the configuration to Factory Defaults.

No : Click to return to the Port State page without resetting the configuration.

5.10.3 SOFTWARE

5.10.3.1 Upload

This page facilitates an update of the firmware controlling the switch.



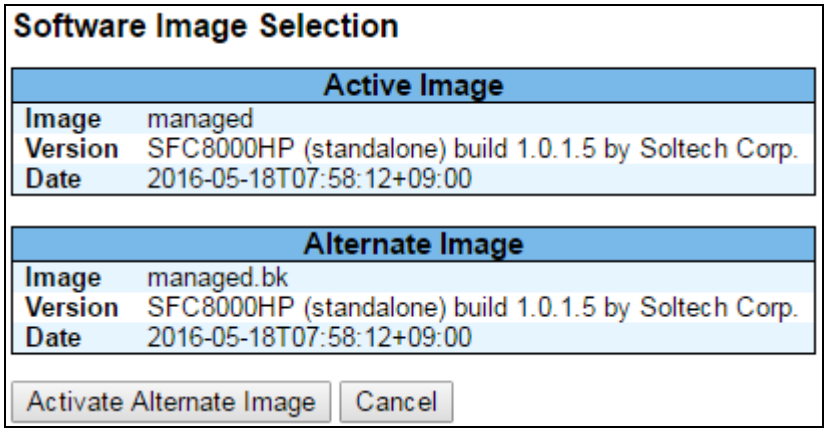
After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

Warning : Do not restart or power off the device at this time or the switch may fail to function afterwards.

5.10.3.2 Image Select

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.



Note:

1. In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the **Activate Alternate Image** button is also disabled.

2. If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Object	Description
• **Image**	The flash index name of the firmware image. The name of primary (preferred) **image** is image, the alternate image is named **image.bk**.
• **Version**	The version of the firmware image.
• **Date**	The date where the firmware was produced.

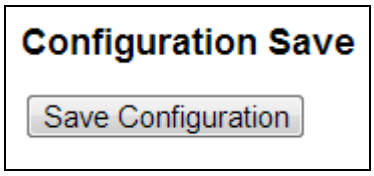
Activate Alternate Image: Click to use the alternate image. This button may be disabled depending on system state.

Cancel: Cancel activating the backup image. Navigates away from this page.

5.10.4 CONFIGURATION

5.10.4.1 Save

This page saves all of setting status of switch as XML file.



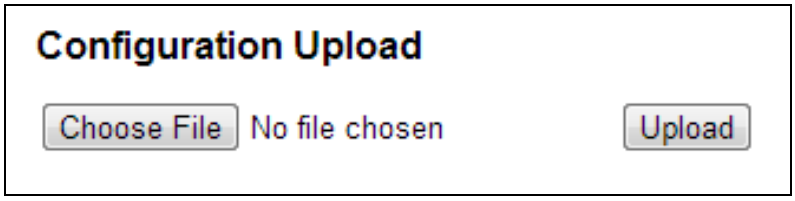
Saving view or loding configuration of switch. Configuration file is a layer structure of tag and XML format.

Parameters, which are configured to a file, expresses attribute value. If users save config file of switch, the config file has explanation of attribute value and all of configuration. Saved file can be revised or loaded into switch.

Save Configuration: Click to save the configuration file

5.10.4.2 Upload

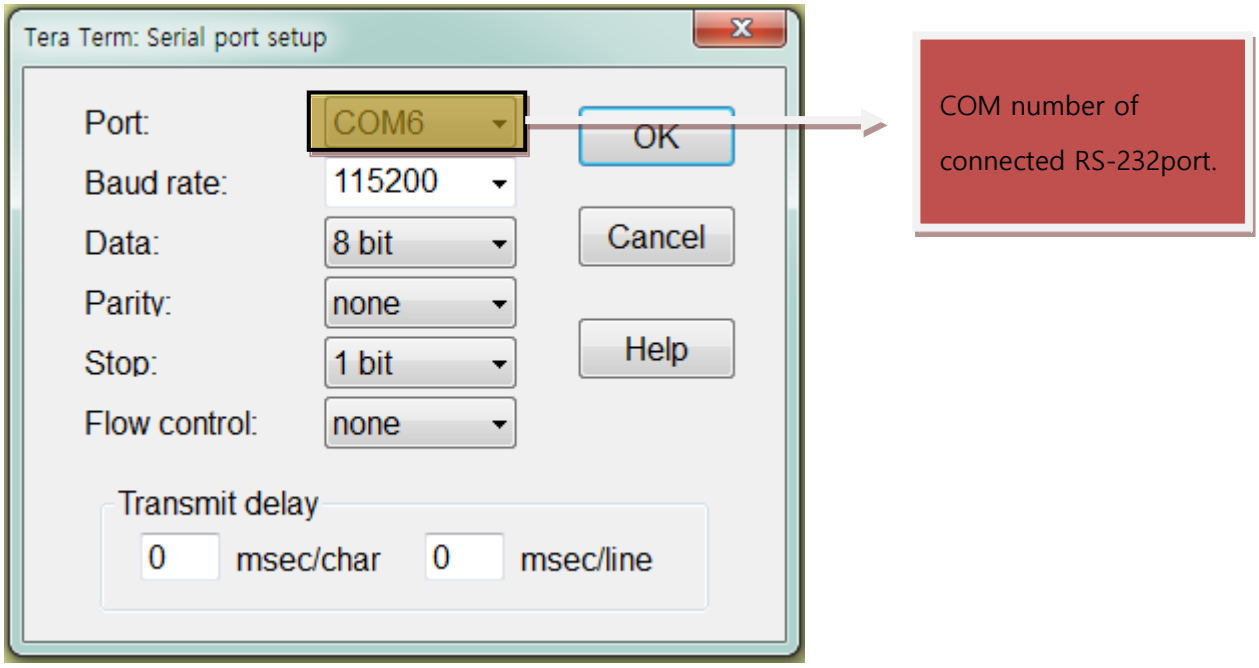
This page loads XML file that all of setting status and applies the switch.



Upload: Click to upload the configuration file.

6 Consol setting(Telnet, SSH)

Consol SETTING is used for simple setting, the device has to connect one to one. Please connect SFC8000HP with RS-232port of PC using CONSOL cable, which is enclosed.
Setting method of below is made by Tera Term(freeware).
Set communication speed like below. (Tera Term → menu → Setup/serial port)

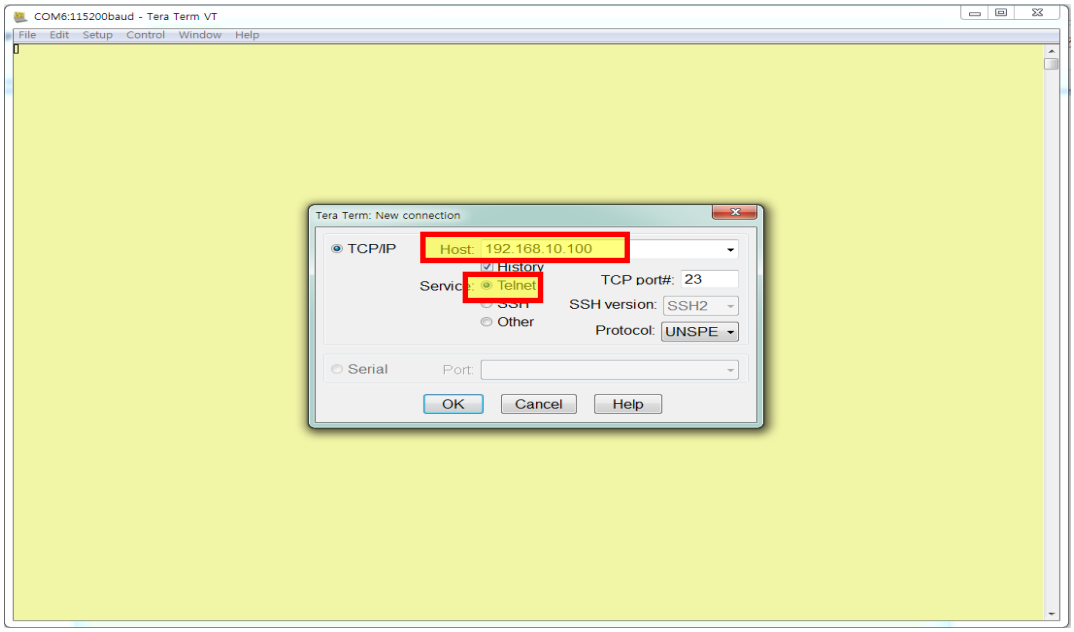


Run Tera Term and login SFC8000HP, User name : admin / Password : admin.

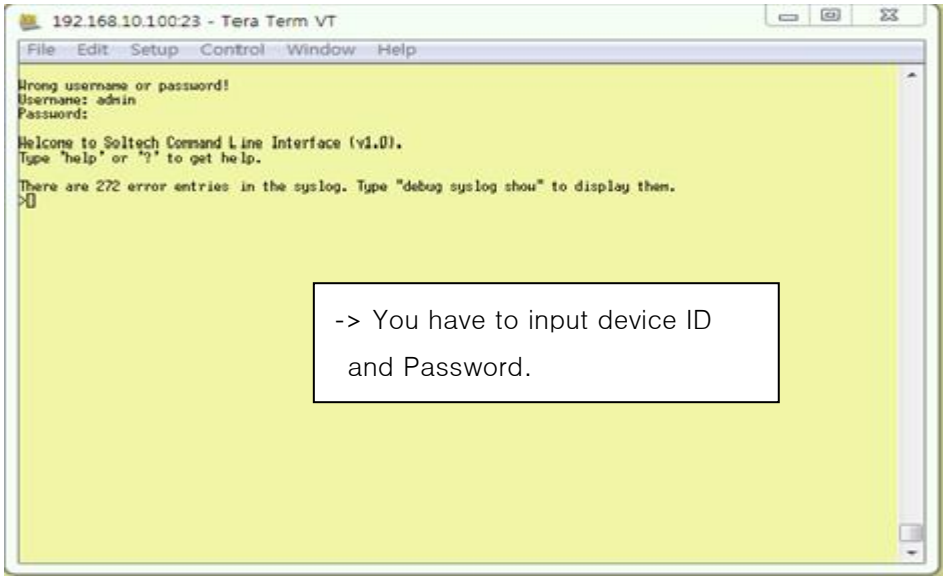
Consol setting of Telnet, SSH is used for simple setting

Setting method of below is made by Tera Term(freeware).

[Telnet setting]



Input an IP address, ready to use, in HOST. Check Talnet in Service than click OK.
You can find that connecting message as below.



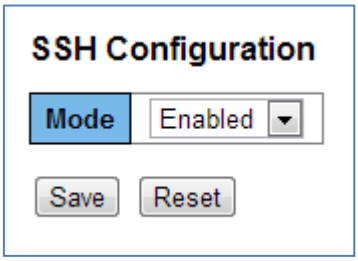
On the next screen, please login. (User name : admin / Password : admin)

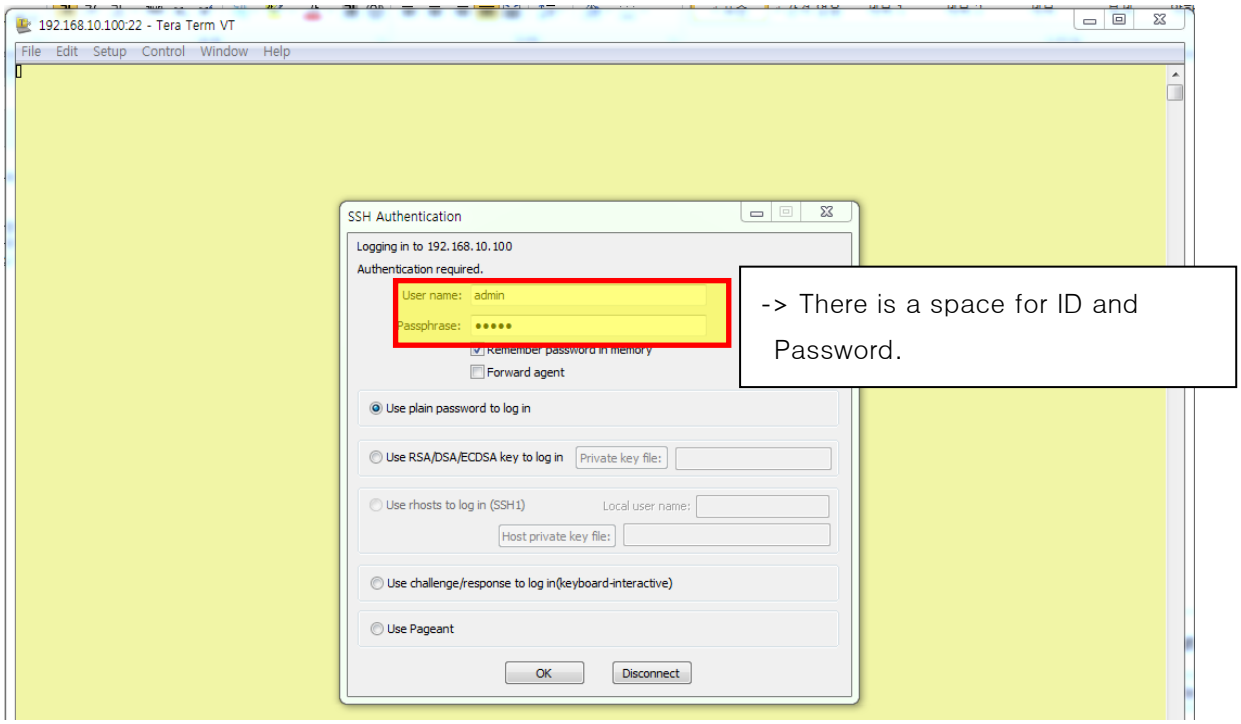
[SSH setting]

System → Security → SSH setting

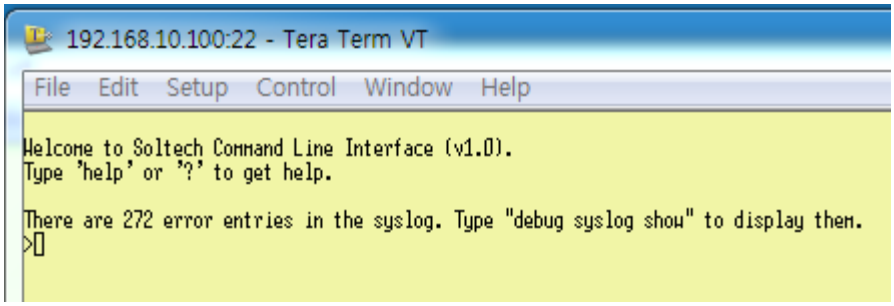
Default value of Mode is Enabled.

To check this, please refer as below.



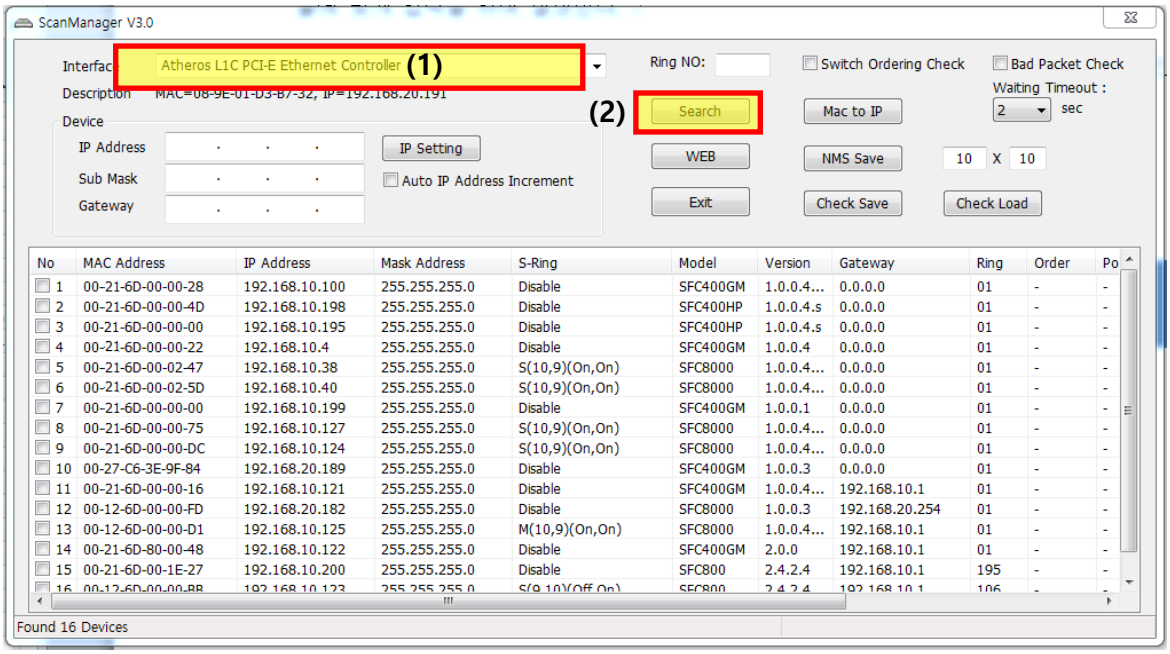


When the next screen is displayed, please input like 'login: admin, Password: admin' to access.



You can check it enters CLI when you input ID and Password.

7 Scan manager



Please download Scan Manager and set up your PC.

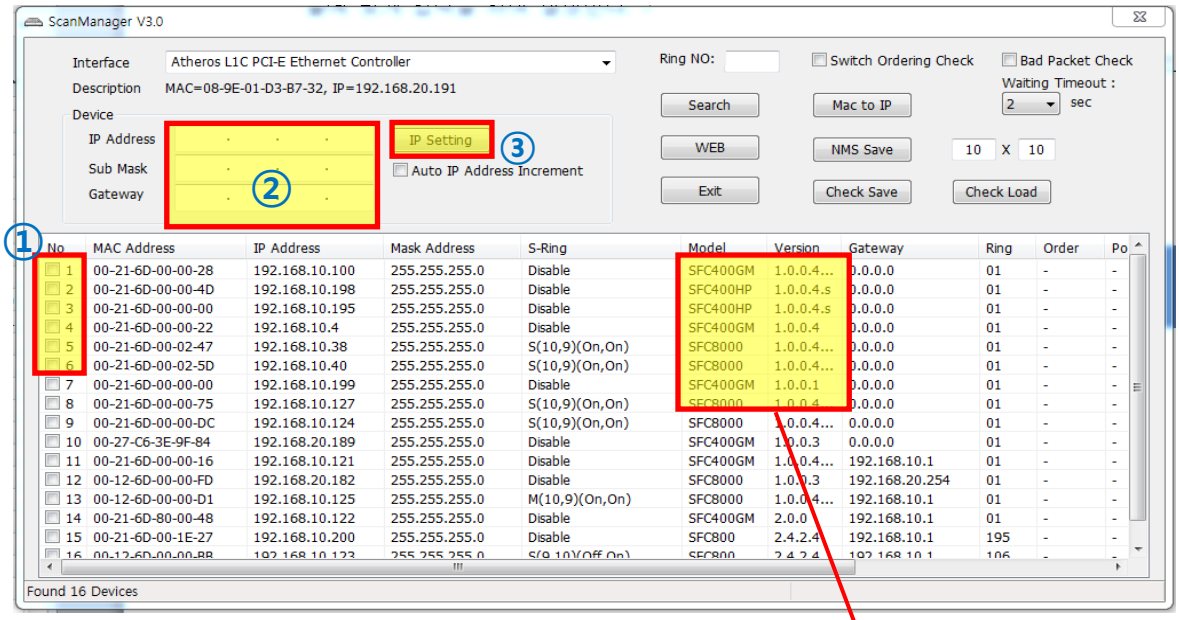
(1) Chose a LAN card that you use now.

(2) Click the Search button. (It shows the device information which is connected.)

(3) Click the searched device.

(4) After setting IP/Netmask, click IP setting button. Auto re-searches.
IP address is changed and saved.

[Changing IP address]



Check model name and version

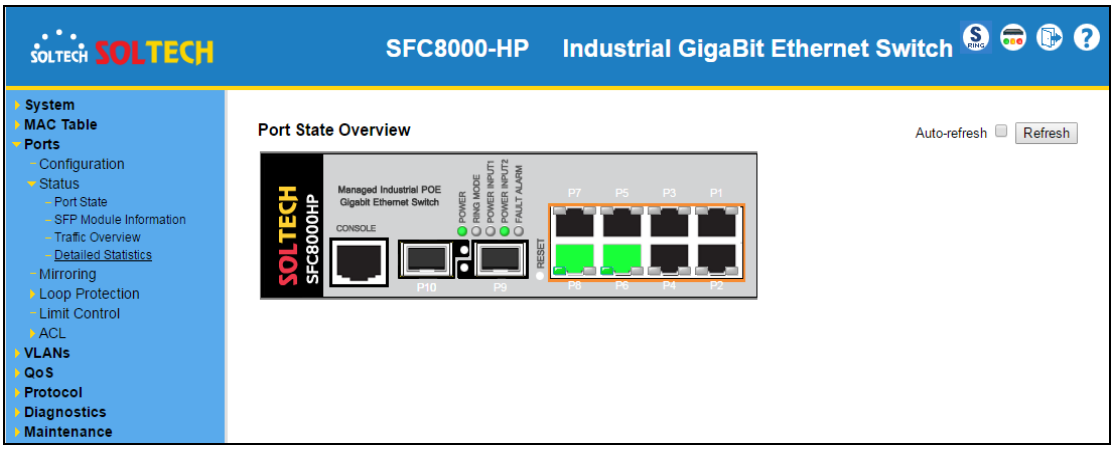
① **Check devices to change.**

② **Input the IP address you want to change into a textbox.**

③ **Click IP setting.**

(5) Double click Web to open web browser.

You can check a screen as below.



8 Maintenance Inspection

8.1 SURVEILLANCE CENTER MAINTENANCE

Inspected Product	Inspection Period	Actions	Procedures
Fiber Optic Switch	Daily	Outlook check	1) Check if the LED indicator is normal. 2) Check if the terminal block of the power supply is plugged in.
		Scan by the scan program	Check whether all equipment is scanned when scanning with the scan program supplied.
		SFP port check	1) Check if SFP Locking is done properly. 2) Check if the jumper cord is properly connected to the SFP port.
		Jumper code check	Check if multiple store codes are too badly twisted.
		PING test	Test the device Ping with multi-ping or general ping test program
	Periodic	RING status check	1) Check if the mastering device status is in ring or open. 2) After connecting the device to the web, check each port bad packet. 3) After connecting the device to the

			web, check Enable/Disable one of the ring ports.
		Power inspection	Check if the 24V power is properly supplied
		Web access check	Access each device through the web

8.2 ETHERNET SWITCH MAINTENANCE

A. Web access inspection method

1) After connecting the master device and a general PC, set the IP
2) After connecting to the device, scan the device connected to the master device using the SCAN PROGRAM
3) Check if the number of scanned equipment and the number of installed equipment are correct.
4) Double click the scanned device and check if it is accessible to the web

B. When the number of installed device and scanned is different

1) After checking the installed device list, access to the web of the upper and lower layer device connected to the unscanned device.
2) If the connection to the ring port on the web of the upper and lower device is disconnected, check if the upper and lower device ring ports status are in Enable.
3) If it is enabled, check the SFP and jumper code status of the unscanned device and reboot.
4) If the device is not scanned even after rebooting, contact supplier for A/S.

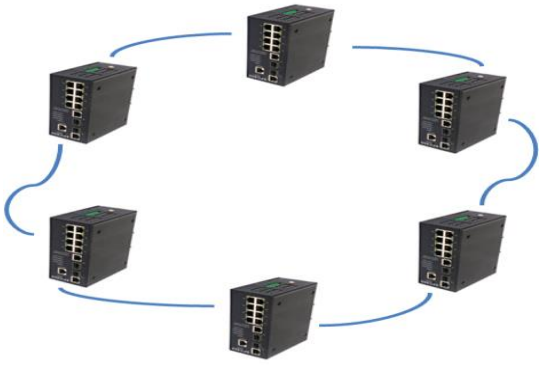
C. Network inspection method

1) When the network speed fails, check the ring port bad packet by accessing the web of the failed ring devices.

2) When the bad packet port is an SFP port, check the SFP and jumper code status or replace.
3) When a bad packet continues, remove the devices connected to the optical switch TP port and check the bad packet.
4) If the bad packets continue to occur after you have taken the above steps, please contact the supplier for A/S.

8.3 ACTIONS FOR RING CONSTRUCTION FAILURES

A. Ring Unit



B. Actions

Procedures	Equipment	Actions	Remarks
1	Fiber Optic Switch	1) check 4.1 procedure if ring equipment scan is not available 2) § Conduct a ping test	
2	SFP	Check if the locking is done properly	
3	Jumper code	Check if the jumper cord is pressed or badly bent	

4	Power and wavelength	Check the power supply and Optical power	

Warranty

Soltech Co., Ltd values your business and always attempts to provide you the best solution.
Any Soltech Products which proves defects during the 12-month warranty period should be returned to the dealer where you purchased the equipment or to the manufacturer. If there is no representative of the manufacturer in your country, send the equipment to the manufacturer, with postage prepaid. In this case, it will take a considerable length of time before the equipment can be returned to you owing to the complicated customs procedures required in Korea in importing and re-exporting Fiber optic equipment. During under the warranty, the charge of repairs and the some parts replaced of equipment is all free, and the equipment will be returned to you upon completion of servicing.

After 12 month warranty, repairing and replacing of some parts will be charged. There also will be charged even though it is under warranty: if the equipment is broken down by users' purpose, negligence, natural disaster or trouble of the other devices.