



## **24-Port 10/100/1000Base-T + 2-Port 10G SFP+ Stackable**

**ALL-SG8826MX-10G**



## **User's Manual**

**Default-IP**  
**192.168.2.1**

**Password:**  
**admin**

### **FCC Warning**

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

### **CE Mark Warning**

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

# Content

1. Products Overview .....	8
1.1 Major Management Features.....	9
1.2 Product Specification .....	10
1.3 Package Contents.....	13
2. Hardware Description .....	14
3. Preparation for Management .....	16
3.1 Preparation for Serial Console .....	16
3.2 Preparation for Web Interface .....	17
3.3 Preparation for Telnet/SSH Interface .....	19
4. Feature Configuration - Web UI.....	21
4.1 System Configuration .....	21
4.1.1 System Information.....	21
4.1.2 IP Configuration:.....	22
4.1.3 IPv6 Configuration .....	23
4.1.4 NTP Configuration: .....	24
4.1.5 System Log Configuration: .....	25
4.2 Power Reduction .....	26
4.2.1 LED Power Reduction Configuration .....	26
4.2.2 EEE Configuration:.....	27
4.3 Port Configuration:.....	28
4.4 Security Configuration:.....	30
4.4.1 Security / Switch .....	30
4.4.1.1 Security / Switch / Users Configuration .....	30
4.4.1.2 Security / Switch / Privilege Levels Configuration:.....	31
4.4.1.3 Security / Switch / Auth Method.....	33
4.4.1.4 Security /Switch / SSH Configuration.....	34
4.4.1.5 Security / Switch / HTTPS Configuration.....	34
4.4.1.6 Security / Switch / Access Management Configuration .....	35
4.4.1.7 Security / Switch / SNMP.....	36
4.4.1.8 RMON Statistics Configuration.....	46
4.4.2 Security /Network.....	52
4.4.2.1 Port Security Limit Control Configuration .....	52
4.4.2.2 Security / Network / Network Access Server Configuration .....	55
4.4.2.3 Security / Network / Access Control List Configuration .....	63
4.4.2.4 Switch / Network / DHCP Configuration .....	77
4.4.2.5 IP Source Guard Configuration .....	80

4.4.2.6 ARP Inspection .....	82
4.4.3 Security / AAA Authentication Server Configuration.....	84
4.5 Aggregation Configuration.....	88
4.5.1 Static Aggregation.....	88
4.5.2 LACP - Dynamic Aggregation .....	89
4.6 Loop Protection.....	91
4.7 Spanning Tree .....	93
4.7.1 Spanning Tree / Bridge Setting.....	93
4.7.2 Spanning Tree / MSTI Mapping .....	95
4.7.3 Spanning Tree / MSTI Priorities.....	96
4.7.4 Spanning Tree / CIST Ports .....	97
4.7.5 Spanning Tree MSTI Ports .....	99
4.8 MVR (Multicast VLAN Registration) .....	101
4.9 IPMC (IP Multicast) .....	104
4.9.1 IGMP Snooping Configuration .....	104
4.9.1.1 Basic Configuration.....	104
4.9.1.2 IGMP Snooping VLAN Configuration.....	106
4.9.1.3 IGMP Snooping / Port Group Filtering .....	107
4.9.2 MLD Snooping Configuration .....	108
4.9.2.1 Basic Configuration.....	108
4.9.2.2 MLD Snooping VLAN Configuration .....	109
4.9.2.3 IPMC / MLD Snooping / Port Group Filtering .....	111
4.10 LLDP Parameters .....	112
4.10.1 LLDP Configuration.....	112
4.10.2 LLDP Media Configuration .....	114
4.11 sFlow Configuration.....	123
4.12 MAC Address Table Configuration.....	126
4.13 VLAN (Virtual LAN) .....	129
4.13.1 VLAN Membership Configuration.....	129
4.13.2 VLAN Port Configuration.....	131
4.14 Private VLANs .....	135
4.14.1 Private VLAN Membership Configuration .....	135
4.14.2 Port Isolation Configuration.....	136
4.15 VCL.....	138
4.15.1 VCL / MAC-Based VLAN Configuration .....	138
4.15.2 VCL / Protocol-based VLAN.....	139
4.15.3 VCL / IP Subnet-based VLAN .....	142
4.16 Voice VLAN Configuration.....	144



4.16.1 Voice VLAN / Configuration.....	144
4.16.2 Voice VLAN / OUI Configuration .....	145
4.17 QoS .....	147
4.17.1 QoS / Ingress Port Classification .....	147
4.17.2 QoS / Ingress Port Policer Config.....	148
4.17.3 QoS / Port Scheduler .....	150
4.17.4 QoS / Egress Port Shapers .....	150
4.17.5 QoS / Port Tag Remarking.....	151
4.17.6 QoS / Port DSCP Configuration.....	152
4.17.7 QoS / DSCP based QoS Ingress Classification .....	154
4.17.8 QoS / DSCP Translation.....	155
4.17.9 QoS / DSCP Classification .....	157
4.17.10 QoS / Control List Configuration .....	158
4.17.11 QoS / Storm Control Configuration.....	160
4.18 Mirroring Configuration.....	162
4.19 UPnP Configuration .....	163
4.20 Stack Configuration .....	163
5. Feature Configuration - CLI .....	168
5.1 System Configuration .....	168
5.2 Power Reduction .....	172
5.3 Port Configuration .....	173
5.4 Security Configuration.....	175
5.5 Aggregation Configuration.....	186
5.6 Loop Protection.....	187
5.7 Spanning Tree .....	187
5.8 MVR .....	189
5.9 IPMC.....	190
5.10 LLDP Configuration.....	192
5.11 sFlow Configuration.....	193
5.12 MAC Address Table Configuration .....	194
5.13 VLAN Configuration .....	194
5.14 Private VLAN Configuration .....	195
5.15 VCL Configuration .....	195
5.16 Voice VLAN Configuration .....	197
5.17 QoS Configuration.....	198
5.18 Mirroring Configuration .....	200
5.19 UPnP Configuration .....	201
5.20 Diagnostic Commands.....	201

5.21 Maintenance Commands .....	202
6. Web Configuration - Monitor, Diagnostic, Maintenance .....	204
6.1 Monitor.....	204
6.1.1 Monitor / System .....	204
6.1.1.1 Monitor / System / Information .....	204
6.1.1.2 CPU Load .....	200
6.1.1.3 System Log Information.....	201
6.1.1.4 System / Detailed Log.....	207
6.1.2 Monitor / Port State .....	208
6.1.2.1 Port State.....	208
6.1.2.2 Traffic Overview .....	209
6.1.2.3 QoS Statistics .....	210
6.1.2.4 QCL Status .....	210
6.1.2.5 Detailed Port Statistics.....	212
6.1.3 Monitor / Security.....	215
6.1.3.1 Security / Access Management Statistics .....	215
6.1.3.2 Security / Network.....	216
6.1.3.3 Security / AAA .....	238
6.1.3.4 Switch / SNMP / RMON.....	245
6.1.4 LACP System Status .....	252
6.1.4.1 System Status.....	252
6.1.4.2 LACP Port Status.....	253
6.1.4.3 LACP statistics.....	254
6.1.5 Loop Protection.....	254
6.1.6 STP Bridge Status .....	255
6.1.6.1 Bridge Status .....	255
6.1.6.2 STP Port Status .....	257
6.1.6.3 STP Port Statistics .....	258
6.1.7 MVR Status .....	260
6.1.7.1 Statistics.....	260
6.1.7.2 MVR Group Table .....	261
6.1.8 Monitor / IPMC / IGMP Snooping .....	262
6.1.8.1 IGMP Snooping .....	262
6.1.8.2 MLD Snooping Status.....	266
6.1.9 Monitor / LLDP .....	271
6.1.9.1 LLDP / Neighbor .....	271
6.1.9.2 LLDP MED Neighbours.....	272
6.1.9.3 LLDP EEE .....	277

6.1.9.4 LLDP Statistics .....	279
6.1.10 Dynamic MAC Table .....	281
6.1.11 VLAN Membership Status .....	283
6.1.13 VCL MAC-Based VLAN Status .....	287
6.1.14 sFlow .....	289
6.2 Diagnostic.....	290
6.2.1 Ping.....	290
6.2.2 Ping6.....	290
6.2.3 VeriPHY Cable Diagnostic.....	291
6.3 Maintenance .....	293
6.3.1 Restart Device.....	293
6.3.2 Factory Defaults .....	293
6.3.3 Software Upload .....	294
6.3.3.1 Firmware Update .....	294
6.3.3.2 Image Select .....	295
6.3.4 Configuration .....	296
7. CE .....	299

# 1. Products Overview

The switch is 24-port 10/100/1000Base-T + 2 10G SFP+ Open Slot Rack-mount L2+ Full Management Network Switch / PoE Switch that is designed for medium or large network environment to strengthen its network connection. The switch supports 128G non-blocking switch fabric, the 24 gigabit ports and 4 10G ports can transmit and receive data traffic without any lost. The EEE feature reduces the power consumption when there is no traffic forwarding even port is still connected. The 10G uplink port design is available and important for high bandwidth uplink request when cascaded with other switch. The switch also supports Layer 2+ full management software features. These features are powerful to provide network control, management, monitor and security feature requests. Including rack-mount brackets, the 19" size fits into your rack environment. It is a superb choice to boost your network with better performance and efficiency.

## 2 x 10 Gigabit SFP+ Open Slots

The switch equips with 2 10G SFP+ open slots as the uplink ports, the 10G uplink design provides an excellent solution for expanding your network from 1G to 10G. By 10G speed, this product provides high flexibility and high bandwidth connectivity to another 10G switch or the Servers, Workstations and other attached devices which support 10G interface. The user can also aggregate the 10G ports as Trunk group to enlarge the bandwidth.

## Stacking Features

The switch includes a stacking feature by using 2 SFP+ ports that allows multiple switches to operate as a single unit. Any single switch in the stack can manage all the other units in the stack and uses a single IP address which allows the user to manage every port in the stack from this one address. These stacks can include up to 16 switches, or total 384 gigabit ports plus 32 ports 10G in a switch.

## Management Features

The switch includes full Layer 2+ Management features. The software set includes up to 4K 802.1Q VLAN groups and advanced Protocol VLAN, Private VLAN, MVR...features. There are 8 physical queues Quality of Service, IPv4/v6 Multicast filtering, Rapid Spanning Tree protocol to avoid network loop, Multiple Spanning Tree Protocol to integrate VLAN and Spanning Tree, LACP, LLDP; sFlow, port mirroring, cable diagnostic and advanced Network Security features. It also provides Console CLI for out of band management and SNMP, Web GUI for in band Management.

## 1.1 Major Management Features

- 24 10/100/1000Base RJ-45 plus 2 10G Base SFP Stackable
- Up to 128Gbps switching capacity, 16K MAC Address Table
- Per-Port Power Management Feature supports Enable/Disable, Priority Setting, Overloading Protection and Power Level settings
- IEEE 802.1D STP and IEEE 802.1w RSTP
- IEEE 802.1Q VLAN, up to 4K VLAN Group
- Port Based VLAN, MAC Based VLAN, Protocol Based VLAN, MVR and QinQ
- IEEE 802.3ad LACP, Static Trunk support up to 14 trunks, up to 8 ports per trunk
- IGMP Snooping V1/V2/V3 and Querier port
- Up to 9K Jumbo Frame
- Rate Control and Storm Control for Broadcast/Multicast/Un-known Unicast
- QoS supports up to 8 priority queues per port, 802.1p/IP Precedence, IP ToS, IP DSCP, DiffServ, the queue scheduling supports WRR, Strict and Hybrid
- Advanced Security supports IEEE 802.1x, RADIUS, TACAS+, IP/MAC Filter
- Support Command Line, Web Management, Telnet, SNMP V1/V2c/V3, RMON, Secured Management supports HTTPS, SSL and SSHv2
- sFlow, NTP, LLDP, Port Mirroring, Cable Diagnostic, UPnP...
- IPv6 Features
- Event/Error Log
- Dual F/W images
- DHCP: Client, Relay/Option82, Snooping

**Note: Please see the most updated datasheet for the detail product specification. You can check the web site or contact the sales of the supplier.**

## 1.2 Product Specification

Hardware Specification		
Interface	Total Port	<b>28</b>
	10/100/1000 Mbps	<b>24</b>
	1G SFP/10G SFP	<b>2</b>
	Stacking slot	<b>2</b>
	Auto negotiation and Auto-MDIX	<b>Yes</b>
	Flow Control	<b>Backpressure for half duplex, 802.3x for full duplex</b>
	Console (RS-232)	<b>Yes</b>
LED	System (State / Color)	<b>Y</b>
	Port (State: Link/Act / Color)	<b>Y</b>
System	CPU	<b>416MHz</b>
	Flash	<b>16MB</b>
	SDRAM	<b>128MB</b>
	Packet Buffer	<b>32MB</b>
	Switching Capacity	<b>128Gbps non-blocking</b>
	Forwarding Architecture	<b>Store and forward</b>
	Package Forwarding Rate	<b>95.2Mpps</b>
	MAC Address Table	<b>16K</b>
	Jumbo Frame	<b>9K</b>
Power Requirement / Consumption	AC Input	<b>100-240V AC, 50/60Hz</b>
	Consumption - not include PSE	<b>25W</b>
Environment	Operating Temperature/ Degree C	<b>0~40</b>
	Relative Humidity at operating	<b>5~90% (non-condensing)</b>
	Storage Temperature / Degree C	<b>-20~80</b>
	Relative Humidity at storage	<b>5~90% (non-condensing)</b>
Mechanical	Dimension mm(H*W*D)	<b>44*440*331mm</b>
	Weight	<b>3.0kg</b>
Regular Compliance	CE, FCC Part 15 Class A	<b>Yes</b>

Software Specification	
Standard	IEEE 802.3 - 10Base-T
	IEEE 802.3u - 100Base-TX
	IEEE 802.3ab - 1000Base-T
	IEEE 802.3z - 1000Base-SX/LX
	IEEE 802.3x - Flow Control
	IEEE 802.1Q - VLAN
	IEEE 802.1p - Class of Service
	IEEE 802.1D - Spanning Tree
	IEEE 802.1w - Rapid Spanning Tree
	IEEE 802.1s - Multiple Spanning Tree
	IEEE 802.3ad - Link Aggregation Control Protocol (LACP)
	IEEE802.1v - Protocol VLAN
	IEEE 802.1AB - LLDP (Link Layer Discovery Protocol)
	IEEE 802.1X - Access Control
Port Configuration	Link State, Speed/Duplex, Auto-Nego, Flow Control
	Rate Control/Limit
VLAN	Port based and 802.1Q Tag based VLAN
	Maximum 4K VLAN Group, 4096 VLANs ID
	QinQ
	Private VLAN
	MVR (Multicast VLAN Registration)
	MAC based VLAN
	IP Subnet-based VLAN
	IEEE802.1v Protocol VLAN
	Voice VLAN
QoS	8 Physical priority queues
	Scheduling – WRR, Strict, Hybrid
	CoS: Port based, 802.1p, DSCP, TCP/UDP Port based
	Storm Control (Broadcast, Multicast, un-known Unicast)
Link Aggregation	Up to 13 LA Group, up to 16 ports per group
	Static and 802.3ad LACP
	Static Trunk
	Hash Algorithm Type (DA, SA, DA+SA MAC-based, SIP...)

Loop Protection	Protect the unexpected network loop by shutdown port
Spanning tree	IEEE 802.1D – Legacy Spanning Tree (STP)
	IEEE 802.1w – Rapid Spanning Tree (RSTP)
	IEEE 802.1s – Multiple Spanning Tree (MSTP)
	BPDU Guard, BPDU Filtering
Multicast	IGMP Snooping v1/v2/v3, MLD(Ipv6) Snooping v1/v2
	Maximum 8K Multicast Groups
	IGMP/MLD Querier, Router Port, Proxy, Immediate Leave
Traffic Mirroring	Port Mirror (1 to 1, 1 to N, N to 1)
	sFlow
MAC Address Table	Dynamic MAC address management
	Static MAC address
Security	Port Security (MAC-Port, IP-MAC-Port Binding)
	802.1x authentication (Port based, MAC address based)
	User Name Password Authentication by Local/Radius...
	Stacking Unit: max 16
	Up to 15 User Privilege Levels
	Access Management by IP
	IP Source Guard
	RADIUS
	TACACS+
	Guest VLAN
	DoS Defence
	SSHv1/SSHv2
	SSLv2/SSLv3/TLSv1
	Access Control List (L2/L3/L4)
Management	Web GUI Management, CLI (Console/Telnet/SSH)
	DHCP Client, Snooping, Relay/Option 82, BOOTP
	SNMP V1/V2c/V3, Trap, RMON
	Firmware upgrade by TFTP/HTTP
	Configuration Backup/Reload
	Link Layer Discovery Protocol (LLDP) by IPv4/v6 types
	System Log for event, warning and information
	NTP/SNTP



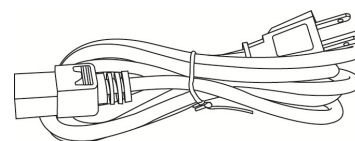
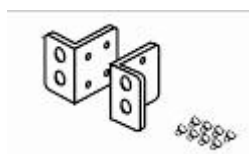
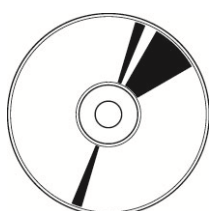
Maintenance	VeriPHY Diagnostic
	IPv4/V6 Ping Diagnostics
	CPU Monitor
	PD Status monitoring

**Note: We reserve the right to change the detail parameters listed in manual without earlier inform. Please always see the most updated datasheet for the detail product specification. You can check the web site or contact the sales of the supplier.**

### 1.3 Package Contents

Before you start to install this switch, please verify your package that contains the following items:

- One Network Switch
- One Power Cord
- One User Manual CD
- One pair Rack-mount kit + 8 Screws



## 2. Hardware Description

This section mainly describes the hardware of Full L2 Management Network Switch and gives a physical and functional overview on the certain switch.

### Front Panel

The front panel of the L2+ management switch consists of 24 10/100/1000 Base-TX RJ-45 ports and 2 Gigabit uplink SFP ports as well as the LED Indicators.



### LED Indicators

The LED Indicators present real-time information of systematic operation status. The following table provides description of LED status and its meaning.

LED	Color / Status	Description	No. of LEDs
Power	Amber On	Power on	Power
10/100/1000M	Green On	Link Up	24(1~24)
	Green Blinking	Data Activating	
SFP	Green On	linked to Power Device	25~26
	Green Blinking	Data Activating	25~26

### Rear Panel

The 3-pronged power plug is placed at the right side of rear panel of the switch which shown as below.



## **Hardware Installation**

The switch is usually mounted in the 19" rack, the rack is usually installed in IT room or other secured places. The switch supports AC power input and rack mount mounting. Make sure all the power cables, Ethernet cables, screws and the air circulation are well prepared and installed as below description.

### **AC Power Input**

Connect the attached power cord to the AC power input connector, the available AC power input is range from 100-264VAC.

### **Ethernet cable Request**

The wiring cable types are as below.

10 Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable, EIA/TIA-568 100-ohm (Max. 100m)

100 Base-TX: 2-pair UTP/STP Cat. 5 cable, EIA/TIA-568 100-ohm (Max. 100m)

1000 Base-T: 4-pair UTP/STP Cat. 5 cable, EIA/TIA-568 100-ohm (Max. 100m)

### **SFP Installation**

While install the SFP transceiver, make sure the SFP type of the 2 ends is the same and the transmission distance, wavelength, fiber cable can meet your request. It is suggested to purchase the SFP transceiver with the switch provider to avoid any incompatible issues.

The way to connect the SFP transceiver is to plug in SFP fiber transceiver slot fist. The SFP transceiver has 2 plug for fiber cable, one is TX (transmit), the other is RX (receive). Cross-connect the transmit channel at each end to the receive channel at the opposite end.

### **Rack mount Installation**

Attach the brackets to the device by using the screws provided in the Rack Mount kit.

Mount the device in the 19" rack by using four rack-mounting screws provided by the rack manufacturer.

### 3. Preparation for Management

The switch provides both in-band and out-band configuration methods.

**Out-band Management:** You can configure the switch via RS232 console cable if you don't attach your admin PC to your network, or if you lose network connection to your switch. It wouldn't be affected by network performance. This is so-called out-band management.

**In-Band Management:** You can remotely manage the switch via the Web browser, such as Microsoft Internet Explorer, or Mozilla, to configure and interrogate the switch from anywhere on the network.

Following topics are covered in this chapter:

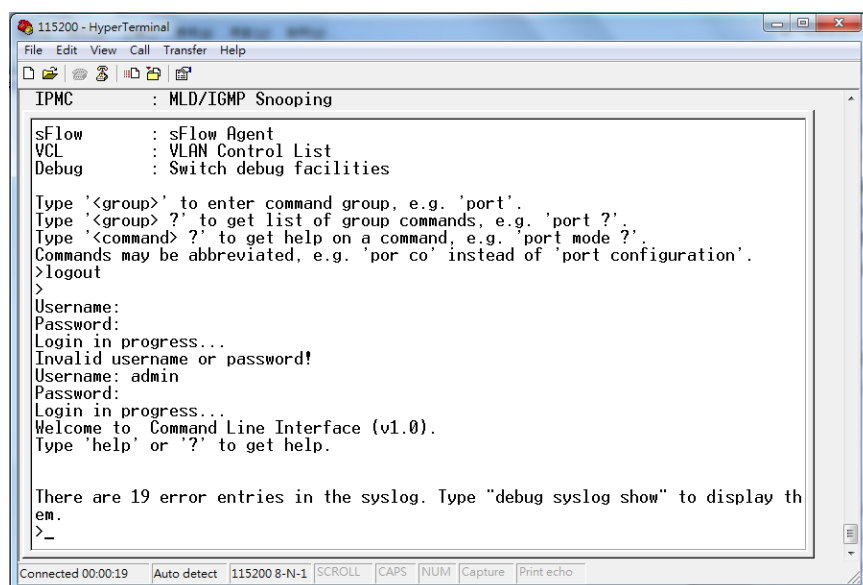
#### 3.1 Preparation for Serial Console

#### 3.2 Preparation for Web Interface

### 3.1 Preparation for Serial Console

In the package, there is one RS-232 console cable. Please attach one end of the console cable to your PC COM port, while the other end to the console port of the switch.

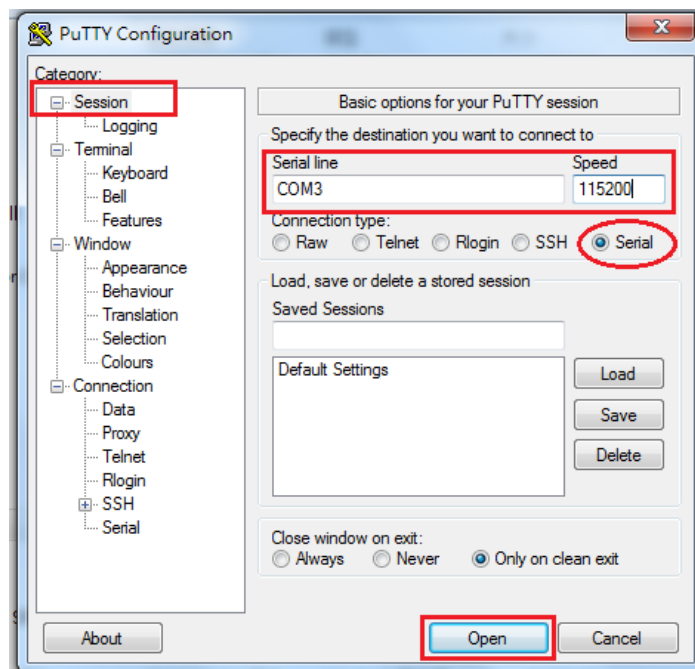
1. Go to Start -> Program -> Accessories -> Communication -> Hyper Terminal
2. Give a name to the new console connection.
3. Choose the COM name
4. Select correct serial settings. The serial settings of the switch are as below:  
Baud Rate: 115200 / Parity: None / Data Bit: 8 / Stop Bit: 1
5. After connected, you can see Switch login request.
6. Login the switch. The default username is "**admin**", password "**admin**".



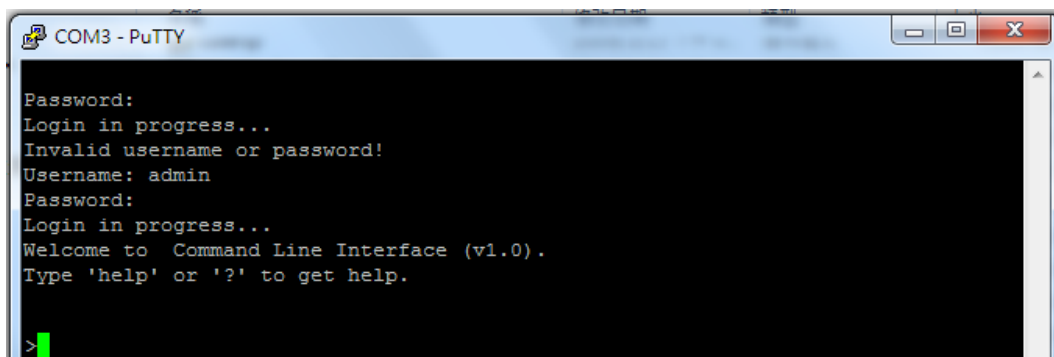
**Figure 3-1 Hyper Terminal Console Screen**

Note: The Win 7 or later OS version doesn't provide Console Terminal tool, please download the tool, Hyper Terminal from Microsoft web site or other terminal tools,

such as PuTTY for console connection. Type Hyper Terminal or Putty in Google web site to find the link to download.



**Figure 3-2 Putty Configuration**



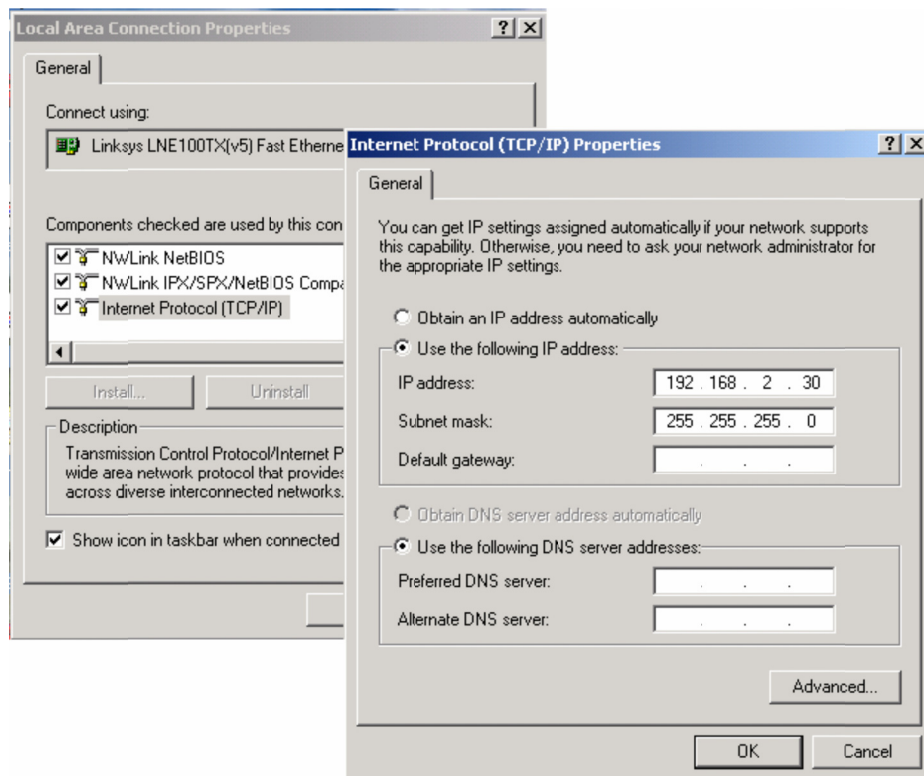
**Figure 3-3 Putty Login Screen**

### 3.2 Preparation for Web Interface

The web management page allows you to use a standard web-browser such as Microsoft Internet Explorer, Google Chrome or Mozilla Firefox, to configure and interrogate the switch from anywhere on the network.

Before you attempt to use the web user interface to manage switch operation, verify that your switch is properly installed on your network and that every PC on this network can access the switch via the web browser.

1. Verify that your network interface card (NIC) is well-functioned, and your operating system supports TCP/IP protocol.
2. Power on the switch and use the RJ-45 cable to connect to your computer.
3. The switch default IP address is 192.168.2.1. The switch and the connected PC should locate within the same IP subnet.
4. Change your computer's IP address to 192.168.2.XX (any number besides 1) or other IP address which is located in the 192.168.2.x (For example: IP Address: 192.168.2.30; Subnet Mask: 255.255.255.0) subnet.



Launch the web browser and Login.

5. Launch the web browser (Internet Explorer or Mozilla Firefox) on the PC.
6. Type **http://192.168.2.1** (or the IP address of the switch). And then press **Enter**.
7. The login screen will appear next.
8. Key in the password. Default user name and password are both **admin**.

If you can't login the switch, the following steps can help you to identify the problem.

1. Switch to DOS command mode and type the "**ipconfig**" to check the NIC's setting. Type the "**ping 192.168.2.1**" to verify a normal response time.
2. Check the security & firewall settings of your computer.
3. Try different Web-browser, like the Mozilla or Google Chrome.

### 3.3 Preparation for Telnet/SSH Interface

If your Window OS is Win XP, Win 2000 or any early versions, you can access the Telnet console by default command. If your OS is Window 7 or later version, please download the terminal tool, such as HyperTerminal or Putty.

The switch support both Telnet and SSH console. The SSH console can be treated as secured Telnet connection, need to enable the SSH feature in "Security / Switch / SSH".

#### Traditional way for Telnet Connection

1. Go to Start -> Run -> cmd. And then press **Enter**
2. Type the **Telnet 192.168.2.1** (or the IP address of the switch). And then press **Enter**.

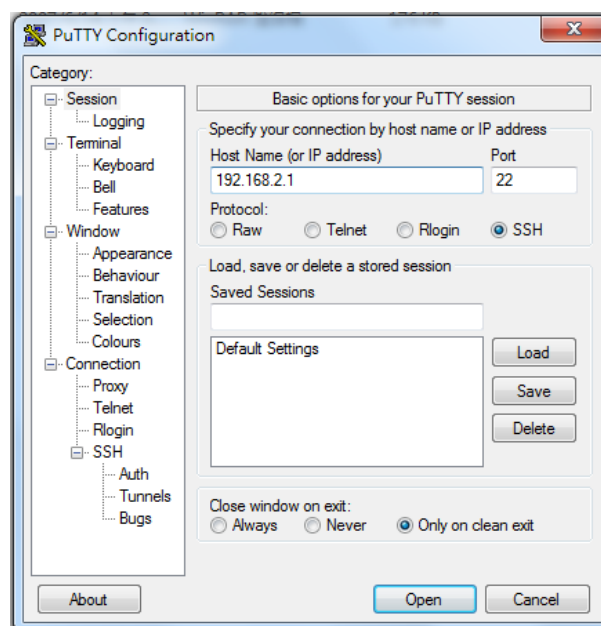
#### Access Telnet or SSH by Terminal tool, Putty.

##### 1. Open Telnet/SSH Client/PuTTY

In the **Session** configuration, choose the Telnet/SSH in Protocol field.

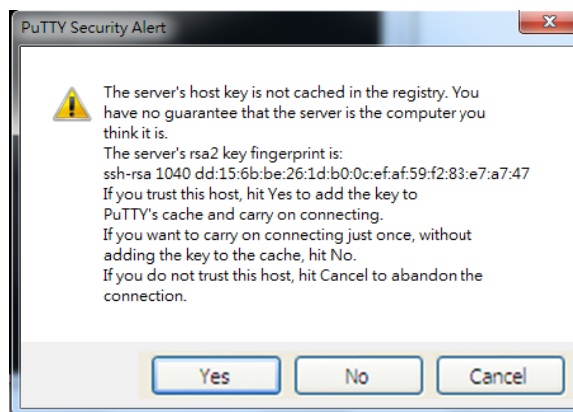
In the **Session** configuration, enter the **Host Name** (IP Address of your switch) and **Port number** (default Telnet =23, SSH = 22).

Then click on "**Open**" to start the SSH session console.

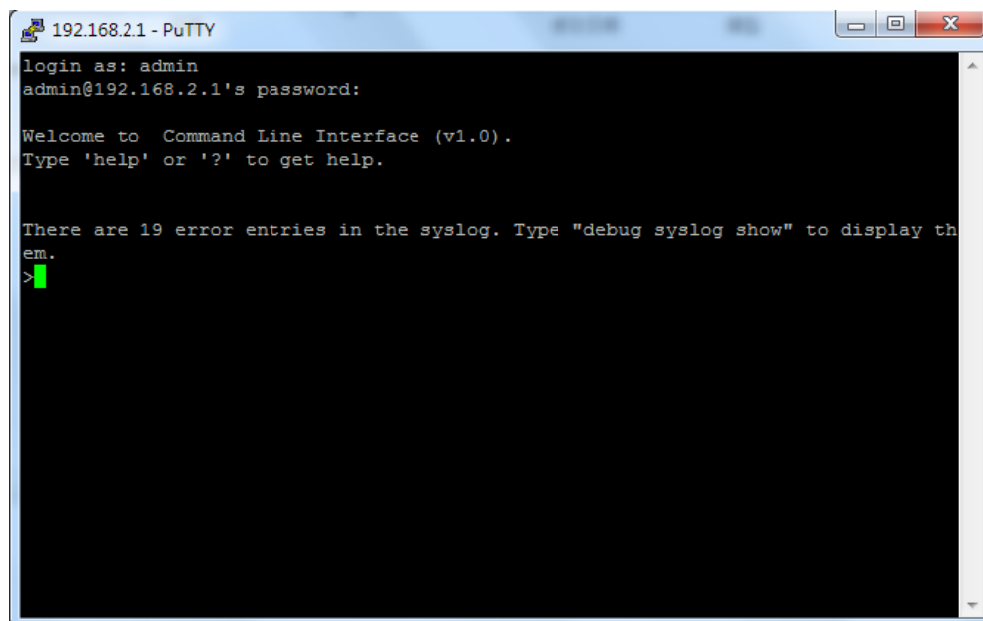


2. After click on **Open**, then you can see the cipher information in the popup screen. Press **Yes** to accept the Security Alert.

If you choose **Telnet** connection, there is no such cipher information and window. It goes to next step directly.



3. After few seconds, the Telnet/SSH connection is established, the login page of Telnet/SSH is the same as console. The command line of Telnet, SSH and console are all the same.





## 4. Feature Configuration - Web UI

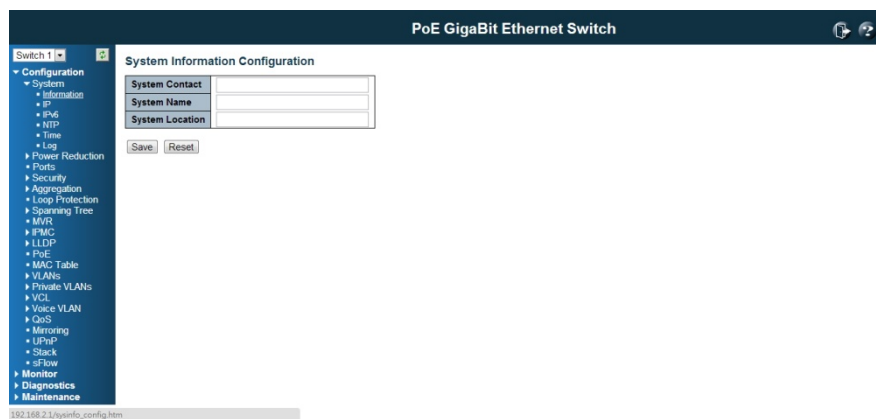
The switch provides abundant software features. After login to the switch, you can start configuring the settings or monitoring the status. This is one question mark on the right top of the screen, you can also click the question mark to get help from the system.

Following are the Web UI configuration guide for your reference.

### 4.1 System Configuration

#### 4.1.1 System Information

This page shows the system information and allows you to configure the new settings.



#### 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

It's the 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.

#### Time zone Offset

Provide the time zone offset relative to UTC/GMT.

The offset is given in minutes east of GMT. The valid range is from **-720** to **720** minutes.

## Buttons:

**Save:** Click to save changes

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

### 4.1.2 IP Configuration:

Configure the switch-managed IP information on this page.

	Configured	Current
DHCP Client	<input type="checkbox"/>	<input type="checkbox"/> Renew
IP Address	192.168.2.1	192.168.2.1
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy ☐

Save Reset

The **Configured** column is used to view or change the IP configuration.

The **Current** column is used to show the active IP configuration.

## DHCP Client

Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

## IP Address

Provide the IP address of this switch in dotted decimal notation.

## IP Mask

Provide the IP mask of this switch dotted decimal notation.

## IP Router

Provide the IP address of the router in dotted decimal notation.

## NTP

Provide the IP address of the NTP Server in dotted decimal notation.

## DNS Server

Provide the IP address of the DNS Server in dotted decimal notation.

## VLAN ID

Provide the managed VLAN ID. The allowed range is **1** to **4095**.

## DNS Proxy

When DNS proxy is enabled, the switch will relay DNS requests to the current configured DNS server on the switch, and reply as a DNS resolver to the client device on the network.

## Buttons

**Save:** Click to save changes

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

**Renew:** Click to renew DHCP. This button is only available if DHCP is enabled.

### 4.1.3 IPv6 Configuration

Configure the switch-managed IPv6 information on this page:

	Configured	Current
Auto Configuration	<input checked="" type="checkbox"/>	<input type="button" value="Renew"/>
Address	192.168.2.1	Link-Local Address: fe80::203:ceff:fe22:6588
Prefix	96	96
Router	192.168.2.1	

The **Configured** column is used to view or change the IPv6 configuration.

The **Current** column is used to show the active IPv6 configuration.

## Auto Configuration

Enable IPv6 auto-configuration by checking this box. If fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.

## Address

Provide the IPv6 address of this switch. 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 only appear once. It can also represent a legally valid IPv4 address. For example, ':::192.1.2.34'.

## Prefix

Provide the IPv6 Prefix of this switch. The allowed range is **1** to **128**.

## Router

Provide the IPv6 gateway address of this switch. 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 only appear once. It can also represent a legally valid IPv4 address. . For example, '::192.1.2.34'.

## Buttons

**Save:** Click to save changes

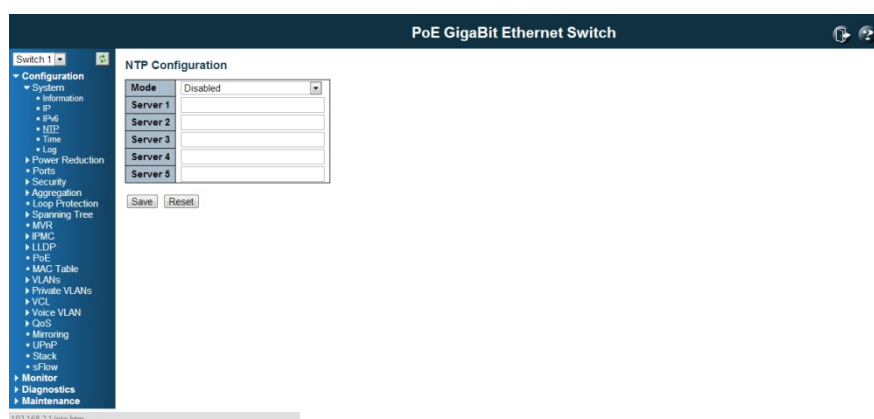
**Reset:** Click to undo any changes made locally and revert to previously saved values

**Renew:** Click to renew IPv6 AUTOCONF. This button is only available if IPv6 AUTOCONF is enabled.

### 4.1.4 NTP Configuration:

NTP is short of Network Time Protocol. Network Time Protocol (NTP) is used to synchronize time clocks on the internet. You can configure NTP Servers' IP address here to synchronize the clocks of the remote time server on the network.

This page indicates the NTP mode operation:



## Mode

The possible modes are:

**Enable** NTP mode operation. When NTP mode operation is enabled, the agent forwards NTP messages between the clients and the server when they are not on the same subnet domain.

**Disable** NTP mode operation.

## Server #

Provide the NTP IPv4 or IPv6 address of this switch. 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 only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

## Buttons

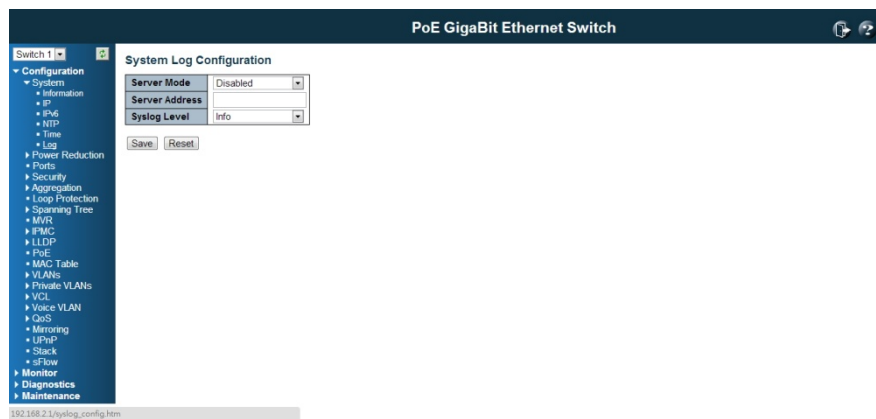
**Save:** Click to save changes

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

### 4.1.5 System Log Configuration:

System Log is useful to provide system administrator monitors the switch events history. The switch supports syslog server mode. User can install the syslog server in one computer, then configure the server address and event types in the switch's system log configuration. When the events occur, the switch will send information or warning message to the syslog server. The administrator can analysis the system logs recorded in the syslog server to find out the cause of the issues.

The switch Web UI allows you to enable the Syslog Server, assign the IP address and assign the syslog level.



#### 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 to the 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:

**Enable** server mode operation.

**Disable** server mode operation.

#### Server Address

Indicates the IPv4 host address of syslog server. If the switch provides DNS feature, it also can be a host name.

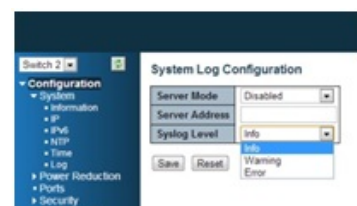
#### Syslog Level

Indicates what kind of message will send to syslog server. Possible modes are:

**Info:** Send information, 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

## 4.2 Power Reduction

### 4.2.1 LED Power Reduction Configuration

#### LEDs Intensity

The LEDs power consumption can be reduced by lowering the LEDs intensity. LEDs intensity for example could be lowered during night time, or they could be turn completely off. It is possible to configure 24 different hours of the day, at where the LEDs intensity should be set.

#### LED Power Reduction Configuration

##### LED Intensity Timers

Delete	Time	Intensity
<input type="checkbox"/>	00:00 ▼	20 ▼ %

Add Time

##### Maintenance

On time at link change	On at errors
10	Sec. <input type="checkbox"/>

Save

Reset

#### Time

The time at which the LEDs intensity shall be set. The time setting is step by one hour.

#### 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 push button has been pushed.

##### Maintenance

On time at link change	On at errors
20	Sec. <input checked="" type="checkbox"/>

Save

Reset

## Buttons

**Save:** Click to save changes

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

### 4.2.2 EEE Configuration:

This page allows the user to inspect and configure the current EEE port settings:

The screenshot shows the configuration interface for a PoE GigaBit Ethernet Switch. The left sidebar contains a navigation menu with categories like Configuration, System, Power Reduction, Security, Aggregation, Loop Protection, Spanning Tree, MVR, IPMG, LLDP, PoE, MAC Table, VLANs, Private VLANs, VCL, Voice VLAN, QoS, Mirroring, URP, Stack, sFlow, Monitor, Diagnostics, and Maintenance. The main area is titled 'EEE Configuration for Switch 1' and features a table with two columns: 'Port' and 'Enabled'. The 'Port' column lists ports from 1 to 26, and the 'Enabled' column contains checkboxes. All checkboxes are currently unchecked. Below the table are 'Save' and 'Reset' buttons. At the bottom left, the URL '192.168.2.1/eee\_config.htm' is visible.

Port	Enabled
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>
9	<input type="checkbox"/>
10	<input type="checkbox"/>
11	<input type="checkbox"/>
12	<input type="checkbox"/>
13	<input type="checkbox"/>
14	<input type="checkbox"/>
15	<input type="checkbox"/>
16	<input type="checkbox"/>
17	<input type="checkbox"/>
18	<input type="checkbox"/>
19	<input type="checkbox"/>
20	<input type="checkbox"/>
21	<input type="checkbox"/>
22	<input type="checkbox"/>
23	<input type="checkbox"/>
24	<input type="checkbox"/>
25	<input type="checkbox"/>
26	<input type="checkbox"/>

EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted, all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange information about the devices wakeup time using the LLDP protocol.

For maximizing the power saving, the circuit won't be powered up once transmit data are ready for a port, but is instead queued until 3000 bytes of data are ready to be transmitted. For not introducing a large delay in case that data less than 3000 bytes shall be transmitted, data are always transmitted after 48 us, giving a maximum latency of 48 us + the wakeup time.

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.

## Port

The switch port number of the logical EEE port.

## EEE Enabled

Controls whether EEE is enabled for this switch port.

## EEE Urgent Queues

Queues set will activate transmission of frames as soon as any data is available. Otherwise the queue will postpone the transmission until 3000 bytes are ready to be transmitted.

## Buttons

**Save:** Click to save changes

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

## 4.3 Port Configuration:

This page displays current port configurations and link status. Some of the Ports' settings can also be configured here.

Port	Link	Speed		Flow Control		Maximum Frame Size	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx			
1	Down	Auto		X	X	10056	Discard	Disabled
2	1Gfdx	Auto		X	X	10056	Discard	Disabled
3	Down	Auto		X	X	10056	Discard	Disabled
4	Down	Auto		X	X	10056	Discard	Disabled
5	Down	Auto		X	X	10056	Discard	Disabled
6	Down	Auto		X	X	10056	Discard	Disabled
7	Down	Auto		X	X	10056	Discard	Disabled
8	Down	Auto		X	X	10056	Discard	Disabled
9	Down	Auto		X	X	10056	Discard	Disabled
10	Down	Auto		X	X	10056	Discard	Disabled
11	Down	Auto		X	X	10056	Discard	Disabled
12	Down	Auto		X	X	10056	Discard	Disabled
13	Down	Auto		X	X	10056	Discard	Disabled
14	Down	Auto		X	X	10056	Discard	Disabled
15	Down	Auto		X	X	10056	Discard	Disabled
16	Down	Auto		X	X	10056	Discard	Disabled
17	Down	Auto		X	X	10056	Discard	Disabled
18	Down	Auto		X	X	10056	Discard	Disabled
19	Down	Auto		X	X	10056	Discard	Disabled
20	Down	Auto		X	X	10056	Discard	Disabled
21	Down	Auto		X	X	10056	Discard	Disabled
22	Down	Auto		X	X	10056	Discard	Disabled
23	Down	Auto		X	X	10056	Discard	Disabled
24	Down	Auto		X	X	10056	Discard	Disabled
25	Down	10Gbps FDX		X	X	10056		
26	Down	10Gbps FDX		X	X	10056		

## Port

This is the port number for this switch.

## Link

The current link state is displayed graphically.

Green indicates the link is up and red means down.

## Current Link Speed

Provides the current link speed of the port.

Ex: 1Gfdx: 1G indicates the Gigabit Speed, fdx indicates the Full Duplex Mode.



## Configured Link Speed

Select any available link speed for the given switch port.

**Auto Speed:** selects the highest speed that is compatible with a link partner.

**Disabled:** disables the switch port operation.

## Fiber Speed

Configure speed for fiber port.

**Note:** Port speed for the Copper ports will automatically be set to Auto when dual media is selected.

**Disable** SFPs (Copper port only).

**SFP-Auto** automatically determines the speed at 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.

1000-X force SFP speed to 1000-X.

100-FX force SFP speed to 100-FX.

## 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.

The switch supports up to 409K Jumbo Frame.

## Excessive Collision Mode

Configure port transmit collision behavior.

**Discard:** Discard frame after 16 collisions (default).

**Restart:** Restart back off algorithm after 16 collisions.

## Power Control

The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port.

**Disabled:** All power savings mechanisms disabled.

**ActiPHY:** Link down power savings enabled.

**Perfect Reach:** Link up power savings enabled.

**Enabled:** Both link up and link down power savings enabled.

## 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. Any changes made locally will be undone.

## 4.4 Security Configuration:

The Security Configuration feature includes 3 sub-titles, Switch, Network and AAA.

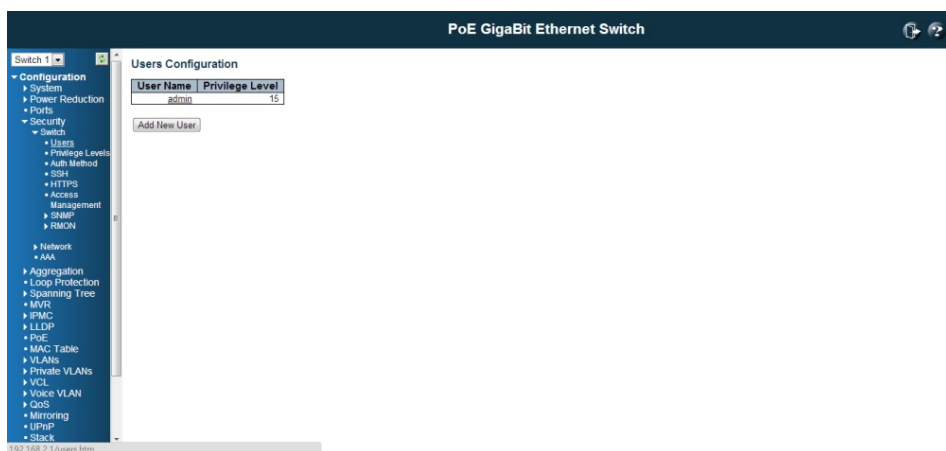
### 4.4.1 Security / Switch

The switch settings includes User Database, Privilege Levels, Authentication Method, SSH, HTTPs, Access Management, SNMP and RMON setting. Following are the topic and configuration guide.

#### 4.4.1.1 Security / Switch / Users Configuration

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 the browser and reopen it.

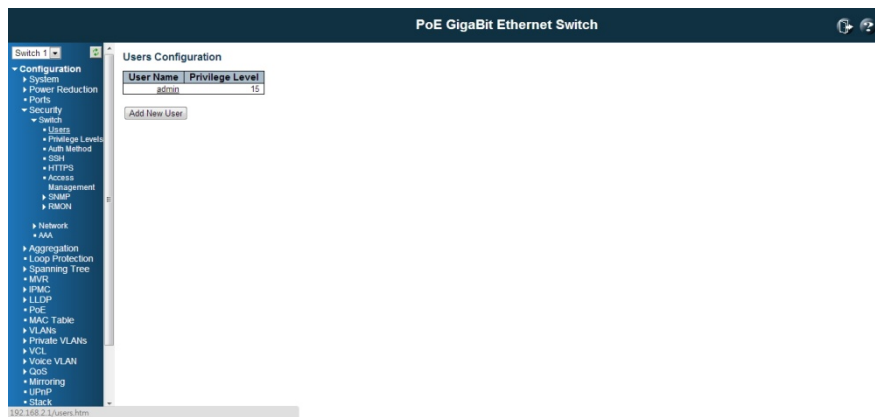
This page configures a user: This is also a link to [Add User](#) & [Edit User](#)



### Add New User/Edit User

Click "**Add New User**", the configuration page goes to "Add User" screen. You can see the User Setting table, follow the below instruction to fill the table.

Click the created User Name, the page goes to "Edit User" screen, you can change the settings on it.



## User Name

A string identifying the user name that this entry should belong to. The allowed string length is **1** to **32**. 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 **32**.

## 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.

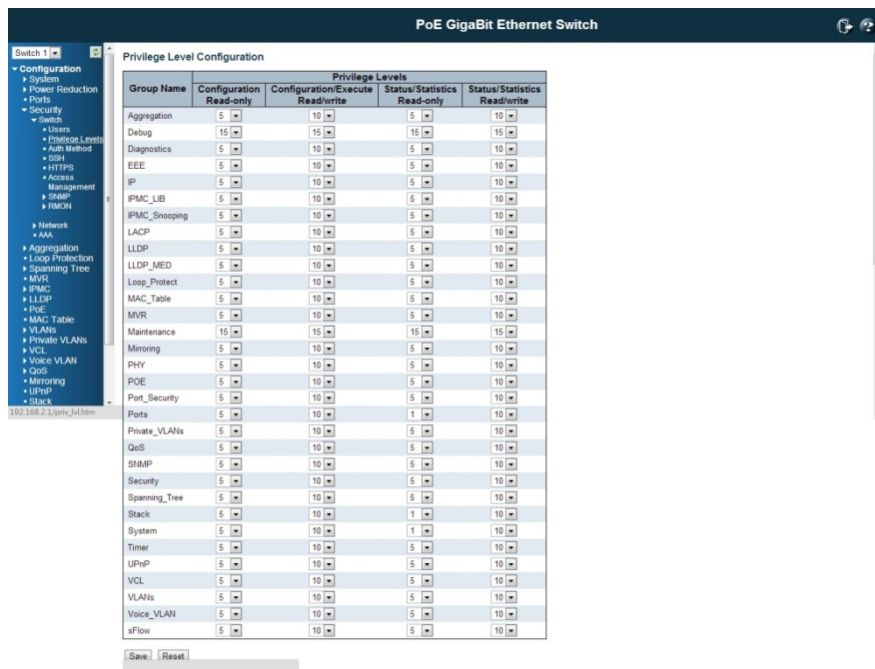
Check the next chapter to see how to configure privilege level.

## Buttons

**Add new user:** Click to add a new user.

### 4.4.1.2 Security / Switch / Privilege Levels Configuration:

This page provides an overview of the privilege levels.



## 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, Time zone, Log.

**Security:** Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and 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.

**Debug:** Only present in CLI.

## 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.

**Insufficient Privilege Level:** If you login with lower level privilege and try to access the high privilege level configuration feature, the following message, "Insufficient Privilege Level" will appear. If you want continue, be sure that you have the valid privilege level.

## Insufficient Privilege Level

The web page is non-accessable. Please use the valid privilege level.

## Buttons

**Save:** Click to save changes

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

### 4.4.1.3 Security / Switch / 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:

Client	Authentication Method	Fallback
console	local	<input type="checkbox"/>
telnet	local	<input type="checkbox"/>
ssh	local	<input type="checkbox"/>
web	local	<input type="checkbox"/>

Save Reset

#### Client

The management client for which the configuration below applies.

#### Authentication Method

Authentication Method can be set to one of the following values:

**none:** authentication is disabled and login is not possible.

**local:** use the local user database on the switch for authentication.

**RADIUS:** use a remote RADIUS server for authentication.

**TACACS+ :** use a remote TACACS server for authentication.

#### Authentication Method Configuration

Client	Authentication Method	Fallback
console	local	<input type="checkbox"/>
telnet	none	<input type="checkbox"/>
ssh	local	<input type="checkbox"/>
web	RADIUS	<input type="checkbox"/>
	TACACS+	<input type="checkbox"/>

Save Reset

#### Fallback

Enable fallback to local authentication by checking this box.

If none of the configured authentication servers are alive, the local user database is used for authentication.

This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.

## Buttons

**Save:** Click to save changes

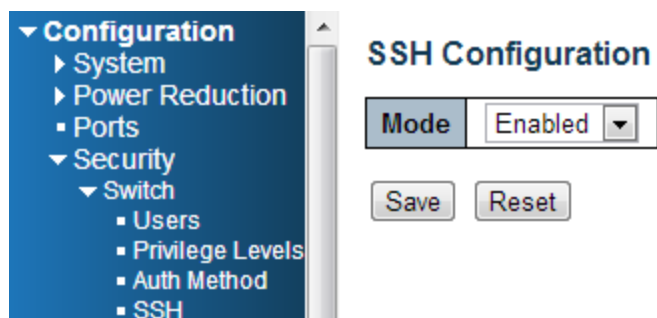
**Reset:** Click to undo any changes made locally and revert to previously saved values

### 4.4.1.4 Security /Switch / SSH Configuration

With SSH, you can remotely connect to the switch by command line interface. The SSH connection can secure all the configuration commands you sent to the switch. It is also known as secured Telnet console.

To access the switch by SSH, you should install SSH client on your computer, such as PuTTY console tool. In the switch side, the switch acts as SSH server for user login, and you can Enable or Disable SSH on this page.

Please check the chapter 3.3 Preparation for Telnet/SSH connection to see how to manage the switch through SSH console.



## Mode

Indicates the SSH mode operation. Possible modes are:

**Enable:** 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

### 4.4.1.5 Security / Switch / HTTPS Configuration

The web management page also provides secured management HTTPS login. All the configuration commands will be secured and will be hard for the hackers to sniff the login password and configuration commands.

This page allows you to configure HTTPS mode.

### Mode

Indicates the HTTPS mode operation. Possible modes are:

**Enable:** Enable HTTPS mode operation.

**Disabled:** Disable HTTPS mode operation.

### Automatic Redirect

Indicates the HTTPS redirect mode operation. Automatically redirect web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

**Enable:** 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

## 4.4.1.6 Security / Switch / Access Management Configuration

The Access Management mode allows user to limit the switch access with specific range of IP address and disable some remote management service, such HTTP, HTTPS, SNMP, Telnet and SSH. This feature is important while user installed the switch on network. After enabled the Access Management, only the pre-configured IP address or a range of IP address can access the switch management interface, and only the available service can be accessed.

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

Example of the below figure, only the IP Addresses range from 192.168.2.101 to 192.168.2.200 can access the switch's management interface. The available services are HTTP, HTTPS, SNMP, Telnet and SSH. For example, if there is one IP address, 192.168.2.201 try to open the web management interface, it is not allowed.

### Access Management Configuration

Mode: Enabled ▼

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
<input type="checkbox"/>	192.168.2.101	192.168.2.200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New Entry

Save Reset

### Mode

Indicates the access management mode operation. Possible modes are:

**Enable:** 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.

### 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.

With the Start and End IP address, you can assign a range of IP addresses.

### 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 group entry

**Save:** Click to save changes

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

#### 4.4.1.7 Security / Switch / SNMP

**Simple Network Management Protocol (SNMP)** is a protocol used for exchanging management information between network devices. The switch supports SNMP and equips lots of OIDs for remote management. All the OIDs are unique and corresponding to one feature/command.

The switch can support SNMP V1, V2c and V3. The following commands show how to configure SNMP and its related parameters.



The screenshot shows the configuration page for a PoE GigaBit Ethernet Switch. The left sidebar contains a tree view of configuration categories: Configuration, System, Power Reduction, Ports, Security, Switch, Users, Privilege Levels, Auth Method, SSH, HTTPS, Access Management, SNMP, Switched, Communities, Users, Groups, Views, Access, RMON, Network, MAC, Aggregation, Loop Protection, Spanning Tree, MVR, RMC, LLDP, PCE, MAC Table, VLANs, Private VLANs, and VCL. The main content area is titled 'SNMP System Configuration' and contains two sections: 'SNMP System Configuration' and 'SNMP Trap Configuration'.

**SNMP System Configuration**

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	80000745017800001

**SNMP Trap Configuration**

Trap Mode	Disabled
Trap Version	SNMP v1
Trap Community	public
Trap Destination Address	
Trap Destination IPv6 Address	
Trap Authentication Failure	Enabled
Trap Link-up and Link-down	Enabled
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

At the bottom of the configuration area are 'Save' and 'Reset' buttons.

## Mode

Indicates the SNMP mode operation. Possible modes are:

**Enable:** Enable SNMP mode operation.

**Disabled:** Disable SNMP mode operation.

## Version

Indicates the SNMP supported version. Possible versions are:

**SNMPv1:** Set SNMP supported version 1.

**SNMPv2c:** Set SNMP supported version 2c.

**SNMPv3:** 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.

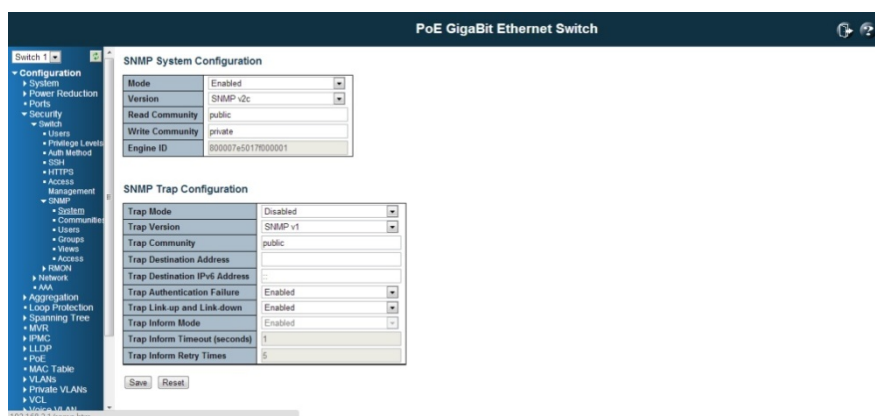
The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a 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.

## SNMP Trap Configuration

Configure SNMP trap on this page.



## Trap Mode

Indicates the SNMP trap mode operation. Possible modes are:

**Enable:** Enable SNMP trap mode operation.

**Disabled:** Disable SNMP trap mode operation.

## Trap 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.

## Trap Destination Address

Indicates the SNMP trap destination address.

## Trap Destination IPv6 Address

Provide the trap destination IPv6 address of this switch. 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 only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

## Trap Authentication Failure

Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are:

**Enable:** SNMP trap authentication failure.

**Disabled:** Disable SNMP trap authentication failure.

## Trap Link-up and Link-down

Indicates the SNMP trap link-up and link-down mode operation. Possible modes are:

**Enable:** Enable SNMP trap link-up and link-down mode operation.

**Disabled:** Disable SNMP trap link-up and link-down mode operation.

### Trap Inform Mode

Indicates the SNMP trap inform mode operation. Possible modes are:

**Enable:** 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:

**Enable:** 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.

### Buttons

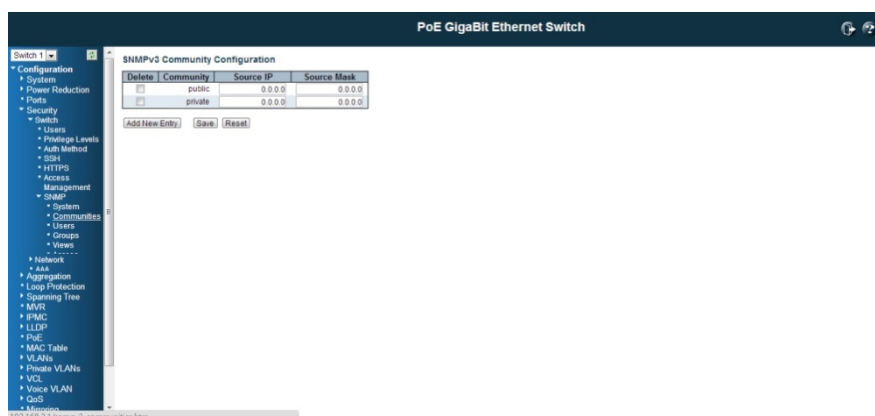
**Save:** Click to save changes

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

### SNMPv3 Community Configuration

In SNMP V3, it is start to support User Name and its privilege. You can configure SNMPv3 community table on this page:

The entry index key is Community.



## 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

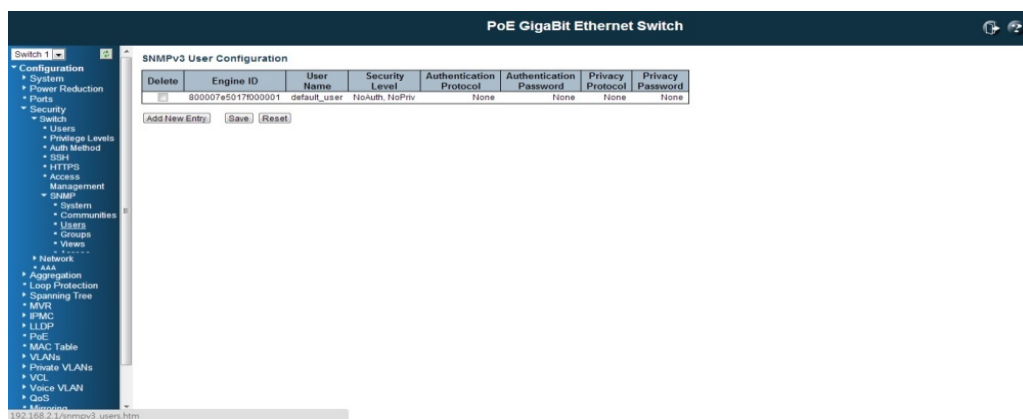
**Add new community:** Click to add a new community entry

**Save:** Click to save changes

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

## SNMPv3 User Configuration

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



## 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 USM User Engine ID and USM User Name are the entry's keys. In a simple agent, USM User Engine ID is always that agent's own SNMP Engine ID value. The value can also take the value of the SNMP Engine ID 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.

## 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 user:** Click to add a new user entry

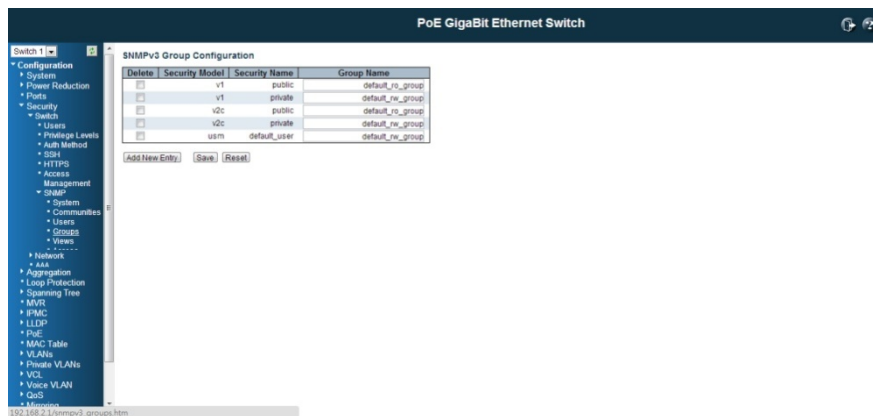
**Save:** Click to save changes

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

## SNMPv3 Group Configuration

Configure SNMPv3 group table on this page:

The entry index keys are **Security Mode** and **Security Name**.



## 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

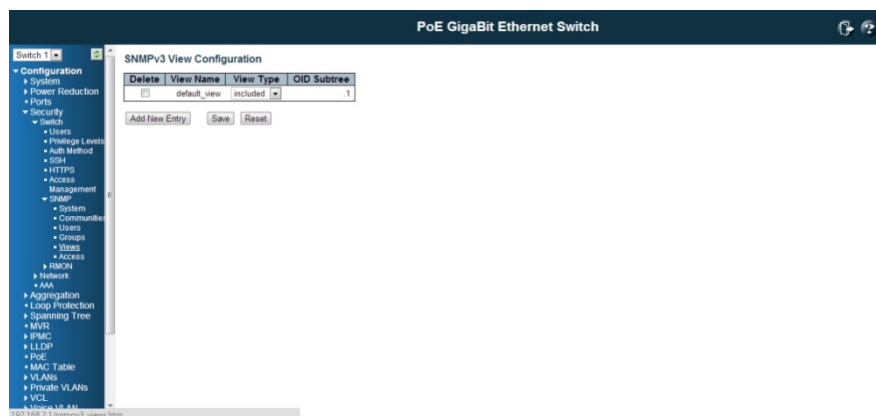
**Add new group:** Click to add a new group entry

**Save:** Click to save changes

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

## SNMPv3 View Configuration

Configure SNMPv3 view table on this page.



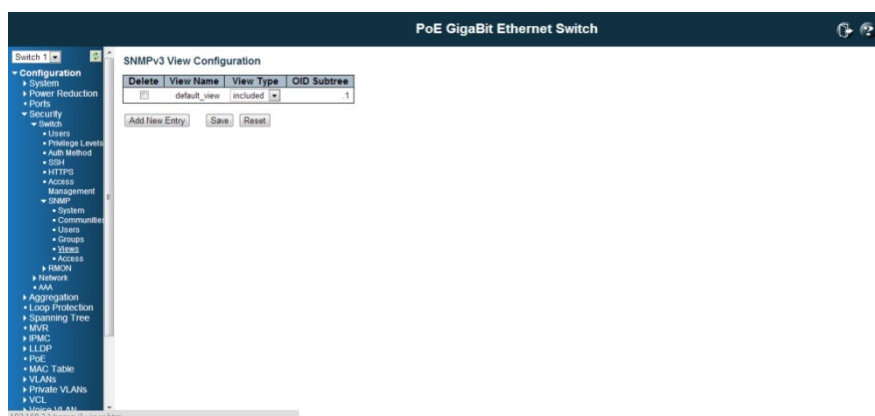
The entry index keys are **View Name** and **OID Sub-tree**.

## 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 sub-tree should be included.

**excluded:** An optional flag to indicate that this view sub-tree 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 sub-tree should overstep the 'excluded' view entry.

## OID Subtree

The OID defining the root of the sub-tree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (\*).

## Buttons

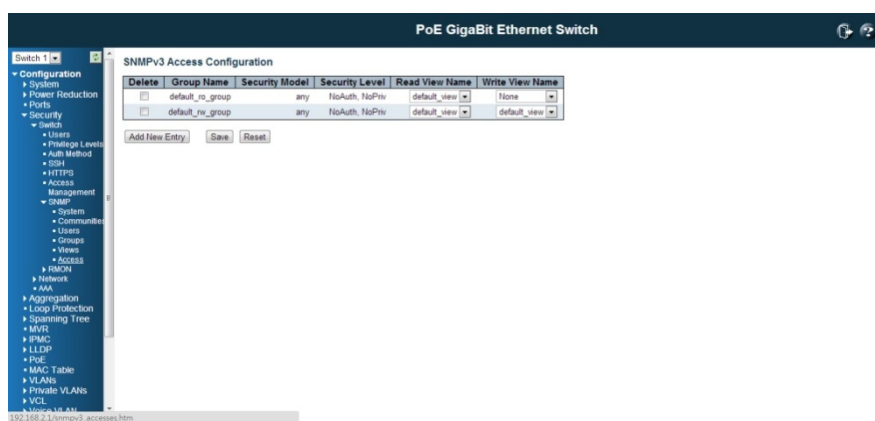
**Add new view:** Click to add a new view entry

**Save:** Click to save changes

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

## SNMPv3 Access Configuration

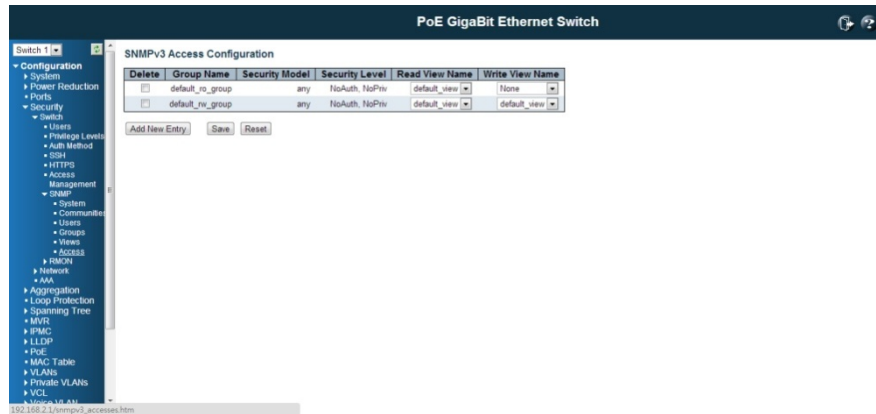
Configure SNMPv3 access table on this page. The entry index keys are **Group Name**, **Security Model**, and **Security Level**.





## 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.

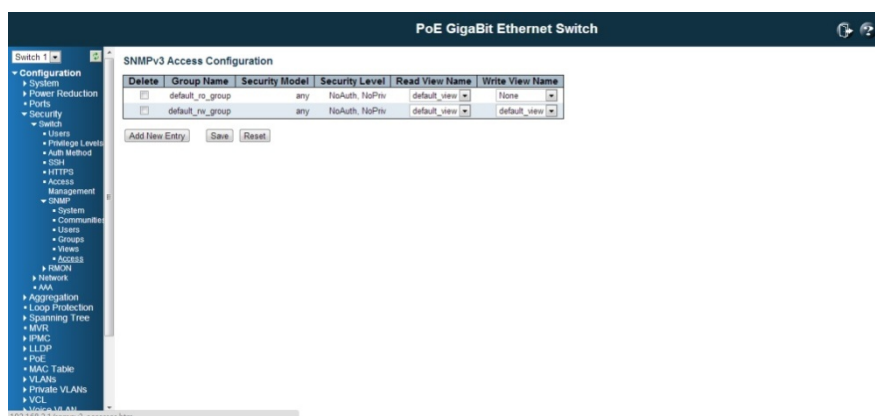
**Auth,Priv:** Authentication and privacy.

## 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 access:** 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

### 4.4.1.8 RMON Statistics Configuration

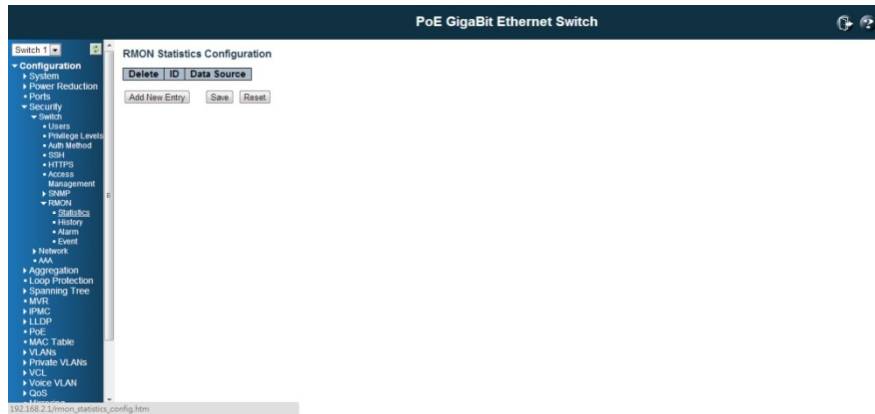
RMON is the abbreviation of Remote Monitoring On Network. An RMON implementation typically operates in a client/server model. Monitoring device (Probe) contains RMON software agents that collect information of the system and ports. The RMON software agent acts as server, and the network management system (NMS) that communicate with it acts as client. The RMON agent of the switch supports 4 groups, such as the Statistics, History, Alarm and Event.

RMON Group	Function	Elements
<b>Statistics</b>	Contains statistics measured by the probe for each monitored interface on this device.  Real-time LAN statistics e.g. utilization, collisions, CRC errors	Packets dropped, packets sent, bytes sent (octets), broadcast packets, multicast packets, CRC errors, undersize packets, oversize packets, fragments, jabbers, collisions, and counters for packets ranging from 64, 65 to 127, 128 to 255, 256 to 511, 512 to 1023, and 1024 to 1518 bytes.
<b>History</b>	Records periodic statistical samples from a network and stores for retrieval.	History of above Statistics.
<b>Alarm</b>	Definitions for RMON SNMP traps to be sent when statistics exceed defined thresholds	Interval for sampling, particular variable, sample type, value of statistics during the last sampling period, startup alarm, rising threshold, rising index, falling threshold, falling index.
<b>Events</b>	Controls the generation and notification of events from this device.	Event index, log index, event log time, event description

The NMS can get the above information through remotely polling. The information from the switch can be collected, analyzed and displayed as table or graphic...etc.

## RMON Statistics Configuration

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



### 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  $1000 * (\text{switch ID} - 1)$ , 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

## RMON History Configuration

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



## 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

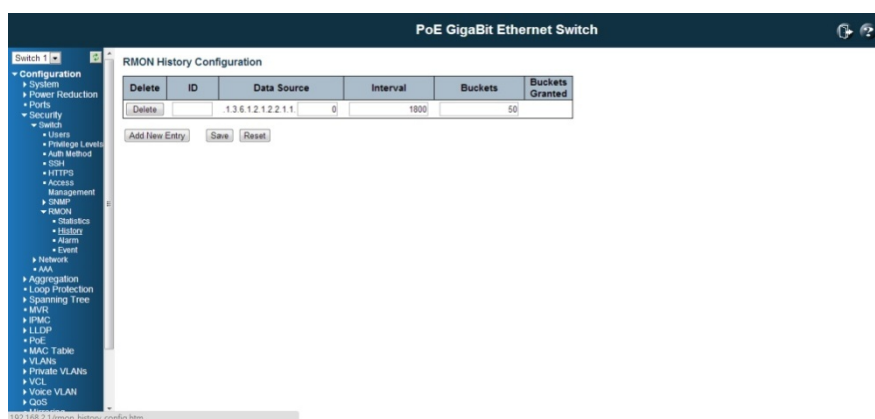
Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

## 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

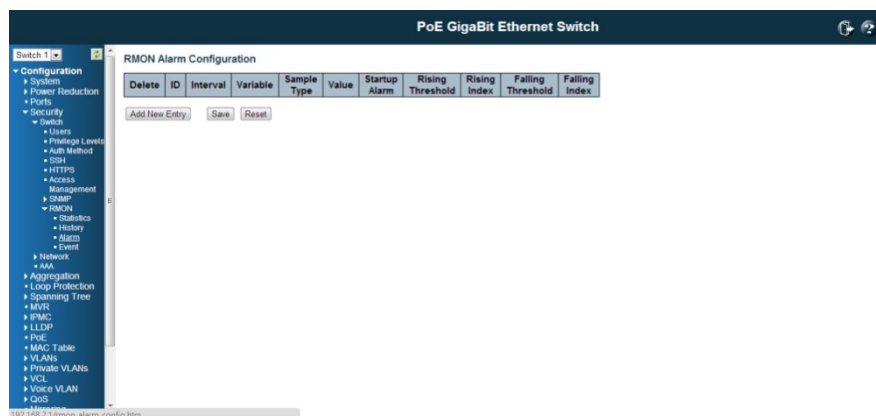
**Add new entry:** Click to add a new community entry.

**Save:** Click to save changes.

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

## RMON Alarm Configuration

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



### 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.

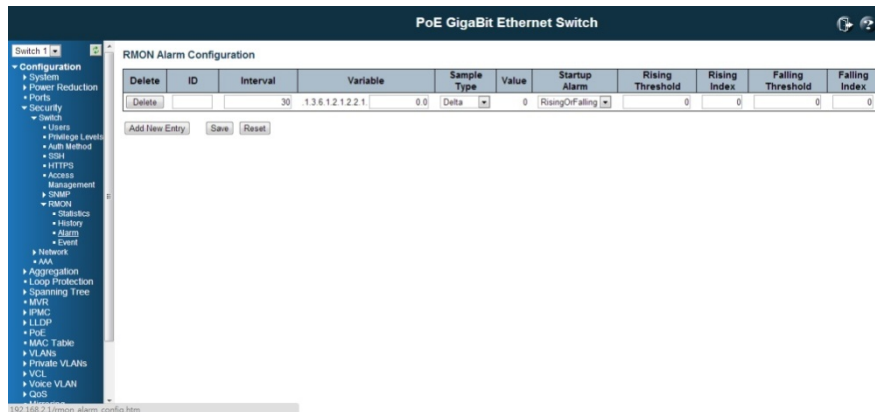
**OutUcastPkts:** The number of uni-cast packets that request to transmit.

**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 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:

**Rising:** Trigger alarm when the first value is larger than the rising threshold.

**Falling:** Trigger alarm when the first value is less than the falling threshold.

**RisingOrFalling:** Trigger 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

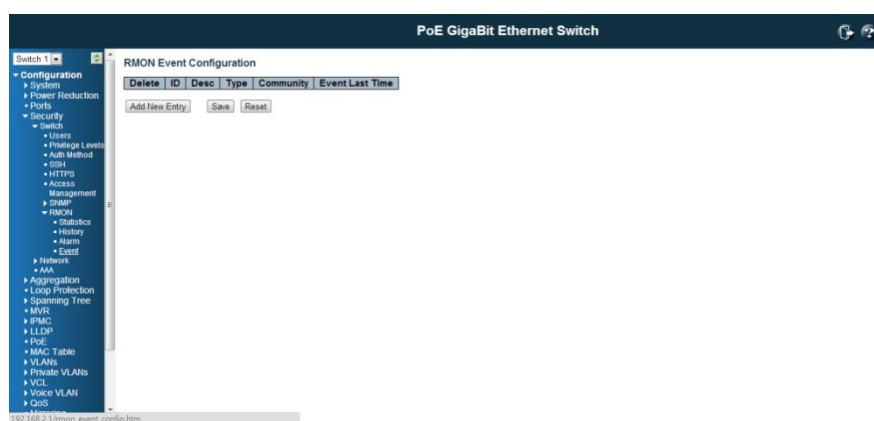
**Add new entry:** Click to add a new community entry.

**Save:** Click to save changes.

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

## RMON Event Configuration

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



## 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 sysUp Time 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.

## 4.4.2 Security /Network

### 4.4.2.1 Port Security Limit Control Configuration

This page allows you to configure the Port Security Limit Control system and port settings.

PoE GigaBit Ethernet Switch

Port Security Limit Control Configuration

System Configuration (Stack Global)

Mode: Disabled

Aging Enabled: ☒

Aging Period: 3600 seconds

Port Configuration for Switch 1

Port	Mode	Limit	Action	State	Re-open
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
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen
21	Disabled	4	None	Disabled	Reopen
22	Disabled	4	None	Disabled	Reopen
23	Disabled	4	None	Disabled	Reopen
24	Disabled	4	None	Disabled	Reopen
25	Disabled	4	None	Disabled	Reopen
26	Disabled	4	None	Disabled	Reopen

Save Reset

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.

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

## System Configuration

### 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.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
  - Switch
    - Users
    - Privilege Levels
    - Auth Method
    - SSH
    - HTTPS
    - Access
    - Management
      - SNMP
      - RMON
    - Networks
    - Limit Control
    - NAC
    - ACL
    - DHCP
    - IP Source Guard
    - ARP Inspection
    - AAA
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - MVR
  - PMF
  - LLDP
  - PoE
  - MAC Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN

Port Security Limit Control Configuration

System Configuration (Stack Global)

Mode: Disabled

Aging Enabled: ☒

Aging Period: 3600 seconds

Port Configuration for Switch 1

Port	Mode	Limit	Action	State	Re-open
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
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen
21	Disabled	4	None	Disabled	Reopen
22	Disabled	4	None	Disabled	Reopen
23	Disabled	4	None	Disabled	Reopen
24	Disabled	4	None	Disabled	Reopen
25	Disabled	4	None	Disabled	Reopen
26	Disabled	4	None	Disabled	Reopen

Save Reset

### Aging Enabled

If checked, secured MAC addresses are subject to aging as discussed under Aging Period.

### Aging Period

If Aging Period 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.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts

looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

## Port Configuration

The table allows you to configure the Port Configuration parameters, which are:

### Port

The port number to which the configuration below applies.

The screenshot shows the configuration interface for a PoE GigaBit Ethernet Switch. The left sidebar contains a navigation tree with categories like Configuration, System, Power Reduction, Ports, Security, and others. The main panel is titled 'Port Security Limit Control Configuration' and includes a 'System Configuration (Stack Global)' section with 'Mode' set to 'Disabled', 'Aging Enabled' checked, and 'Aging Period' set to 3600 seconds. Below this is a 'Port Configuration for Switch 1' table with 26 rows, each representing a port. Each row has columns for Port, Mode, Limit, Action, State, and Re-open. All ports are currently in a 'Disabled' state.

Port	Mode	Limit	Action	State	Re-open
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
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen
19	Disabled	4	None	Disabled	Reopen
20	Disabled	4	None	Disabled	Reopen
21	Disabled	4	None	Disabled	Reopen
22	Disabled	4	None	Disabled	Reopen
23	Disabled	4	None	Disabled	Reopen
24	Disabled	4	None	Disabled	Reopen
25	Disabled	4	None	Disabled	Reopen
26	Disabled	4	None	Disabled	Reopen

### 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

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

**Save:** Click to save changes.

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

### 4.4.2.2 Security / Network / Network Access Server Configuration

This page allows you to configure the IEEE802.1X and MAC-based authentication system and port settings.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
  - Switch
  - Network
    - Limit Control
    - NAS
    - ACL
    - DHCP
    - IP Source Guard
    - ARP Inspection
    - AAA
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - MVR
  - PMF
  - LLDP
  - PoE
  - MAC Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
  - Mirroring
  - UPnP
  - Stack
  - sFlow
- Monitor
- Diagnostics
- Maintenance

Network Access Server Configuration

System Configuration (Stack Global)

Mode: Disabled

Reauthentication Enabled: ☐

Reauthentication Period: 3600 seconds

EAPOL Timeout: 30 seconds

Aging Period: 300 seconds

Hold Time: 10 seconds

RADIUS-Assigned QoS Enabled: ☐

RADIUS-Assigned VLAN Enabled: ☐

Guest VLAN Enabled: ☐

Guest VLAN ID: 1

Max. Reauth. Count: 2

Allow Guest VLAN if EAPOL Seen: ☐

Port Configuration for Switch 1

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
11	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
12	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
13	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
14	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
15	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
16	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
17	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
18	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
19	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
20	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
21	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
22	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
23	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
24	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
25	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
26	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize

Save Reset

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

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

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

## System Configuration

### Mode

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

### Enabled

If checked, successfully authenticated supplicants/clients are re-authenticated after the interval specified by the Re-authentication Period. Re-authentication 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, re-authentication 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).

### **Re-authentication Period**

Determines the period, in seconds, after which a connected client must be re-authenticated. This is only active if the Re-authentication 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 re-authentication 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 re-authentication, which will fail. But if re-authentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, re-authentication 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**

Port VLAN ID is the value for a single port, 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 Configuration**

The table has number of columns which allows you to configure the port mode based on IEEE 802.1X standard. Select the port and configure the settings.



PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
  - Switch
  - Network
    - Limit Control
    - NAS
    - ACL
    - DHCP
    - IP Source Guard
    - ARP Inspection
  - AAA
- Aggregation
- Loop Protection
- Spanning Tree
- MVR
- PMF
- LLDP
- PoE
- MAC Table
- VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
  - Mirroring
  - UPnP
  - Stack
  - sFlow
- Monitor
- Diagnostics
- Maintenance

Network Access Server Configuration

System Configuration (Stack Global)

Mode: Disabled

Reauthentication Enabled: ☐

Reauthentication Period: 3600 seconds

EAPOL Timeout: 30 seconds

Aging Period: 300 seconds

Hold Time: 10 seconds

RADIUS-Assigned QoS Enabled: ☐

RADIUS-Assigned VLAN Enabled: ☐

Guest VLAN Enabled: ☐

Guest VLAN ID: 1

Max. Reauth. Count: 2

Allow Guest VLAN if EAPOL Seen: ☐

Port Configuration for Switch 1

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
11	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
12	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
13	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
14	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
15	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
16	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
17	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
18	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
19	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
20	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
21	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
22	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
23	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
24	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
25	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
26	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize

Save Reset

## 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:

### Force Authorized

In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

### Force Unauthorized

In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

## Port-based 802.1X

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames.

EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-CHALLENGE, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed

for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

**Note:** Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

### **Single 802.1X**

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

### **Multi 802.1X**

Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

### **MAC-based Auth.**

Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following



form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port-Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

### **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.

- Port-based 802.1X
- Single 802.1X0`

#### **RADIUS attributes used in identifying a QoS Class:**

The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].

### **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.

- Port-based 802.1X
- Single 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

#### **RADIUS attributes used in identifying a VLAN ID:**

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
  - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
  - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
  - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

### 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-based 802.1X
- Single 802.1X
- Multi 802.1X

For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

#### **Guest VLAN Operation:**

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max., Reauth., Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If

Allow guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

### 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 re-initialization 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

**Refresh:** Click to refresh the page.

**Save:** Click to save changes.

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

### 4.4.2.3 Security / Network / Access Control List Configuration

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.

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	2362
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
13	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
14	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
15	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
16	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
17	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
18	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
19	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
20	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
21	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
22	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
23	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
24	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
25	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
26	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0

The settings relate to the currently selected stack unit, as reflected by the page header.

## 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.

PoE GigaBit Ethernet Switch

Switch 1

ACL Ports Configuration for Switch 1

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	2362
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
13	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
14	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
15	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
16	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
17	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
18	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
19	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
20	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
21	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
22	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
23	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
24	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
25	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
26	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0

Save Reset

## 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 Copy

Select which port frames are copied on. The allowed values are **Disabled** or a specific port number. 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".

## 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. Any changes made locally will be undone..

**Clear:** Click to clear the counter

## ACL Rate Limiters Configuration

Configure the rate limiter for the ACL of the switch

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
  - Switch
    - Network
      - Limit Control
      - NAS
      - ACL
        - Ports
        - Rate Limiters
        - Access Control List
      - DHCP
      - IP Source Guard
      - ARP Inspection
    - AAA
    - Aggregation
    - Loop Protection
    - Spanning Tree
    - MVR
    - PMAC
    - LLDP
    - PoE
    - MAC Table
    - VLANs
    - Private VLANs
    - VCL
    - Voice VLAN
    - QoS
    - Mirroring
    - UPnP
    - Stack
    - sFlow
  - Monitor
  - Diagnostics
  - Maintenance

ACL Rate Limiter Configuration

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

Save Reset

## 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.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
  - Switch
    - Network
      - Limit Control
      - NAS
      - ACL
        - Ports
        - Rate Limiters
        - Access Control List
      - DHCP
      - IP Source Guard
      - ARP Inspection
    - AAA
    - Aggregation
    - Loop Protection
    - Spanning Tree
    - MVR
    - PMAC
    - LLDP
    - PoE
    - MAC Table
    - VLANs
    - Private VLANs
    - VCL
    - Voice VLAN
    - QoS
    - Mirroring
    - UPnP
    - Stack
    - sFlow
  - Monitor
  - Diagnostics
  - Maintenance

ACL Rate Limiter Configuration

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

Save Reset

## Unit

**Specify** the rate unit. The allowed values are:

**pps:** packets per second.

**kbps:** Kbits per second.

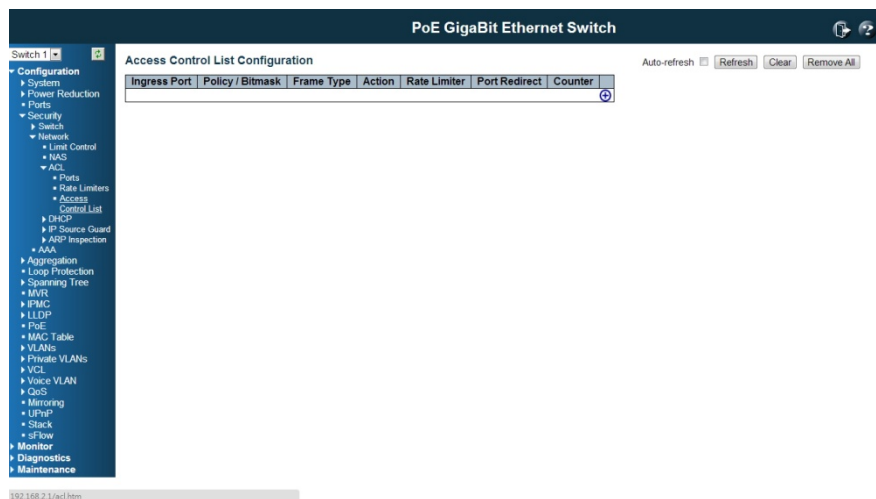
## Buttons

**Save:** Click to save changes.

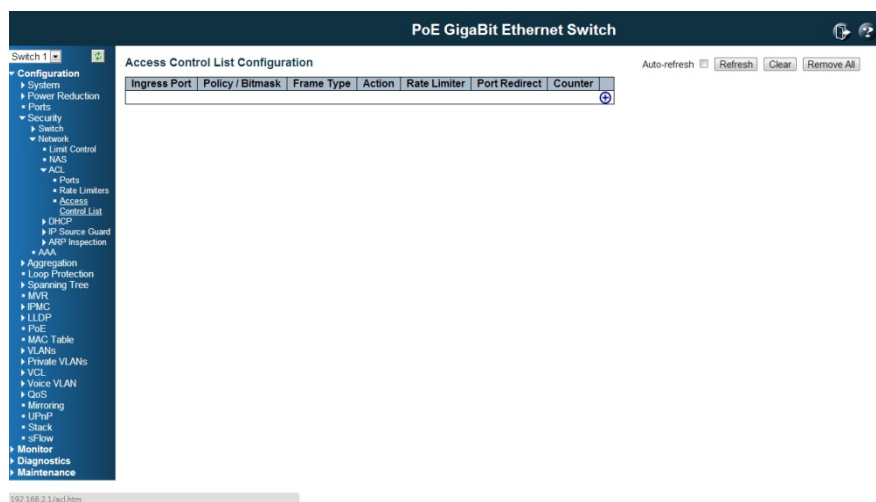
**Reset:** Click to undo any changes made locally and revert to previously saved values.

## Access Control List Configuration

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.



Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.



## 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.

## 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 Copy

Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are **Disabled** or a specific port number. When **Disabled** is displayed, the port copy 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 at regular intervals.

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

**Clear:** Click to clear the counter

**Remove All:** Click to remove all ACEs

## ACE Configuration

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.

The screenshot shows the 'GigaBit Ethernet Switch' configuration interface. On the left is a sidebar with a tree view containing categories like Configuration, System, Power Reduction, Ports, Security, Network, and AAA. The main area is titled 'ACE Configuration'. It has four tabs: 'Ingress Port', 'Policy Filter', 'Switch', and 'Frame Type'. The 'Ingress Port' tab is active, showing a dropdown menu with 'All' selected. Below the tabs are 'MAC Parameters' with a 'DMAC Filter' dropdown set to 'Any'. At the bottom are 'Save', 'Reset', and 'Cancel' buttons. To the right of the tabs is a list of actions: 'Action' (Permit), 'Rate Limiter' (Disabled), 'Port Redirect' (Disabled), 'Logging' (1), 'Shutdown' (2), 'Counter' (3), 'VLAN Parameters' (4-16), and 'Tag Priority' (17-18). Each action has a corresponding number in a column to its right.

## Ingress Port

Select the ingress port for which this ACE applies.

**All:** The ACE applies to all port.

**Port  $n$ :** The ACE applies to this port number, where  $n$  is the number of the switch port. You can select one port or select multiple ports for the entry.

## Policy Filter

Specify the policy number filter for this ACE. The policy ID should be the same when you want apply it to the ACL or Port.



**Any:** No policy filter is specified. (policy filter status is "don't-care".)

**Specific:** If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.

## Policy Value

When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is **0** to **255**.

## Policy Bitmask

When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is **0x0** to **0xff**.

Select the switch to which this ACE applies. [This parameter is reserved to the Stacking model. If the switch doesn't support stacking, the parameter will not display here.](#)

**Any:** The ACE applies to any port.

**Switch n:** The ACE applies to this switch number, where n is the number of the switch.

## Frame Type

Select the frame type for this ACE. These frame types are mutually exclusive.

**Any:** Any frame can match this ACE.

**Ethernet Type:** Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).

**ARP:** Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.

**IPv4:** Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.

**IPv6:** Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with ethernet type.

## Action

Specify the action to take with a frame that hits this ACE.

**Permit:** The frame that hits this ACE is granted permission for the ACE operation.

**Deny:** The frame that hits this ACE is dropped.

The screenshot displays the configuration interface for a GigaBit Ethernet Switch. The left sidebar shows a navigation tree with 'Switch 2' selected under 'Configuration'. The main area is titled 'ACE Configuration'. It contains several sections: 'Ingress Port' with a dropdown set to 'All'; 'Policy Filter' with a dropdown set to 'Any'; 'Switch' with a dropdown set to 'Any'; and 'Frame Type' with a dropdown set to 'Any'. Below these is the 'MAC Parameters' section with a 'DMAC Filter' dropdown set to 'Any'. To the right, there are two columns of options: 'Action' (Permit, Deny) and 'Rate Limiter' (Disabled, 1-16). The 'Rate Limiter' dropdown is currently set to 'Disabled'. Below these are 'VLAN Parameters' including 'VLAN ID Filter' and 'Tag Priority'. At the bottom are 'Save', 'Reset', and 'Cancel' buttons.

## Rate Limiter

Specify the rate limiter in number of base units. The allowed range is **1** to **16**. **Disabled** indicates that the rate limiter operation is disabled.

## Port Copy

Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. **Disabled** indicates that the port copy 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".

## Logging

Specify the logging operation of the ACE. The allowed values are:

**Enabled:** Frames matching the ACE are stored in the System Log.

**Disabled:** Frames matching the ACE are not logged.

Please note that the System Log memory size and logging rate is limited.

## Shutdown

Specify the port shut down operation of the ACE. The allowed values are:

**Enabled:** If a frame matches the ACE, the ingress port will be disabled.

**Disabled:** Port shut down is disabled for the ACE.

## Counter

The counter indicates the number of times the ACE was hit by a frame.

## MAC Parameters

### SMAC Filter

*(Only displayed when the frame type is Ethernet Type or ARP.)*

Specify the source MAC filter for this ACE.

**Any:** No SMAC filter is specified. (SMAC filter status is "don't-care".)

**Specific:** If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

### SMAC Value

When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.

### DMAC Filter

Specify the destination MAC filter for this ACE.

**Any:** No DMAC filter is specified. (DMAC filter status is "don't-care".)

**MC:** Frame must be multicast.

**BC:** Frame must be broadcast.

**UC:** Frame must be unicast.

**Specific:** If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

## DMAC Value

When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.

## VLAN Parameters

### 802.1Q Tagged

Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:

**Any:** Any value is allowed ("don't-care").

**Enabled:** Tagged frame only.

**Disabled:** Untagged frame only.

The default value is "Any".

### VLAN ID Filter

Specify the VLAN ID filter for this ACE.

**Any:** No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)

**Specific:** If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.

### VLAN ID

When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is **1** to **4095**. A frame that hits this ACE matches this VLAN ID value.

### Tag Priority

Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is **0** to **7**. The value **Any** means that no tag priority is specified (tag priority is "don't-care".)

## ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

### ARP/RARP

Specify the available ARP/RARP opcode (OP) flag for this ACE.

**Any:** No ARP/RARP OP flag is specified. (OP is "don't-care".)

**ARP:** Frame must have ARP/RARP opcode set to ARP.

**RARP:** Frame must have ARP/RARP opcode set to RARP.

**Other:** Frame has unknown ARP/RARP Opcode flag.

### Request/Reply

Specify the available ARP/RARP opcode (OP) flag for this ACE.

**Any:** No ARP/RARP OP flag is specified. (OP is "don't-care".)

**Request:** Frame must have ARP Request or RARP Request OP flag set.

**Reply:** Frame must have ARP Reply or RARP Reply OP flag.

### Sender IP Filter

Specify the sender IP filter for this ACE.

**Any:** No sender IP filter is specified. (Sender IP filter is "don't-care".)

**Host:** Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.

**Network:** Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

### Sender IP Address

When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.

### Sender IP Mask

When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

### Target IP Filter

Specify the target IP filter for this specific ACE.

**Any:** No target IP filter is specified. (Target IP filter is "don't-care".)

**Host:** Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.

**Network:** Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

### Target IP Address

When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.

### Target IP Mask

When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

### ARP SMAC Match

Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

**0:** ARP frames where SHA is not equal to the SMAC address.

**1:** ARP frames where SHA is equal to the SMAC address.

**Any:** Any value is allowed ("don't-care").

### RARP DMAC Match

Specify whether frames can hit the action according to their target hardware address field (THA) settings.

**0:** RARP frames where THA is not equal to the DMAC address.

**1:** RARP frames where THA is equal to the DMAC address.

**Any:** Any value is allowed ("don't-care").

### IP/Ethernet Length

Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

**0:** ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).

**1:** ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to

IPv4 (0x04).

**Any:** Any value is allowed ("don't-care").

## IP

Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

**0:** ARP/RARP frames where the HLD is not equal to Ethernet (1).

**1:** ARP/RARP frames where the HLD is equal to Ethernet (1).

**Any:** Any value is allowed ("don't-care").

## Ethernet

Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

**0:** ARP/RARP frames where the PRO is not equal to IP (0x800).

**1:** ARP/RARP frames where the PRO is equal to IP (0x800).

**Any:** Any value is allowed ("don't-care").

## IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

## IP Protocol Filter

Specify the IP protocol filter for this ACE.

**Any:** No IP protocol filter is specified ("don't-care").

**Specific:** If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.

**ICMP:** Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.

**UDP:** Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.

**TCP:** Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

## IP Protocol Value

When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is **0** to **255**. A frame that hits this ACE matches this IP protocol value.

## IP TTL

Specify the Time-to-Live settings for this ACE.

**zero:** IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

**non-zero:** IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

**Any:** Any value is allowed ("don't-care").

## IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

**No:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

**Yes:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

**Any:** Any value is allowed ("don't-care").

## IP Option

Specify the options flag setting for this ACE.

**No:** IPv4 frames where the options flag is set must not be able to match this entry.

**Yes:** IPv4 frames where the options flag is set must be able to match this entry.

**Any:** Any value is allowed ("don't-care").

## SIP Filter

Specify the source IP filter for this ACE.

**Any:** No source IP filter is specified. (Source IP filter is "don't-care".)

**Host:** Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

**Network:** Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

## SIP Address

When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

## SIP Mask

When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.

## DIP Filter

Specify the destination IP filter for this ACE.

**Any:** No destination IP filter is specified. (Destination IP filter is "don't-care".)

**Host:** Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.

**Network:** Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

## DIP Address

When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.

## DIP Mask

When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

## ICMP Parameters

### ICMP Type Filter

Specify the ICMP filter for this ACE.

**Any:** No ICMP filter is specified (ICMP filter status is "don't-care").

**Specific:** If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

### ICMP Type Value

When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is **0** to **255**. A frame that hits this ACE matches this ICMP value.

### ICMP Code Filter

Specify the ICMP code filter for this ACE.

**Any:** No ICMP code filter is specified (ICMP code filter status is "don't-care").

**Specific:** If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

### ICMP Code Value

When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is **0** to **255**. A frame that hits this ACE matches this ICMP code value.

## TCP/UDP Parameters

### TCP/UDP Source Filter

Specify the TCP/UDP source filter for this ACE.

**Any:** No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").

**Specific:** If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.

**Range:** If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

### TCP/UDP Source No.

When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP source value.

### TCP/UDP Source Range

When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP source value.

### TCP/UDP Destination Filter

Specify the TCP/UDP destination filter for this ACE.

**Any:** No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").

**Specific:** If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.

**Range:** If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

### TCP/UDP Destination Number

When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.

### TCP/UDP Destination Range

When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.

#### TCP FIN

Specify the TCP "No more data from sender" (FIN) value for this ACE.

**0:** TCP frames where the FIN field is set must not be able to match this entry.

**1:** TCP frames where the FIN field is set must be able to match this entry.

**Any:** Any value is allowed ("don't-care").

#### TCP SYN

Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

**0:** TCP frames where the SYN field is set must not be able to match this entry.

**1:** TCP frames where the SYN field is set must be able to match this entry.

**Any:** Any value is allowed ("don't-care").

#### TCP RST

Specify the TCP "Reset the connection" (RST) value for this ACE.

**0:** TCP frames where the RST field is set must not be able to match this entry.

**1:** TCP frames where the RST field is set must be able to match this entry.

**Any:** Any value is allowed ("don't-care").

#### TCP PSH

Specify the TCP "Push Function" (PSH) value for this ACE.

**0:** TCP frames where the PSH field is set must not be able to match this entry.

**1:** TCP frames where the PSH field is set must be able to match this entry.

**Any:** Any value is allowed ("don't-care").

#### TCP ACK

Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

**0:** TCP frames where the ACK field is set must not be able to match this entry.

**1:** TCP frames where the ACK field is set must be able to match this entry.

**Any:** Any value is allowed ("don't-care").

#### TCP URG

Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

**0:** TCP frames where the URG field is set must not be able to match this entry.

**1:** TCP frames where the URG field is set must be able to match this entry.

**Any:** Any value is allowed ("don't-care").

### Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

#### EtherType Filter

Specify the Ethernet type filter for this ACE.

**Any:** No EtherType filter is specified (EtherType filter status is "don't-care").

**Specific:** If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

#### Ethernet Type Value



When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is **0x600** to **0xFFFF** but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

### Buttons

**Save:** Click to save changes.

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

**Cancel:** Return to the previous page.

The screenshot shows the 'GigaBit Ethernet Switch' configuration page. The left sidebar contains a navigation tree with categories like Configuration, System, Power Reduction, Ports, Security, and Network. The main area is titled 'ACE Configuration' and includes sections for 'Ingress Port', 'Policy Filter', 'Switch', 'Frame Type', 'MAC Parameters', and 'VLAN Parameters'. The 'Ingress Port' section has dropdowns for 'Ingress Port', 'Policy Filter', 'Switch', and 'Frame Type'. The 'MAC Parameters' section has a 'DMAC Filter' dropdown. The 'VLAN Parameters' section has 'VLAN ID Filter' and 'Tag Priority' dropdowns. The right sidebar shows a list of actions: 'Action' (Permit), 'Rate Limiter' (Disabled), 'Port Redirect' (Disabled), 'Logging' (1-16), 'Shutdown' (1-16), and 'Counter' (1-16). At the bottom of the main area are 'Save', 'Reset', and 'Cancel' buttons.

## 4.4.2.4 Switch / Network / DHCP Configuration

### DHCP Snooping Configuration

Configure DHCP Snooping on this page.

#### 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

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.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
  - Switch
  - Network
    - Limit Control
    - NAS
    - ACL
    - DHCP
      - Snooping
      - Relay
    - IP Source Guard
    - ARP Inspection
    - AAA
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - MVR
  - IPMC
  - LLDP
  - PoE
  - MAC Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
  - Mirroring
  - UPnP
  - Stack
  - sFlow
- Monitor
- Diagnostics
- Maintenance

DHCP Snooping Configuration

Stack Global Settings

Snooping Mode Disabled

Port Mode Configuration for Switch 1

Port	Mode
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted
9	Trusted
10	Trusted
11	Trusted
12	Trusted
13	Trusted
14	Trusted
15	Trusted
16	Trusted
17	Trusted
18	Trusted
19	Trusted
20	Trusted
21	Trusted
22	Trusted
23	Trusted
24	Trusted
25	Trusted
26	Trusted

Save Reset

## Buttons

**Save:** Click to save changes.

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

## DHCP Relay Configuration

Configure DHCP Relay on this page.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
  - Switch
  - Network
    - Limit Control
    - NAS
    - ACL
    - DHCP
      - Snooping
      - Relay
    - IP Source Guard
    - ARP Inspection
    - AAA
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - MVR
  - IPMC
  - LLDP
  - PoE
  - MAC Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
  - Mirroring
  - UPnP
  - Stack
  - sFlow
- Monitor
- Diagnostics
- Maintenance

DHCP Relay Configuration

Relay Mode Disabled

Relay Server 0.0.0.0

Relay Information Mode Enabled

Relay Information Policy Replace

Save Reset

## 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.

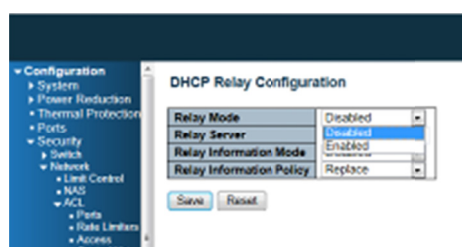
## Relay Server

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 agent receives a DHCP message that already contains relay agent information it will enforce the policy. And it only works under DHCP if relay information operation mode is enabled. 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.

### 4.4.2.5 IP Source Guard Configuration

## IP Source Guard Configuration

This page provides IP Source Guard related configuration.

Port	Mode	Max Dynamic Clients
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited
13	Disabled	Unlimited
14	Disabled	Unlimited
15	Disabled	Unlimited
16	Disabled	Unlimited
17	Disabled	Unlimited
18	Disabled	Unlimited
19	Disabled	Unlimited
20	Disabled	Unlimited
21	Disabled	Unlimited
22	Disabled	Unlimited
23	Disabled	Unlimited
24	Disabled	Unlimited
25	Disabled	Unlimited
26	Disabled	Unlimited

## 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.

## Static IP Source Guard Table

### 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.

### Adding new entry

Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click "Save".

## Buttons

**Save:** Click to save changes.

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

PoE GigaBit Ethernet Switch

Switch 1

- Configuration
  - System
  - Power Reduction
  - Ports
  - Security
    - Switch
    - Network
      - Limit Control
      - NAS
      - ACL
      - DHCP
      - IP Source Guard
        - Configuration
          - Static Table
          - ARP Inspection
        - AAA
        - Aggregation
        - Loop Protection
        - Spanning Tree
        - MVR
        - IPMC
        - LLDP
        - PoE
        - MAC Table
        - VLANs
          - Private VLANs
          - VCL
          - Voice VLAN
        - QoS
        - Mirroring
        - UPnP
        - Stack
        - sFlow
    - Monitor
    - Diagnostics
    - Maintenance

IP Source Guard Configuration

Stack Global Settings

Mode Disabled

Translate dynamic to static

Port Mode Configuration for Switch 1

Port	Mode	Max Dynamic Clients
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited
13	Disabled	Unlimited
14	Disabled	Unlimited
15	Disabled	Unlimited
16	Disabled	Unlimited
17	Disabled	Unlimited
18	Disabled	Unlimited
19	Disabled	Unlimited
20	Disabled	Unlimited
21	Disabled	Unlimited
22	Disabled	Unlimited
23	Disabled	Unlimited
24	Disabled	Unlimited
25	Disabled	Unlimited
26	Disabled	Unlimited

Save Reset

#### 4.4.2.6 ARP Inspection

### ARP Inspection

This page provides ARP Inspection related configuration.

PoE GigaBit Ethernet Switch

Switch 1

- Configuration
  - System
  - Power Reduction
  - Ports
  - Security
    - Switch
    - Network
      - Limit Control
      - NAS
      - ACL
      - DHCP
      - IP Source Guard
        - Configuration
          - Static Table
          - ARP Inspection
        - AAA
        - Aggregation
        - Loop Protection
        - Spanning Tree
        - MVR
        - IPMC
        - LLDP
        - PoE
        - MAC Table
        - VLANs
          - Private VLANs
          - VCL
          - Voice VLAN
        - QoS
        - Mirroring
        - UPnP
        - Stack
        - sFlow
    - Monitor
    - Diagnostics
    - Maintenance

ARP Inspection Configuration

Stack Global Settings

Mode Disabled

Translate dynamic to static

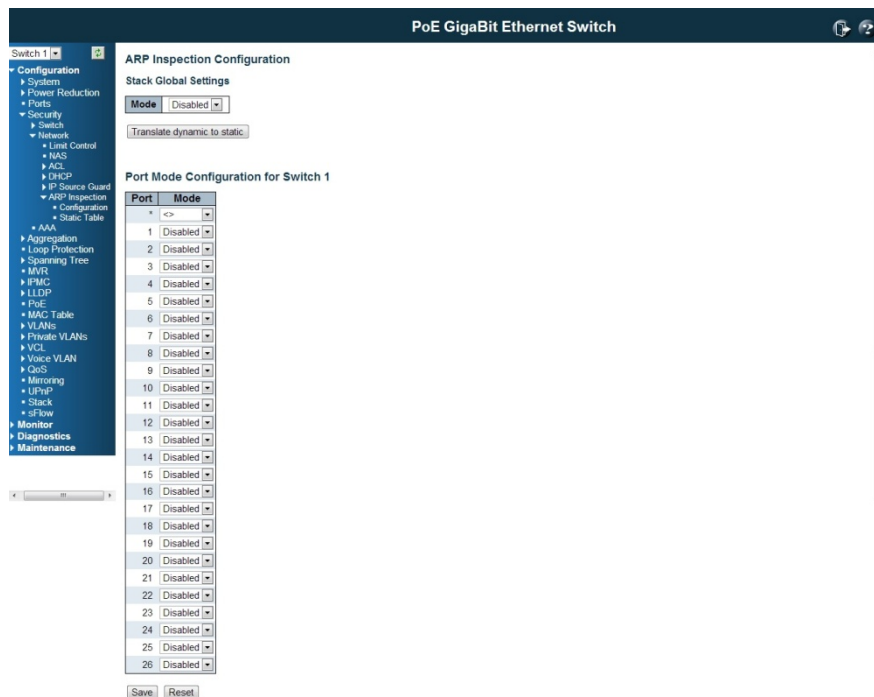
Port Mode Configuration for Switch 1

Port	Mode
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled

Save Reset

## 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.

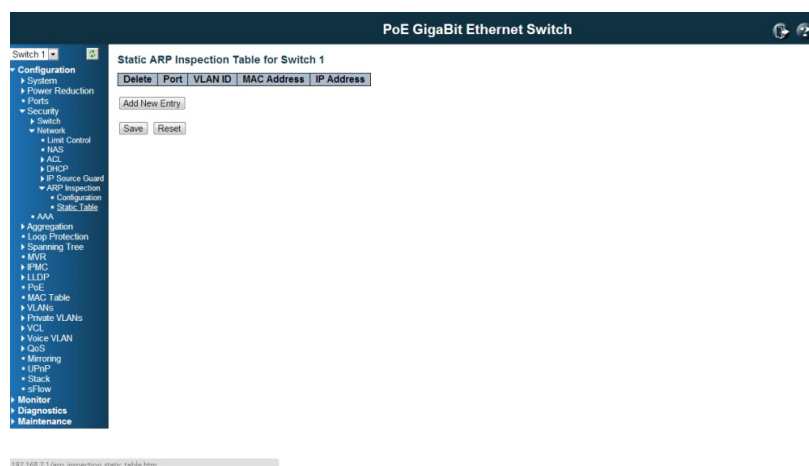
### Buttons

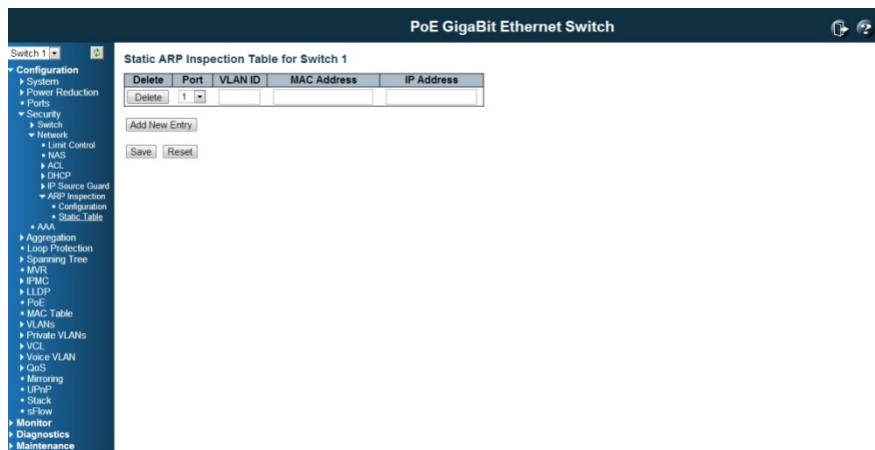
**Save:** Click to save changes.

**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.

## Static ARP Inspection Table





## 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.

## Adding new entry

Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Save".

## Buttons

**Save:** Click to save changes.

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

### 4.4.3 Security / AAA Authentication Server Configuration

This page allows you to configure the Authentication Servers.

#### Common Server Configuration

These setting are common for all of the Authentication Servers.



PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
  - Switch
    - Network
      - Limit Control
      - NAS
      - ACL
      - DHCP
      - IP Source Guard
      - ARP Inspection
      - AAA
        - Authentication
        - Aggregation
        - Loop Protection
        - Spanning Tree
        - MVR
        - IPMC
        - LLDP
        - PAE
          - MAC Table
          - VLANs
          - Private VLANs
          - VCL
          - Voice VLAN
          - QoS
          - Mirroring
          - UPnP
          - Stack
          - Flow
- Monitor
- Diagnostics
- Maintenance

Authentication Server Configuration

Common Server Configuration

Timeout 15 seconds

Dead Time 300 seconds

RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		1812	
2	<input type="checkbox"/>		1812	
3	<input type="checkbox"/>		1812	
4	<input type="checkbox"/>		1812	
5	<input type="checkbox"/>		1812	

RADIUS Accounting Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		1813	
2	<input type="checkbox"/>		1813	
3	<input type="checkbox"/>		1813	
4	<input type="checkbox"/>		1813	
5	<input type="checkbox"/>		1813	

TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		49	
2	<input type="checkbox"/>		49	
3	<input type="checkbox"/>		49	
4	<input type="checkbox"/>		49	
5	<input type="checkbox"/>		49	

Save Reset

## Timeout

The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any).

RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

## Dead Time

The Dead Time, which can be set to a number between 0 and 3600 seconds, 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 Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

## RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

#

The RADIUS Authentication Server number for which the configuration below applies.

### Enabled

Enable the RADIUS Authentication Server by checking this box.

### IP Address/Hostname

The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.

### Port

The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.

### Secret

The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.

## RADIUS Accounting Server Configuration

The table has one row for each RADIUS Accounting Server and a number of columns, which are:

### #

The RADIUS Accounting Server number for which the configuration below applies.

### Enabled

Enable the RADIUS Accounting Server by checking this box.

### IP Address/Hostname

The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.

### Port

The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.

### Secret

The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch.

## TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ Authentication Server and a number of columns, which are:

### #

The TACACS+ Authentication Server number for which the configuration below applies.

### Enabled

Enable the TACACS+ Authentication Server by checking this box.

### **IP Address/Hostname**

The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.

### **Port**

The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.

### **Secret**

The secret - up to 29 characters long - shared between the TACACS+ Authentication Server and the switch.

### **Buttons**

**Save:** Click to save changes.

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

## 4.5 Aggregation Configuration

Link Aggregation is also known as Port Trunking. It allows user using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability. The switch support both Static and Dynamic link aggregation, LACP. The switch also supports different Hash mechanism to forward traffic according to the MAC address or IP, Protocol Port Number.

### 4.5.1 Static Aggregation

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

[illegible]

The aggregation hash mode settings are global, whereas the aggregation group relate to the currently selected stack unit, as reflected by the page header.

## Hash Code Contributors

## 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.

## Aggregation Group Configuration

### 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.

## 4.5.2 LACP - Dynamic Aggregation

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

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
- Aggregation
  - Static
  - LACP
- Loop Protection
- Spanning Tree
- MVR
- PMAC
- LLDP
- PoE
- MAC Table
- VLANs
  - Private VLANs
  - VLAN
  - Voice VLAN
- QoS
- Monitoring
- UPnP
- Stack
- iflow
- Monitor
- Diagnostics
- Maintenance

LACP Port Configuration for Switch 1

Port	LACP Enabled	Key	Role	Timeout	Prio
*	<input type="checkbox"/>	<>	<>	<>	32768
1	<input type="checkbox"/>	Auto	Active	Fast	32768
2	<input type="checkbox"/>	Auto	Active	Fast	32768
3	<input type="checkbox"/>	Auto	Active	Fast	32768
4	<input type="checkbox"/>	Auto	Active	Fast	32768
5	<input type="checkbox"/>	Auto	Active	Fast	32768
6	<input type="checkbox"/>	Auto	Active	Fast	32768
7	<input type="checkbox"/>	Auto	Active	Fast	32768
8	<input type="checkbox"/>	Auto	Active	Fast	32768
9	<input type="checkbox"/>	Auto	Active	Fast	32768
10	<input type="checkbox"/>	Auto	Active	Fast	32768
11	<input type="checkbox"/>	Auto	Active	Fast	32768
12	<input type="checkbox"/>	Auto	Active	Fast	32768
13	<input type="checkbox"/>	Auto	Active	Fast	32768
14	<input type="checkbox"/>	Auto	Active	Fast	32768
15	<input type="checkbox"/>	Auto	Active	Fast	32768
16	<input type="checkbox"/>	Auto	Active	Fast	32768
17	<input type="checkbox"/>	Auto	Active	Fast	32768
18	<input type="checkbox"/>	Auto	Active	Fast	32768
19	<input type="checkbox"/>	Auto	Active	Fast	32768
20	<input type="checkbox"/>	Auto	Active	Fast	32768
21	<input type="checkbox"/>	Auto	Active	Fast	32768
22	<input type="checkbox"/>	Auto	Active	Fast	32768
23	<input type="checkbox"/>	Auto	Active	Fast	32768
24	<input type="checkbox"/>	Auto	Active	Fast	32768
25	<input type="checkbox"/>	Auto	Passive	Slow	0
26	<input type="checkbox"/>	Auto	Passive	Slow	0

Save Reset

192.168.2.1/lacp\_port\_config.htm

## 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. LACP can form max 12 LLAGs per switch and 2 GLAGs per stack.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
- Aggregation
  - Static
  - LACP
- Loop Protection
- Spanning Tree
- MVR
- PMAC
- LLDP
- PoE
  - MAC Table
- VLANs
  - Private VLANs
- VLC
- Voice VLAN
- QoS
- Monitoring
  - UPnP
- Stack
  - sFlow
- Monitor
- Diagnostics
- Maintenance

LACP Port Configuration for Switch 1

Port	LACP Enabled	Key	Role	Timeout	Prio
*	<input type="checkbox"/>	<>	<>	<>	32768
1	<input type="checkbox"/>	Auto	Active	Fast	32768
2	<input type="checkbox"/>	Auto	Active	Fast	32768
3	<input type="checkbox"/>	Auto	Active	Fast	32768
4	<input type="checkbox"/>	Auto	Active	Fast	32768
5	<input type="checkbox"/>	Auto	Active	Fast	32768
6	<input type="checkbox"/>	Auto	Active	Fast	32768
7	<input type="checkbox"/>	Auto	Active	Fast	32768
8	<input type="checkbox"/>	Auto	Active	Fast	32768
9	<input type="checkbox"/>	Auto	Active	Fast	32768
10	<input type="checkbox"/>	Auto	Active	Fast	32768
11	<input type="checkbox"/>	Auto	Active	Fast	32768
12	<input type="checkbox"/>	Auto	Active	Fast	32768
13	<input type="checkbox"/>	Auto	Active	Fast	32768
14	<input type="checkbox"/>	Auto	Active	Fast	32768
15	<input type="checkbox"/>	Auto	Active	Fast	32768
16	<input type="checkbox"/>	Auto	Active	Fast	32768
17	<input type="checkbox"/>	Auto	Active	Fast	32768
18	<input type="checkbox"/>	Auto	Active	Fast	32768
19	<input type="checkbox"/>	Auto	Active	Fast	32768
20	<input type="checkbox"/>	Auto	Active	Fast	32768
21	<input type="checkbox"/>	Auto	Active	Fast	32768
22	<input type="checkbox"/>	Auto	Active	Fast	32768
23	<input type="checkbox"/>	Auto	Active	Fast	32768
24	<input type="checkbox"/>	Auto	Active	Fast	32768
25	<input type="checkbox"/>	Auto	Passive	Slow	0
26	<input type="checkbox"/>	Auto	Passive	Slow	0

(Save) (Reset)

192.168.2.1/lacp\_port\_config.htm

## 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).

## Buttons

**Save:** Click to save changes.

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

## 4.6 Loop Protection

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well. The loop protection feature is very important to protect the unexpected network loop, especially when you install the switch on the internet. The incorrect installation, failure media, or hacker attacking may create network loop.

The switch supports the Loop Protection feature, the port can be shutdown or log information per your configuration when the switch do detect the network loop. After the port is shutdown, it may hard to manually reconnect it, so that there is a shutdown time timeout design can help re-enable the port link automatically. With the Loop Protection feature, it can help you to avoid the failure and protect your network.

### General Settings

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<>	<>
1	<input checked="" type="checkbox"/>	Shutdown Port	Enable
2	<input checked="" type="checkbox"/>	Shutdown Port	Enable
3	<input checked="" type="checkbox"/>	Shutdown Port	Enable
4	<input checked="" type="checkbox"/>	Shutdown Port	Enable

### 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 Configuration

### 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. The valid values are:

**Shutdown Port:** Shutdown the port until the Shutdown Time timeout.

**Shutdown Port and Log:** Shutdown the port and log the status.

**Log Only:** Only log the status.

### 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.



## 4.7 Spanning Tree

The switch supports Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP) and Legacy Spanning Tree Protocol (STP).

The STP and RSTP is combined and defined in IEEE 802.1D-2004, Rapid Spanning Tree Protocol. The RSTP protocol is applied to single network domain no matter how many VLANs in your network. In RSTP domain, one of the switch acts as the Root Switch and block one of the link with highest path cost to avoid network loop. There are maximum 23 level switches within one RSTP domain, the network size may be limited.

Multiple Spanning Tree Protocol (MSTP) is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. With the Spanning Tree and VLAN mapping, each VLAN has its own root and blocking path, the STP region size becomes lower, the convergence time of topology change becomes faster as well.

There are some important abbreviation as below.

**CST (Common Spanning Tree):** Common Spanning Tree (CST) interconnects all adjacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network.

**CIST (Common and Internal Spanning Tree):** MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

**MSTI (Multiple Spanning Tree Instance):** One VLAN can be mapped to a MSTI. Each instance has its own root switch, forwarding path, blocking path and table. An MST Region may contain multiple MSTI.

### 4.7.1 Spanning Tree / Bridge Setting

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

The screenshot shows the configuration interface for a PoE GigaBit Ethernet Switch. The left sidebar contains a navigation menu with categories like Configuration, System, Power Reduction, Ports, Security, Aggregation, Loop Protection, Spanning Tree, Bridge Settings, MSTI Mapping, MSTI Priorities, CST Ports, MSTI Ports, MVR, IPMC, LLDP, FRR, MAC Table, VLANs, Private VLANs, VCL, Voice VLAN, QoS, Mirroring, Uniflow, Stack, SFlow, Monitor, Diagnostics, and Maintenance. The main content area is titled 'STP Bridge Configuration' and is divided into two tabs: 'Basic Settings' and 'Advanced Settings'. The 'Basic Settings' tab is active, showing fields for Protocol Version (MSTP), Bridge Priority (32768), Forward Delay (15), Max Age (20), Maximum Hop Count (20), and Transmit Hold Count (6). The 'Advanced Settings' tab is also visible, showing fields for Edge Port BPDU Filtering, Edge Port BPDU Guard, Port Error Recovery, and Port Error Recovery Timeout. At the bottom of the configuration area are 'Save' and 'Reset' buttons.

STP Bridge Configuration	
<b>Basic Settings</b>	
Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6
<b>Advanced Settings</b>	
Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

Save Reset

192.168.2.1/mstp\_sys\_config.htm

## Basic Settings

### Protocol Version

The 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  $\leq (\text{FwdDelay}-1)*2$ .

### 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.

## Advanced Settings

This section describes the advanced settings of the Spanning Tree Protocol.

### 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.

## 4.7.2 Spanning Tree / MSTI Mapping

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

The screenshot shows the configuration interface for a PoE GigaBit Ethernet Switch. The left sidebar contains a navigation menu with categories like Configuration, System, Power Reduction, Ports, Security, Aggregation, Loop Protection, Spanning Tree, Bridge Settings, MSTI Mapping, MSTI Priorities, CST Ports, and MSTI Ports. The main content area is titled 'MSTI Configuration' and includes a note: 'Add VLANs separated by spaces or comma. Unmapped VLANs are mapped to the CIST. (The default bridge instance)'. Below this, there is a 'Configuration Identification' section with fields for 'Configuration Name' (00-03-ce-22-65-88) and 'Configuration Revision' (0). The 'MSTI Mapping' section features a table with columns 'MSTI' and 'VLANs Mapped'. The table lists MSTI1 through MSTI7, each with a corresponding input field for mapping. At the bottom of the configuration area are 'Save' and 'Reset' buttons. A status bar at the very bottom indicates the URL: 192.168.2.1/mstp\_mst\_map\_config.htm.

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

## Configuration Identification

### 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 Mapping

### 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 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.)

## Buttons

**Save:** Click to save changes.

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

## 4.7.3 Spanning Tree / MSTI Priorities

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

The screenshot shows the 'MSTI Configuration' page for a 'PoE GigaBit Ethernet Switch'. On the left is a navigation menu with categories like Configuration, System, Ports, Security, Aggregation, Loop Protection, Spanning Tree, Bridge Settings, MSTI Mapping, MSTI Priorities, CIST Ports, and MSTI Ports. The 'MSTI Priorities' option is selected. The main area is titled 'MSTI Priority Configuration' and contains a table with two columns: 'MSTI' and 'Priority'. The table lists MSTI instances from CIST to MSTI7, each with a dropdown menu showing the value '32768'. Below the table are 'Save' and 'Reset' buttons. The top of the interface shows 'Switch 1' and a help icon.

MSTI	Priority
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

192.168.2.1/mstp\_mst\_config.htm

## 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*.

PoE GigaBit Ethernet Switch

Switch 1

STP CIST Port Configuration

CIST Aggregated Port Configuration (Stack Global)

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Forced True

CIST Normal Port Configuration for Switch 1

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
*	<input checked="" type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<>
1	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
2	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
3	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
5	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
6	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
7	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
8	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
9	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
10	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
11	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
12	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
13	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
14	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
15	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
16	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
17	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
18	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
19	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
20	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
21	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
22	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
23	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
24	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
25	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto
26	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auto

Save Reset

## Buttons

**Save:** Click to save changes.

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

## 4.7.4 Spanning Tree / 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.

The STP port settings relate to the currently selected stack unit, as reflected by the page header.

## 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 favor 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).

## operEdge (state flag)

Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having *operEdge true*) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

## Admin Edge

Controls whether the *operEdge* flag should start as set or cleared. (The initial *operEdge* state when a port is initialized).

## Auto Edge

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.

#### Point2Point

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

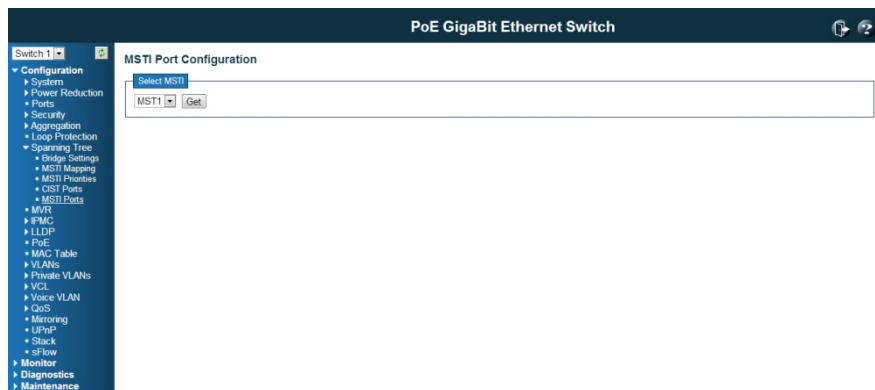
**Save:** Click to save changes.

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

### 4.7.5 Spanning Tree MSTI Ports

#### STP MSTI Port Configuration

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.

Apart from the selected MSTI, the STP MSTI port settings also relate to the currently selected stack unit, as reflected by the page header.

## 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 favor 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.



## 4.8 MVR (Multicast VLAN Registration)

MVR is short of Multicast VLAN Registration. The MVR is a protocol for layer 2 network that enables multicast traffic from a source VLAN to be shared with client/subscriber VLANs. MVR is typically used for IPTV-like service. In non-MVR environment, the IPTV source to different VLAN would be copied multiple copies based on how many client/subscriber VLANs it would deliver.

The IPTV actually delivers the same source with multiple the same content IP streams, the duplicated traffic occupies the bandwidth of the uplink port. Once the traffic is heavy, some unexpected lost or lag appears. However, after MVR enabled, the client/subscriber VLANs are registered to the same source VLAN, then there is only one source stream will be delivered to the registered VLANs.

This page provides MVR related configurations.

**PoE GigaBit Ethernet Switch**

**MVR Configurations**

**Global Setting**

MVR Mode: Disabled

VLAN Interface Setting for Switch 1 (Role [I:Inactive / S:Source / R:Receiver])

Buttons: Delete | MVR VID | MVR Name | Mode | Tagging | Priority | LLQI | Interface Channel Setting

Add New MVR VLAN

**Immediate Leave Setting for Switch 1**

Port	Immediate Leave
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled
27	Disabled
28	Disabled

Buttons: Save | Reset

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header.

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a

channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- MVR
- IPMC
- IGMP Snooping
  - Basic Configuration
  - VLAN Configuration
  - Port Group
  - Filing
  - MLD Snooping
  - LLDP
  - PoE
  - MAG Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
  - Mirroring
  - UPnP
  - Stack
  - sFlow
- Monitor
- Diagnostics
- Maintenance

IGMP Snooping Configuration

Stack Global Settings

Global Configuration

Snooping Enabled ☐

Unregistered IP/MCv4 Flooding Enabled ☒

IGMP SSM Range 232.0.0.0 / 8

Leave Proxy Enabled ☐

Proxy Enabled ☐

Port Related Configuration for Switch 1

Port	Router Port	Fast Leave	Throttling
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
15	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
16	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
17	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
18	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
19	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
20	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
21	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
22	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
23	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
24	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
25	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
26	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Save Reset

## MVR Mode

Enable/Disable the Global MVR.

## VLAN ID

Specify the Multicast VLAN ID.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- MVR
- IPMC
- IGMP Snooping
  - Basic Configuration
  - VLAN Configuration
  - Port Group
  - Filing
  - MLD Snooping
  - LLDP
  - PoE
  - MAG Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
  - Mirroring
  - UPnP
  - Stack
  - sFlow
- Monitor
- Diagnostics
- Maintenance

IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

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

Add New IGMP VLAN

Save Reset

192.168.2.1/pmc/igmp\_vlan.htm

## Mode

Enable MVR on the port.

### Type

Specify the MVR port type on the port.

### Immediate Leave

Enable the fast leave on the port.

### Buttons

**Save:** Click to save changes.

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

## 4.9 IPMC (IP Multicast)

IPMC is short of IP Multicast, the switch support IPv4 and IPv6 multicast forwarding and filtering. The IGMP Snooping defines how to manage IPv4 multicast traffic, the MLD defines how to manage IPv6 multicast traffic.

### 4.9.1 IGMP Snooping Configuration

Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups. By listening to and analyzing IGMP messages, a Layer 2 device running IGMP Snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

#### 4.9.1.1 Basic Configuration

This page provides IGMP Snooping related configuration.

The screenshot displays the IGMP Snooping Configuration interface for a PoE GigaBit Ethernet Switch. The left sidebar shows a navigation tree with 'Switch 1' selected. The main content area is titled 'IGMP Snooping Configuration' and is divided into two sections: 'Stack Global Settings' and 'Port Related Configuration for Switch 1'.

**Stack Global Settings**

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IP/MCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

**Port Related Configuration for Switch 1**

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
15	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
16	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
17	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
18	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
19	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
20	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
21	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
22	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
23	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
24	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
25	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
26	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

At the bottom of the port configuration table, there are 'Save' and 'Reset' buttons.

### Global Configuration

#### Snooping Enabled

Enable the Global IGMP Snooping.

## Unregistered IPMCv4 Flooding enabled

Enable unregistered IPMCv4 traffic flooding. Unregistered IPMCv4 traffic is so-called unknown multicast. After selected, the unregistered multicast stream will be forwarded like normal packets. Once you un-selected it, such stream will be discarded.

## 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.

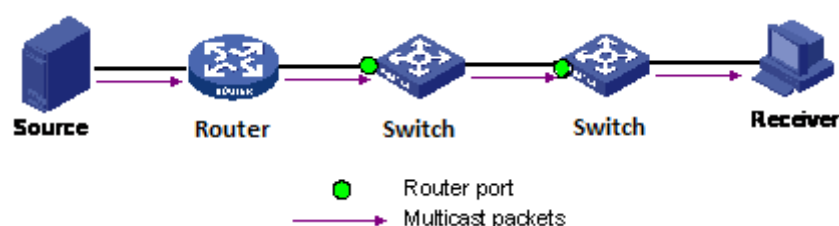
## Proxy Enabled

Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

## Port Related Configuration

### 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. Normally, the router port is the uplink port to the upper L3 Router or IGMP Querier. For example in below figure, the green port of the 2 switches are Router port.



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.

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD

## 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.

### 4.9.1.2 IGMP Snooping VLAN Configuration

#### Navigating the IGMP Snooping VLAN Table

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.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table.

Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.

The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

#### IGMP Snooping VLAN Configuration

Refresh |<< >>|

Start from VLAN  with  entries per page.

VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IGMP-Auto	2	125	100	10	1
10	<input type="checkbox"/>	<input type="checkbox"/>	-	-	-	-	-	-
20	<input type="checkbox"/>	<input type="checkbox"/>	-	-	-	-	-	-

Save Reset

#### IGMP Snooping VLAN Table Columns

##### VLAN ID

The VLAN ID of the entry.

##### IGMP Snooping Enabled

Enable the per-VLAN IGMP Snooping. Only up to 64 VLANs can be selected.

##### IGMP Querier

Enable the IGMP Querier in the VLAN.

##### 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.

##### 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 Max Response Time used to calculate the Max Resp 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 (LMQI for IGMP)

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 VALN Table, i.e. the entry with the lowest VLAN ID.

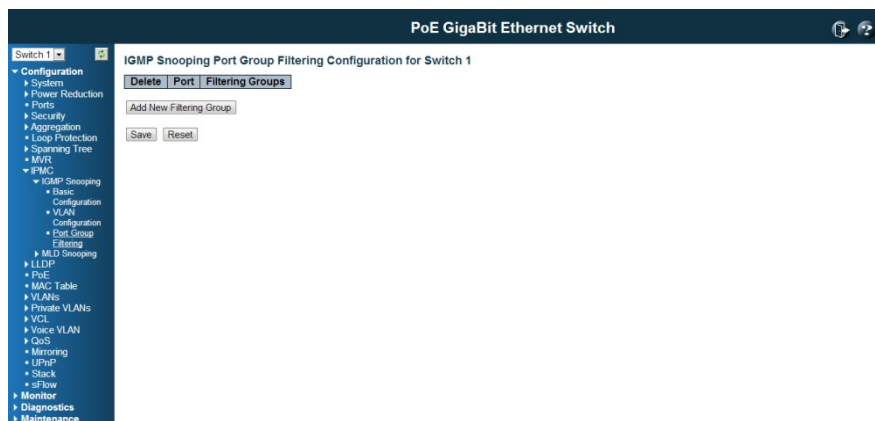
**>>:** Update the table, starting with the entry after the last entry currently displayed.

**Save:** To save the configuration.

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

### 4.9.1.3 IGMP Snooping / Port Group Filtering

#### IGMP Snooping Port Group Filtering Configuration



## Delete

Check to delete the entry. It will be deleted during the next save.

## Port

The logical port for the settings.

## Filtering Groups

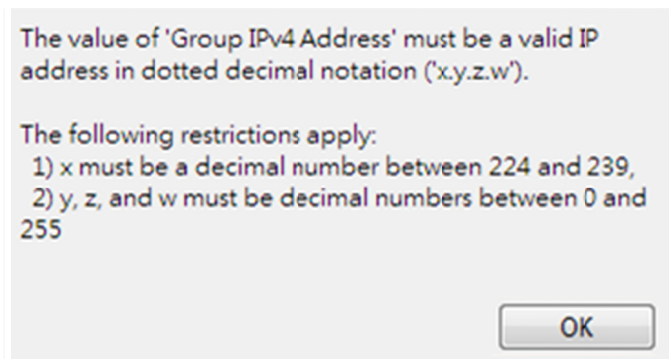
The IP Multicast Group that will be filtered.

## Adding New Filtering Group

Click to add a new entry to the Group Filtering table. Specify the Port, and Filtering Group of the new entry. Click "Save".

Warning message about the Filtering Group.

The range of the IP Multicast is 224.0.0.0 ~239.255.255.255



## Buttons

**Save:** Click to save changes.

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

## 4.9.2 MLD Snooping Configuration

This section provides MLD Snooping related configuration. The MLD is for IPv6 Multicast Snooping. The difference between the 2 IGMP and MLD is that the IGMP is applied to IPv4 Multicast stream, the MLD is applied to IPv6 Multicast stream. While configuring the MLD Snooping configuration, the only thing you need to understand is the IPv6 packet format.

### 4.9.2.1 Basic Configuration

This basic configuration of the MLD, IPv6 Multicast Routing.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header.

## Snooping Enabled

Enable the Global MLD Snooping.

## Unregistered IPMCv6 Flooding enabled

Enable unregistered IPMCv6 traffic flooding. Please note that disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.



## 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

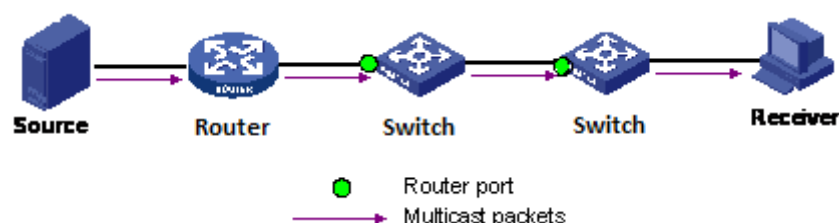
Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

## 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. Normally, the router port is the uplink port to the upper L3 Router or IGMP Querier. For example in below figure, the green port of the 2 switches are Router port.



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.

### 4.9.2.2 MLD Snooping VLAN Configuration

#### Navigating the MLD Snooping VLAN Table

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. The "VLAN" input fields allow the user to select the starting point in the VLAN Table.

Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.

The will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

### MLD Snooping VLAN Table Columns

#### VLAN ID

The VLAN ID of the entry.

#### MLD Snooping Enabled

Enable the per-VLAN MLD Snooping. Only up to 64 VLANs can be selected.

#### MLD Querier

Enable the IGMP Querier in the VLAN.

#### 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**, **ForcedMLDv1**, **Forced MLDv2**, default compatibility value is MLD-Auto.

#### 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 variable denotes 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.

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

### 4.9.2.3 IPMC / MLD Snooping / Port Group Filtering

#### MLD Snooping Port Group Filtering Configuration

##### Delete

Check to delete the entry. It will be deleted during the next save.

##### Port

The logical port for the settings.

##### Filtering Groups

The IP Multicast Group that will be filtered.

##### Adding New Filtering Group

Click to add a new entry to the Group Filtering table. Specify the Port and Filtering Group for the new entry. Click "Save".

#### Buttons

**Save:** Click to save changes.

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

## 4.10 LLDP Parameters

The **Link Layer Discovery Protocol (LLDP)** is a vendor-neutral link layer protocol. LLDP information is sent by devices from each of their interfaces at a fixed interval, in the form of an Ethernet Frame. Each frame contains one **LLDP Data Unit (LLDPDU)**. Each LLDPDU is a sequence of **Type-Length-Value (TLV)** structures. Each LLDP frame starts with the following mandatory TLVs: *Chassis ID*, *Port ID*, and *Time-to-Live*. The mandatory TLVs are followed by any number of optional TLVs. This section allows the user to inspect and configure the current LLDP port settings.

### 4.10.1 LLDP Configuration

**PoE GigaBit Ethernet Switch**

Switch 1

**LLDP Configuration**

**LLDP Parameters**

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

**LLDP Port Configuration for Switch 1**

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<->	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
25	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
26	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Reset

#### 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, signaling 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.

## LLDP Port Configuration

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.

### 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.

### 4.10.2 LLDP Media Configuration

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

PoE GigaBit Ethernet Switch

Switch 1

- Configuration
  - System
  - Power Reduction
  - Ports
  - Security
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - MVR
  - IPMC
  - LLDP
    - LLDP-MED
  - RAC
  - MAC Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
  - Mirroring
  - UPnP
  - Stack
- Monitor
- Diagnostics
- Maintenance

### 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	
		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

## Fast start repeat count

### 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 LLDPDU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour has been detected in order share LLDP-MED information as fast as possible to new neighbours.

Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With **Fast start repeat count** it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

## Coordinates Location

### 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 the 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.

## Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

### 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 (Neighborhood)**

Neighborhood 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

### **House no. 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 (e.g. E911 and others), such as defined by TIA or NENA.

### **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.

PoE GigaBit Ethernet Switch

Switch 1

- Configuration
  - System
  - Power Reduction
  - Ports
  - Security
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - MVR
  - IPMC
  - LLDP
    - LLDP-MED
    - RAC
    - MAC Table
    - VLANs
    - Private VLANs
    - VCL
    - Voice VLAN
    - QoS
    - Mirroring
    - UPnP
    - Stack
- Monitor
- Diagnostics
- Maintenance

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

## Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

**Policies** are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Soft phone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (Conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be

advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

### 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 policies 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 Signaling** (conditional) - for use in network topologies that require a different policy for the voice signaling 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 Signaling** (conditional) - for use in network topologies that require a different policy for the guest voice signaling 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 Signaling** (conditional) - for use in network topologies that require a separate policy for the video signaling 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 behavior 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.

## Adding a 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".

## Port Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

## 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

**Save:** Click to save changes.

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

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- MVR
- IPMC
- LLDP
  - LLDP-MED
- RAC
- MAC Table
- VLANs
- Private VLANs
- VCL
- Voice VLAN
- QoS
- Mirroring
- UPnP
- Stack

Monitor

Diagnostics

Maintenance

PoE GigaBit Ethernet Switch

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count4

Coordinates Location

Latitude0° NorthLongitude0° EastAltitude0MetersMap DatumWGS84

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

## 4.11 sFlow Configuration

Sampled Flow (sFlow) is a traffic monitoring technology mainly used to collect and analyze traffic statistics. The switch supports sFlow feature. The sFlow software agent collects traffic statistics and packet information from the sFlow-enabled interfaces on the switch, encapsulates them into sFlow packets. The sFlow agent then sends the packet to a specified sFlow collector, the IP Address you assigned in the switch UI. The sFlow collector analyzes the sFlow packets and displays the result.

sFlow has the following two sampling mechanisms:

- \* Flow sampling: Packet-based sampling, used to obtain packet content information.
- \* Counter sampling: Time-based sampling, used to obtain port traffic statistics.

**sFlow Configuration**

**Receiver Configuration**

Owner	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

**Port Configuration**

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0

Type the IP address of sFlow collector in the Receiver Configuration. The sFlow agent will send the collected information to it.

This next page displays the configured **sFlow Samplers** on the switch.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- System
- Power Reduction
- Ports
- Security
- Aggregation
- Loop Protection
- Spanning Tree
- MVR
- RMAC
- LLDP
- PoE
- MAC Table
- VLANs
- Private VLANs
- VCL
- Voice VLAN
- QoS
- Mirroring
- UPnP
- Stack
- sFlow

Monitor

Diagnostics

Maintenance

sFlow Configuration

Receiver Configuration

Owner: <none> [Release]

IP Address/Hostname: 0.0.0.0

UDP Port: 6343

Timeout: 0 seconds

Max. Datagram Size: 1400 bytes

Port Configuration for Switch 1

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
2	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
3	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
4	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
5	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
6	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
7	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
8	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
9	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
10	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
11	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
12	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
13	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
14	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
15	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
16	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
17	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
18	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
19	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
20	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
21	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
22	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
23	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
24	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
25	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
26	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0

Save Reset

## sFlow Ports

List of the port numbers on which sFlow is configured.

## sFlow Instance

Configured sFlow instance for the port number.

## Flow Sampling

Packet flow sampling refers to arbitrarily choosing some packets out of a specified number, reading the first "Max Hdr Size" bytes and exporting the sampled datagram for analysis.

The attributes associated with the flow sampling are: sampler type, sampling rate, maximum header size.

## Sampler Type

Configured sampler type on the port and could be any of the types: None, RX, TX, ALL.

Default value is "none".

## Sampling Rate

Configured sampling rate on the ports.

## Max Hdr Size

Configured size of the header of the sampled frame.

## Counter Sampling

Counter sampling performs periodic, time-based sampling or polling of counters




associated with an interface enabled for sFlow.  
Attribute associated with counter sampling is polling interval.

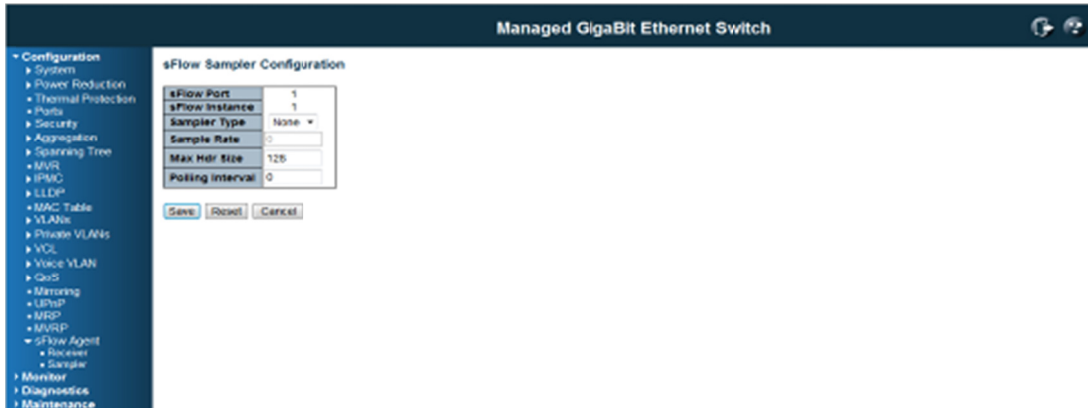
## Polling Interval

Configured polling interval for the counter sampling.

## Editing Button

You can modify each port's sampler configuration the table using the following button:

: Edits the port sampler configuration.



The screenshot shows the configuration interface for a Managed GigaBit Ethernet Switch. On the left is a navigation menu with categories like Configuration, System, and Monitor. The main area displays the 'sFlow Sampler Configuration' dialog box. This dialog contains fields for sFlow Port (set to 1), sFlow Instance (set to 1), Sampler Type (set to None), Sample Rate (set to 0), Max Hdr Size (set to 128), and Polling Interval (set to 0). At the bottom of the dialog are buttons for Save, Reset, and Cancel.

sFlow Sampler Configuration	
sFlow Port	1
sFlow Instance	1
Sampler Type	None
Sample Rate	0
Max Hdr Size	128
Polling Interval	0

Save Reset Cancel

## 4.12 MAC Address Table 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.

PoE GigaBit Ethernet Switch

Switch 1

MAC Address Table Configuration

Stack Aging Configuration

Disable Automatic Aging ☐

Aging Time 300 seconds

MAC Table Learning for Switch 1

	Port Members																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Static MAC Table Configuration for Switch 1

	Port Members																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Delete																										
VLAN ID																										
MAC Address																										

Add New Static Entry

Save Reset

### Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, **Age time** seconds.

The allowed range is **10** to **1000000** seconds.

Disable the automatic aging of dynamic entries by checking ☐ **Disable automatic aging**.

### MAC Table Learning

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

Each port can do learning based upon the following settings:

#### Auto

Learning is done automatically as soon as a frame with unknown SMAC is received.

#### Disable

No learning is done.

#### Secure

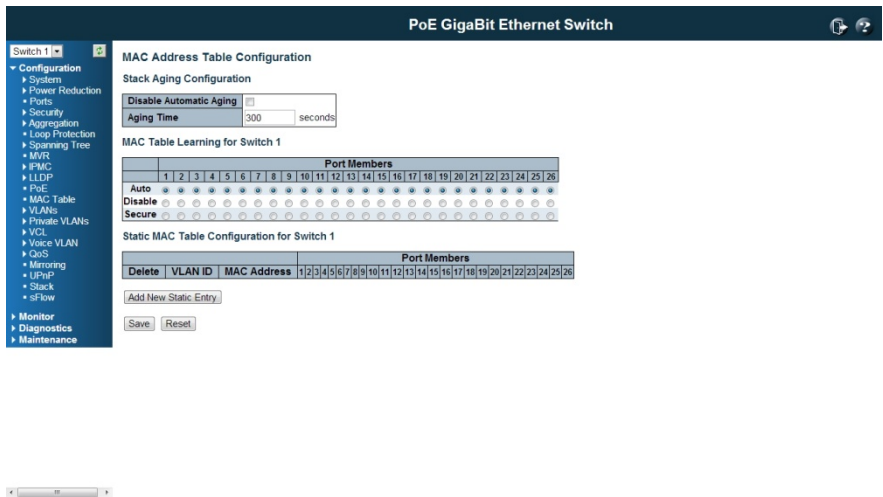
Only static MAC entries are learned, all other frames are dropped.

**Note:** Make sure that the link used for managing the switch is added to the Static Mac

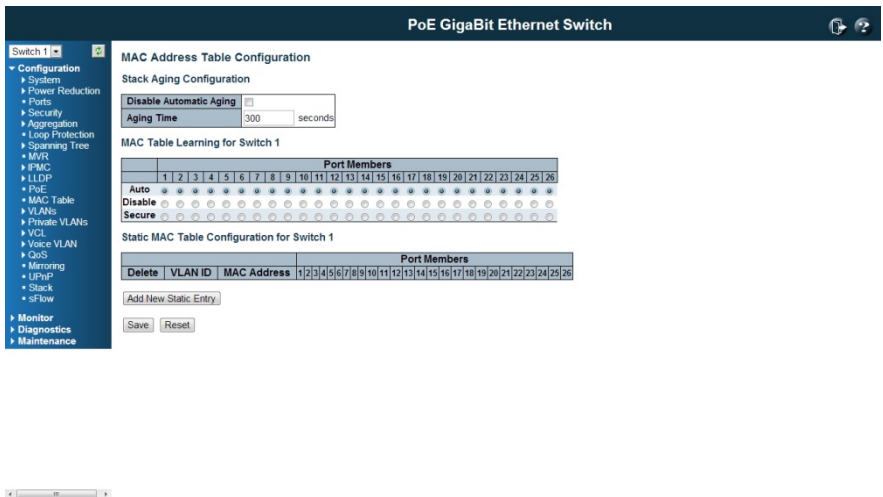
Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

### Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.



The table is sorted first by VLAN ID and then by MAC address.



### Delete

Check to delete the entry. It will be deleted during the next save.

### VLAN ID

The VLAN ID of the entry.

### MAC Address

The MAC address of the entry.

### Port Members

Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

### Adding a 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".

### Buttons

**Save:** Click to save changes.

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

## 4.13 VLAN (Virtual LAN)

The VLAN is short of Virtual LAN (Local Area Network.) The VLAN technology allows you to divide the physical ports to different logical groups. Each group is a virtual LAN, the clients within the VLAN is a broadcast domain. While the clients in different VLANs need to communicate, the VLAN Overlapping setting or an additional upper router is needed.

There are 2 typical types VLAN technology, Port-Based and Tag Based. The Port-based VLAN is the simplest approach to LAN implementation. The idea is to assign the ports on a switch to different VLANs, the settings is only applied to the ports of the switch.

Tag-based VLAN follows IEEE 802.1Q technology to tag VLAN ID to the packets. The tagged VID is not only apply to the switch, but also can be forwarded to next switch and whole network depends on how you configuring the switch settings.

### 4.13.1 VLAN Membership Configuration

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.

PoE GigaBit Ethernet Switch

VLAN Membership Configuration for Switch 1

Start from VLAN 1 with 20 entries per page. Refresh << >>

Delete	VLAN ID	VLAN Name	Port Members
<input type="checkbox"/>	1	default	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Add New VLAN

Save Reset

### Navigating the VLAN Table

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.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

## 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 only contain alphabets or numbers. VLAN name should contain at least one alphabet. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.

## Port Members

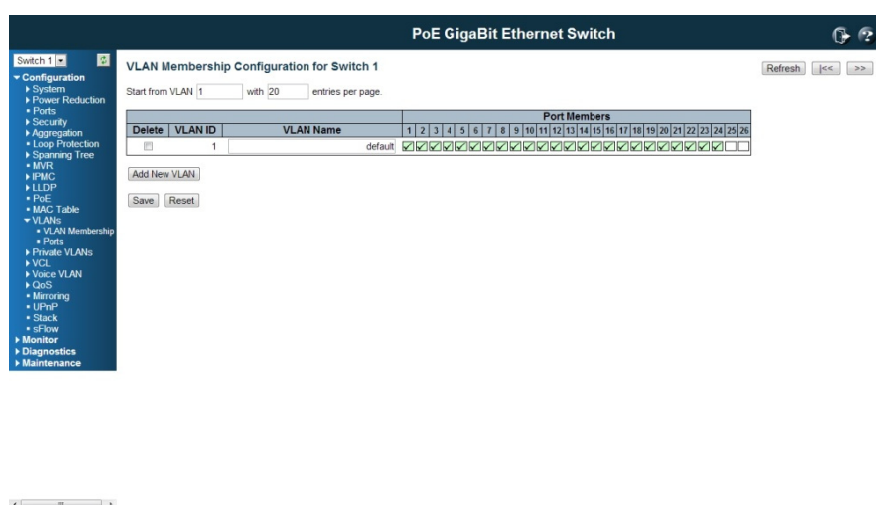
A row of check boxes for each port is displayed for each VLAN ID.

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.



PoE GigaBit Ethernet Switch

Switch 1

VLAN Membership Configuration for Switch 1

Start from VLAN 1 with 20 entries per page

Delete	VLAN ID	VLAN Name	Port Members
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 16 <input checked="" type="checkbox"/> 17 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 19 <input checked="" type="checkbox"/> 20 <input checked="" type="checkbox"/> 21 <input checked="" type="checkbox"/> 22 <input checked="" type="checkbox"/> 23 <input checked="" type="checkbox"/> 24 <input checked="" type="checkbox"/> 25 <input checked="" type="checkbox"/> 26

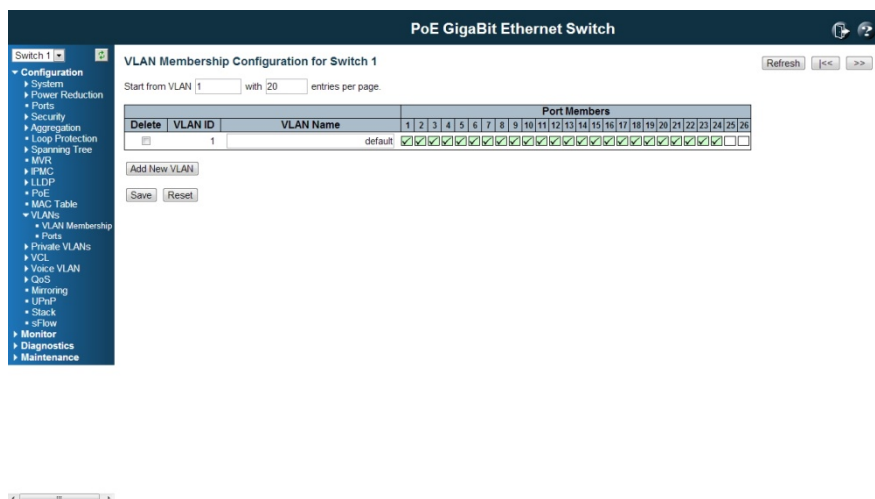
Add New VLAN

Save Reset

## Adding a New VLAN

Click 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". A VLAN without any port members will be deleted when you click "Save".



The button can be used to undo the addition of new VLANs.

## Buttons

**Save:** Click to save changes.

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

**Refresh:** Refreshes the displayed the table starting from the “VLAN ID” input fields.

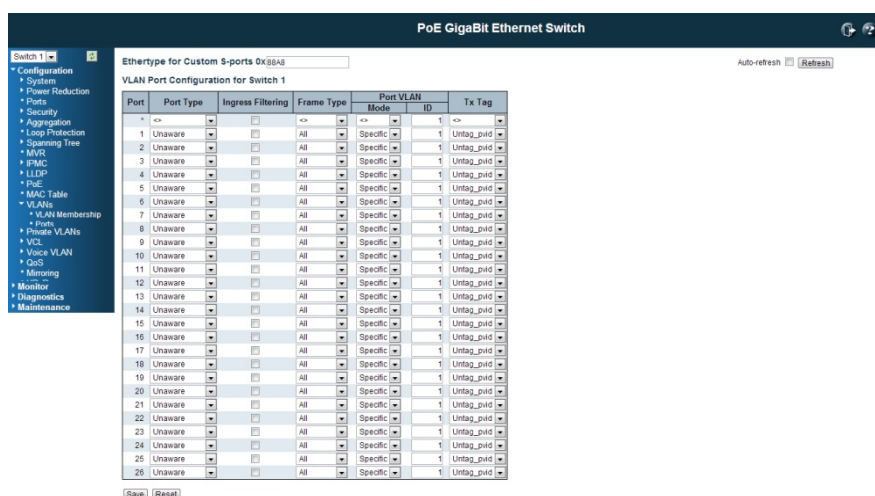
**<<:** Updates the table starting from the first entry in the VALN Table, i.e. the entry with the lowest VLAN ID.

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

### 4.13.2 VLAN Port Configuration

This page is used for configuring the selected stack switch unit port VLAN.

This page is used for configuring the switch port VLAN.



## Ether type 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.

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 **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**

**Save:** Click to save changes.

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

## 4.14 Private VLANs

The Private VLAN feature provides the ability to extend the capabilities of a "standard" VLAN. The additional concepts, Primary VLAN, Community VLAN and Isolated VLAN are introduced in Private VLAN.

The Primary VLAN can be considered the master in the master/slave relationship with the other 2 sub-types, Community VLAN and Isolated VLAN. The switch Ports assigned with the primary VLAN are able to access the ports in the 2 sub-types.

Both the Community VLN and Isolated VLAN can be considered slaves in the master/slave relationship with the primary VLAN. The switch ports assigned to a Community VLAN can see traffic from all other devices in the same Community. The switch ports assigned to an Isolated VLAN can send traffic to the primary VLAN, but CANNOT see traffic from other devices in the same Isolated VLAN.

In this section, the switch allows you to assign Private VLAN Member Configuration and Port Isolation Configuration.

### 4.14.1 Private VLAN Membership Configuration

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.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

PoE GigaBit Ethernet Switch

Switch 1

VLAN Membership Configuration for Switch 1

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	VLAN Name	Port Members
<input type="checkbox"/>	1	default	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Buttons: Add New VLAN, Save, Reset

Private VLANs do not work across the stack.

### 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.

### Adding a New Private VLAN

Click 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 button can be used to undo the addition of new Private VLANs.

### Buttons

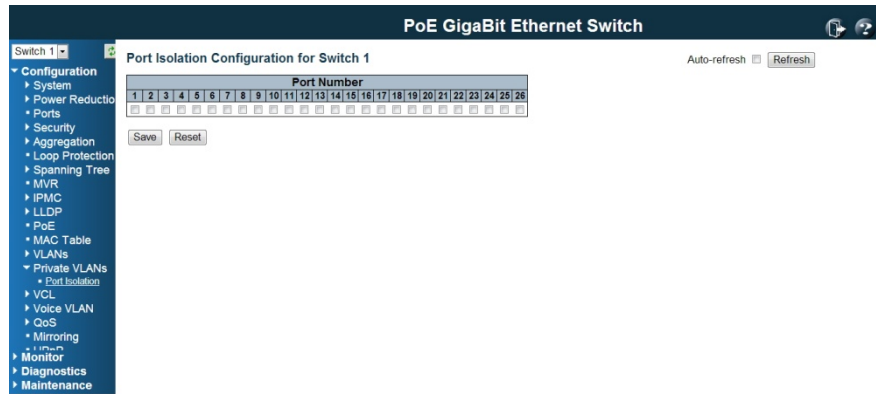
**Save:** Click to save changes.

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

## 4.14.2 Port Isolation Configuration

### Overview

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



192.168.2.1/port\_isolation.htm

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

The port settings relate to the currently selected stack unit, as reflected by the page header.

This feature works across the stack.

## Configuration

### Port Members

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

**Save:** Click to save changes.

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

## 4.15 VCL

### 4.15.1 VCL / MAC-Based VLAN Configuration

The MAC-based VLAN entries 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.

PoE GigaBit Ethernet Switch

MAC-based VLAN Membership Configuration for Switch 1

Auto-refresh ☐ Refresh

Delete	MAC Address	VLAN ID	Port Members
Currently no entries present			

Add New Entry

Save Reset

192.168.2.1/mac\_based\_vlan.htm

#### 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.

#### Adding a New MAC-based VLAN

Click 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 button can be used to undo the addition of new MAC-based VLANs.

## 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.

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

## 4.15.2 VCL / Protocol-based VLAN

### Protocol to Group Mapping Table

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.

The displayed settings are:

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
<input type="checkbox"/>	Ethernet	0888	Eth0888
<input type="checkbox"/>	Ethernet	0800	Eth0800

Buttons: Add New Entry, Save, Reset

Auto-refresh ☐ Refresh

### 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 preceding Frame Type selection menu.

Below is the criteria for three different Frame Types:

**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

**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)

**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.

#### Adding a New Group to VLAN mapping entry

Click 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.

#### Buttons

**Save:** Click to save changes.

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



## VLC / Protocol-based VLAN / Group Name to VLAN mapping Table

The screenshot shows the configuration interface for a PoE GigaBit Ethernet Switch. On the left is a navigation menu with categories like Configuration, System, Power Reduction, Ports, Security, Aggregation, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, PoE, VLANs, Private VLANs, and VCL. The 'VLANs' section is expanded, showing 'Protocol-based VLAN' and 'Group Name to VLAN mapping Table'. The main area displays the 'Group Name to VLAN mapping Table' with a table containing one entry: Group Name 'IP22' and VLAN ID '20'. The table has columns for 'Delete', 'Group Name', 'VLAN ID', and 'Port Members' (ports 1-26). The 'Delete' checkbox is checked. Below the table are buttons for 'Add New Entry', 'Save', and 'Reset'. An 'Auto-refresh' checkbox and a 'Refresh' button are in the top right of the table area.

Delete	Group Name	VLAN ID	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input checked="" type="checkbox"/>	IP22	20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

This page allows you to map an already configured Group Name to a VLAN for the switch. The displayed settings are:

### 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 of at 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.

### Adding a New Group to VLAN mapping entry

Click 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 button can be used to undo the addition of new entry.

## Buttons

**Save:** Click to save changes.

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

### 4.15.3 VCL / IP Subnet-based VLAN

The IP subnet-based VLAN entries 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.

The screenshot shows the configuration interface for a PoE GigaBit Ethernet Switch. The left sidebar contains a navigation tree with categories like Configuration, System, Power Reduction, Ports, Security, Aggregation, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, PoE, MAC Table, VLANs, Private VLANs, and VCL. The main area is titled 'IP Subnet-based VLAN Membership Configuration' and includes an 'Auto-refresh' checkbox and a 'Refresh' button. Below this is a table with columns: Delete, VCE ID, IP Address, Mask Length, VLAN ID, and Port Members. The Port Members column is a grid of checkboxes for ports 1 through 26. A single entry is shown with VCE ID 1, IP Address 192.168.2.100, Mask Length 24, and VLAN ID 1. Below the table are buttons for 'Add New Entry', 'Save', and 'Reset'.

Delete	VCE ID	IP Address	Mask Length	VLAN ID	Port Members																									
<input type="checkbox"/>	1	192.168.2.100	24	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### 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 0-256. 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.

### **Adding a New IP subnet-based VLAN**

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.

### **Buttons**

**Save:** Click to save changes.

**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:** Refreshes the displayed table.

## 4.16 Voice VLAN Configuration

### 4.16.1 Voice VLAN / 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.

The screenshot shows the configuration interface for a PoE GigaBit Ethernet Switch. The left sidebar contains a navigation tree with categories like Configuration, System, Power Reduction, Ports, Security, Aggregation, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, PVE, MAC Table, VLANs, Private VLANs, VCL, Voice VLAN, QoS, Mirroring, L2/L3, Stack, all, Monitor, Diagnostics, and Maintenance. The main area is titled 'Voice VLAN Configuration' and is divided into 'Stack Global Settings' and 'Port Configuration for Switch 1'.

**Stack Global Settings**

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

**Port Configuration for Switch 1**

Port	Mode	Security	Discovery Protocol
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI
11	Disabled	Disabled	OUI
12	Disabled	Disabled	OUI
13	Disabled	Disabled	OUI
14	Disabled	Disabled	OUI
15	Disabled	Disabled	OUI
16	Disabled	Disabled	OUI
17	Disabled	Disabled	OUI
18	Disabled	Disabled	OUI
19	Disabled	Disabled	OUI
20	Disabled	Disabled	OUI
21	Disabled	Disabled	OUI
22	Disabled	Disabled	OUI
23	Disabled	Disabled	OUI
24	Disabled	Disabled	OUI
25	Disabled	Disabled	OUI
26	Disabled	Disabled	OUI

At the bottom of the port configuration table are 'Save' and 'Reset' buttons.

#### 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 1000000 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 modes are:

**Disabled:** 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

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.

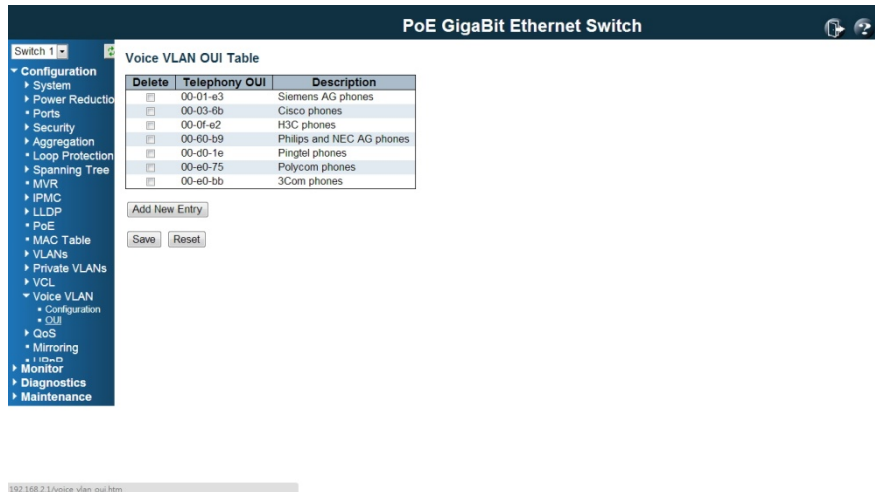
### Buttons

**Save:** Click to save changes.

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

## 4.16.2 Voice VLAN / OUI Configuration

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



## 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.

**Refresh:** Refreshes the displayed the 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

## 4.17 QoS

### 4.17.1 QoS / Ingress Port Classification

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

The settings relate to the currently selected stack unit, as reflected by the page header.

The displayed settings are:

PoE GigaBit Ethernet Switch

Switch 1

QoS Ingress Port Classification for Switch 1

Port	QoS class	DP level	DSCP Based
1	0	0	<input checked="" type="checkbox"/>
2	0	0	<input checked="" type="checkbox"/>
3	0	0	<input checked="" type="checkbox"/>
4	0	0	<input checked="" type="checkbox"/>
5	0	0	<input checked="" type="checkbox"/>
6	0	0	<input checked="" type="checkbox"/>
7	0	0	<input checked="" type="checkbox"/>
8	0	0	<input checked="" type="checkbox"/>
9	0	0	<input checked="" type="checkbox"/>
10	0	0	<input checked="" type="checkbox"/>
11	0	0	<input checked="" type="checkbox"/>
12	0	0	<input checked="" type="checkbox"/>
13	0	0	<input checked="" type="checkbox"/>
14	0	0	<input checked="" type="checkbox"/>
15	0	0	<input checked="" type="checkbox"/>
16	0	0	<input checked="" type="checkbox"/>
17	0	0	<input checked="" type="checkbox"/>
18	0	0	<input checked="" type="checkbox"/>
19	0	0	<input checked="" type="checkbox"/>
20	0	0	<input checked="" type="checkbox"/>
21	0	0	<input checked="" type="checkbox"/>
22	0	0	<input checked="" type="checkbox"/>
23	0	0	<input checked="" type="checkbox"/>
24	0	0	<input checked="" type="checkbox"/>
25	0	0	<input checked="" type="checkbox"/>
26	0	0	<input checked="" type="checkbox"/>

Save Reset

#### Port

The port number for which the configuration below applies.

#### QoS class

Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

#### DP level

Controls the default Drop Precedence Level i.e., the DP level for frames not classified in any other way.

#### PCP

Controls the default PCP for untagged frames.

#### DEI

Controls the default DEI for untagged frames.

#### 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.

## 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.

### 4.17.2 QoS / Ingress Port Policer Config

This page allows you to configure the Policer settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

The displayed settings are:

PoE GigaBit Ethernet Switch

Switch 1

QoS Ingress Port Policers for Switch 1

Port	Enabled	Rate	Unit	Flow Control
1	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
8	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
9	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
10	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
11	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
12	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
13	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
14	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
15	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
16	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
17	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
18	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
19	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
20	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
21	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
22	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
23	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
24	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
25	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>
26	<input type="checkbox"/>	500	Kbps	<input type="checkbox"/>

Save Reset

192.168.2.1/qos\_port\_policers.htm

## 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".









Switch 1

- Configuration
  - System
  - Power Reduction
  - Ports
  - Security
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - MVR
  - IFMC
  - LLDP
  - PAE
  - MAC Table
  - VLANs
  - Private VLANs
  - VOL
  - Voice VLAN
  - QoS
    - Port Classification
    - Port Policing
    - Port Scheduler
    - Port Shaping
    - Port Tag Remark
    - Port DSCP
    - DSCP-based QoS
    - DSCP Translation
    - DSCP Classification
  - Mirroring
  - UPnP
  - Stack
  - Flow
  - Monitor
  - Diagnostics
  - Maintenance

PoE GigaBit Ethernet Switch

QoS Egress Port Tag Remarking for Switch 1

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified
21	Classified
22	Classified
23	Classified
24	Classified
25	Classified

192.168.2.1/qos\_port\_tag\_remarking.htm

## 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.

## QoS / DSCP

### 4.17.6 QoS / Port DSCP Configuration

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

The settings relate to the currently selected stack unit, as reflected by the page header.

The displayed settings are:

PoE GigaBit Ethernet Switch

Switch 1

- Configuration
  - System
  - Power Reduction
  - Ports
  - Security
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - MVR
  - IPMC
  - LLDP
  - PAE
  - MAC Table
  - VLANs
  - Private VLANs
  - VCL
  - Voice VLAN
  - QoS
    - Port Classification
    - Port Policing
    - Port Scheduler
    - Port Shaping
    - Port Tag Remarking
    - Port DSCP
    - DSCP-Based QoS
    - DSCP Translation
    - DSCP Classification
  - Mirroring
  - UPnP
  - Stack
  - sFlow
  - Monitor
  - Diagnostics
  - Maintenance

GoS Port DSCP Configuration for Switch 1

Port	Ingress		Egress
	Translate	Classify	Rewrite
1	<input type="checkbox"/>	Disable	Disable
2	<input type="checkbox"/>	Disable	Disable
3	<input type="checkbox"/>	Disable	Disable
4	<input type="checkbox"/>	Disable	Disable
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable
7	<input type="checkbox"/>	Disable	Disable
8	<input type="checkbox"/>	Disable	Disable
9	<input type="checkbox"/>	Disable	Disable
10	<input type="checkbox"/>	Disable	Disable
11	<input type="checkbox"/>	Disable	Disable
12	<input type="checkbox"/>	Disable	Disable
13	<input type="checkbox"/>	Disable	Disable
14	<input type="checkbox"/>	Disable	Disable
15	<input type="checkbox"/>	Disable	Disable
16	<input type="checkbox"/>	Disable	Disable
17	<input type="checkbox"/>	Disable	Disable
18	<input type="checkbox"/>	Disable	Disable
19	<input type="checkbox"/>	Disable	Disable
20	<input type="checkbox"/>	Disable	Disable
21	<input type="checkbox"/>	Disable	Disable
22	<input type="checkbox"/>	Disable	Disable
23	<input type="checkbox"/>	Disable	Disable
24	<input type="checkbox"/>	Disable	Disable
25	<input type="checkbox"/>	Disable	Disable
26	<input type="checkbox"/>	Disable	Disable

Save Reset

192.168.2.1/qos\_port\_dscp\_config.htm

## Port

The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

## 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

### 1. Translate

To Enable the Ingress Translation click the checkbox.

### 2. Classify

Classification for a port have 4 different values.

**Disabled:** 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 -

**Disabled:** 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.

### 4.17.7 QoS / DSCP based QoS Ingress Classification

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

The displayed settings are:

PoE GigaBit Ethernet Switch

Switch 1

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
0 (BE)	<input type="checkbox"/>	0	0
1	<input type="checkbox"/>	0	0
2	<input type="checkbox"/>	0	0
3	<input type="checkbox"/>	0	0
4	<input type="checkbox"/>	0	0
5	<input type="checkbox"/>	0	0
6	<input type="checkbox"/>	0	0
7	<input type="checkbox"/>	0	0
8 (CS1)	<input type="checkbox"/>	0	0
9	<input type="checkbox"/>	0	0
10 (AF11)	<input type="checkbox"/>	0	0
11	<input type="checkbox"/>	0	0
12 (AF12)	<input type="checkbox"/>	0	0
13	<input type="checkbox"/>	0	0
14 (AF13)	<input type="checkbox"/>	0	0
15	<input type="checkbox"/>	0	0
16 (CS2)	<input type="checkbox"/>	0	0
17	<input type="checkbox"/>	0	0
18 (AF21)	<input type="checkbox"/>	0	0
19	<input type="checkbox"/>	0	0
20 (AF22)	<input type="checkbox"/>	0	0
21	<input type="checkbox"/>	0	0
22 (AF23)	<input type="checkbox"/>	0	0
23	<input type="checkbox"/>	0	0
24 (CS3)	<input type="checkbox"/>	0	0
25	<input type="checkbox"/>	0	0
26 (AF31)	<input type="checkbox"/>	0	0
27	<input type="checkbox"/>	0	0
28 (AF32)	<input type="checkbox"/>	0	0
29	<input type="checkbox"/>	0	0
30 (AF33)	<input type="checkbox"/>	0	0
31	<input type="checkbox"/>	0	0
32 (CS4)	<input type="checkbox"/>	0	0
33	<input type="checkbox"/>	0	0
34 (AF41)	<input type="checkbox"/>	0	0
35	<input type="checkbox"/>	0	0
36 (AF42)	<input type="checkbox"/>	0	0
37	<input type="checkbox"/>	0	0
38 (AF43)	<input type="checkbox"/>	0	0
39	<input type="checkbox"/>	0	0
40 (CS5)	<input type="checkbox"/>	0	0
41	<input type="checkbox"/>	0	0
42	<input type="checkbox"/>	0	0
43	<input type="checkbox"/>	0	0
44	<input type="checkbox"/>	0	0
45	<input type="checkbox"/>	0	0
46 (EF)	<input type="checkbox"/>	0	0
47	<input type="checkbox"/>	0	0
48 (CS6)	<input type="checkbox"/>	0	0
49	<input type="checkbox"/>	0	0
50	<input type="checkbox"/>	0	0
51	<input type="checkbox"/>	0	0
52	<input type="checkbox"/>	0	0
53	<input type="checkbox"/>	0	0
54	<input type="checkbox"/>	0	0
55	<input type="checkbox"/>	0	0
56 (CS7)	<input type="checkbox"/>	0	0
57	<input type="checkbox"/>	0	0
58	<input type="checkbox"/>	0	0
59	<input type="checkbox"/>	0	0
60	<input type="checkbox"/>	0	0
61	<input type="checkbox"/>	0	0
62	<input type="checkbox"/>	0	0
63	<input type="checkbox"/>	0	0

Save Reset

## 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 un-trusted 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.

### 4.17.8 QoS / 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.

The displayed settings are:

PoE GigaBit Ethernet Switch

Switch 1

- Configuration
  - System
  - Power Reduction
  - Ports
  - Security
  - Aggregation
  - Loop Protection
  - Spanning Tree
  - MVR
  - PMPC
  - LLDP
  - PoE
  - MAC Table
  - VLANs
  - Private VLANs
  - VPL
  - Voice VLAN
  - QoS
    - Port Classification
    - Port Policing
    - Port Scheduler
    - Port Shaping
    - Port Tag Remarking
    - Port DSCP
    - DSCP-based QoS
    - DSCP Translation
    - DSCP Classification
  - Mirroring
  - Uplink
  - Stack
  - sFlow
  - Monitor
- Diagnostics
- Maintenance

### DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	
1	<>	<input type="checkbox"/>	<>
0 (BE)	0 (BE)	<input type="checkbox"/>	0 (BE)
1	1	<input type="checkbox"/>	1
2	2	<input type="checkbox"/>	2
3	3	<input type="checkbox"/>	3
4	4	<input type="checkbox"/>	4
5	5	<input type="checkbox"/>	5
6	6	<input type="checkbox"/>	6
7	7	<input type="checkbox"/>	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)
9	9	<input type="checkbox"/>	9
10 (AF11)	10 (AF11)	<input type="checkbox"/>	10 (AF11)
11	11	<input type="checkbox"/>	11
12 (AF12)	12 (AF12)	<input type="checkbox"/>	12 (AF12)
13	13	<input type="checkbox"/>	13
14 (AF13)	14 (AF13)	<input type="checkbox"/>	14 (AF13)
15	15	<input type="checkbox"/>	15
16 (CS2)	16 (CS2)	<input type="checkbox"/>	16 (CS2)
17	17	<input type="checkbox"/>	17
18 (AF21)	18 (AF21)	<input type="checkbox"/>	18 (AF21)
19	19	<input type="checkbox"/>	19
20 (AF22)	20 (AF22)	<input type="checkbox"/>	20 (AF22)
21	21	<input type="checkbox"/>	21
22 (AF23)	22 (AF23)	<input type="checkbox"/>	22 (AF23)
23	23	<input type="checkbox"/>	23
24 (CS3)	24 (CS3)	<input type="checkbox"/>	24 (CS3)
25	25	<input type="checkbox"/>	25
26 (AF31)	26 (AF31)	<input type="checkbox"/>	26 (AF31)
27	27	<input type="checkbox"/>	27
28 (AF32)	28 (AF32)	<input type="checkbox"/>	28 (AF32)
29	29	<input type="checkbox"/>	29
30 (AF33)	30 (AF33)	<input type="checkbox"/>	30 (AF33)
31	31	<input type="checkbox"/>	31
32 (CS4)	32 (CS4)	<input type="checkbox"/>	32 (CS4)
33	33	<input type="checkbox"/>	33
34 (AF41)	34 (AF41)	<input type="checkbox"/>	34 (AF41)
35	35	<input type="checkbox"/>	35
36 (AF42)	36 (AF42)	<input type="checkbox"/>	36 (AF42)
37	37	<input type="checkbox"/>	37
38 (AF43)	38 (AF43)	<input type="checkbox"/>	38 (AF43)
39	39	<input type="checkbox"/>	39
40 (CS5)	40 (CS5)	<input type="checkbox"/>	40 (CS5)
41	41	<input type="checkbox"/>	41
42	42	<input type="checkbox"/>	42
43	43	<input type="checkbox"/>	43
44	44	<input type="checkbox"/>	44
45	45	<input type="checkbox"/>	45
46 (EF)	46 (EF)	<input type="checkbox"/>	46 (EF)
47	47	<input type="checkbox"/>	47
48 (CS6)	48 (CS6)	<input type="checkbox"/>	48 (CS6)
49	49	<input type="checkbox"/>	49
50	50	<input type="checkbox"/>	50
51	51	<input type="checkbox"/>	51
52	52	<input type="checkbox"/>	52
53	53	<input type="checkbox"/>	53
54	54	<input type="checkbox"/>	54
55	55	<input type="checkbox"/>	55
56 (CS7)	56 (CS7)	<input type="checkbox"/>	56 (CS7)
57	57	<input type="checkbox"/>	57
58	58	<input type="checkbox"/>	58
59	59	<input type="checkbox"/>	59
60	60	<input type="checkbox"/>	60
61	61	<input type="checkbox"/>	61
62	62	<input type="checkbox"/>	62
63	63	<input type="checkbox"/>	63

Save Reset

## 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

#### 1. Translate

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

#### 2. 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.

### 1. Remap DP0

Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

### 2. Remap DP1

Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

## Buttons

**Save:** Click to save changes.

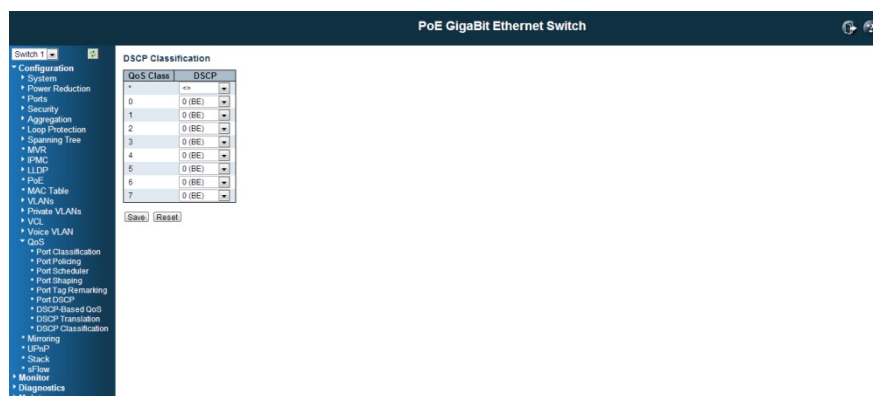
**Reset:** Click to undo any changes made locally and revert to previously saved values.

## 4.17.9 QoS / DSCP Classification

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

The settings relate to the currently selected stack unit, as reflected by the page header.

The displayed settings are:

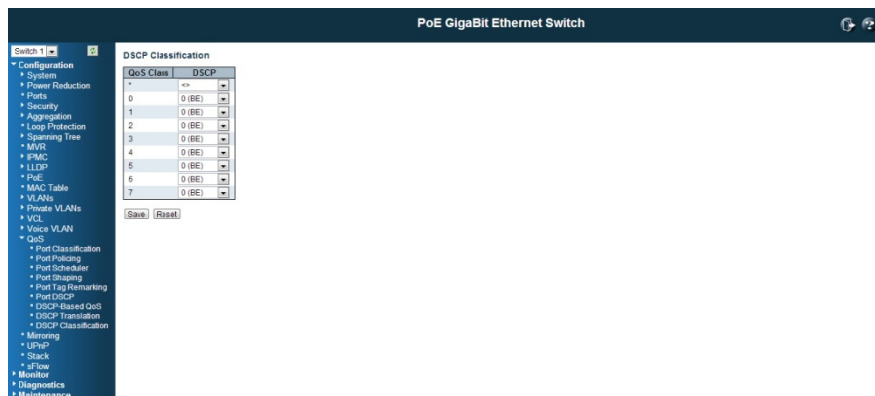


## QoS Class

Actual QoS class.

## DPL

Actual Drop Precedence Level.



## DSCP

Select the classified DSCP value (0-63).

### Buttons

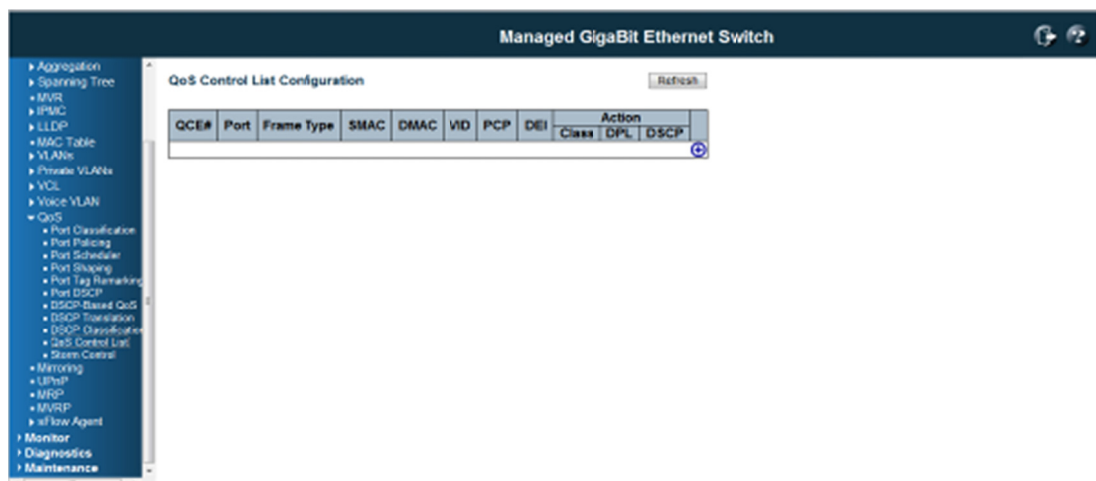
**Save:** Click to save changes.

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

### 4.17.10 QoS / Control List Configuration

#### QoS Control List Configuration

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.



### 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

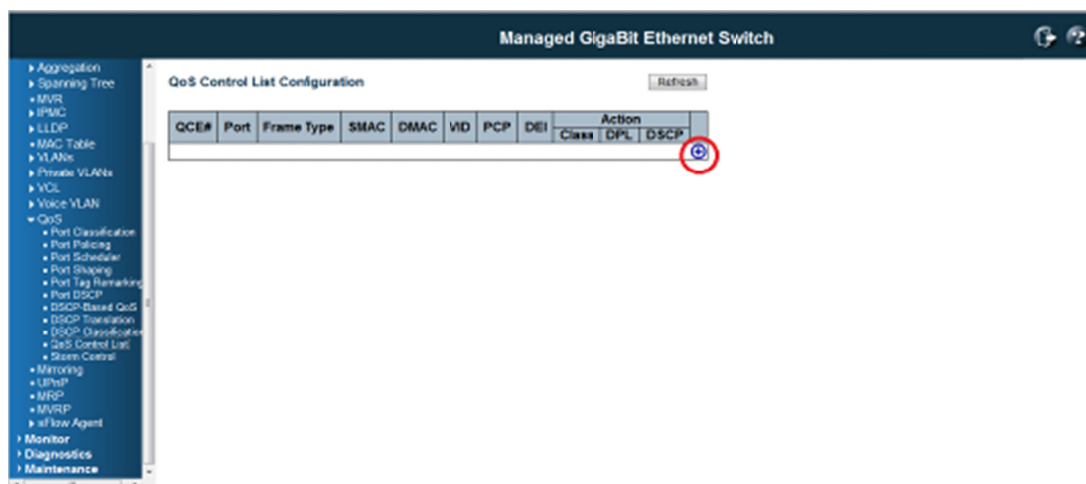
Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

### DEI

Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.

### Conflict

Displays QCE status. It may happen that resources required to add a QCE may not 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 resource required by the QCE and pressing 'Refresh' button.



## 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:

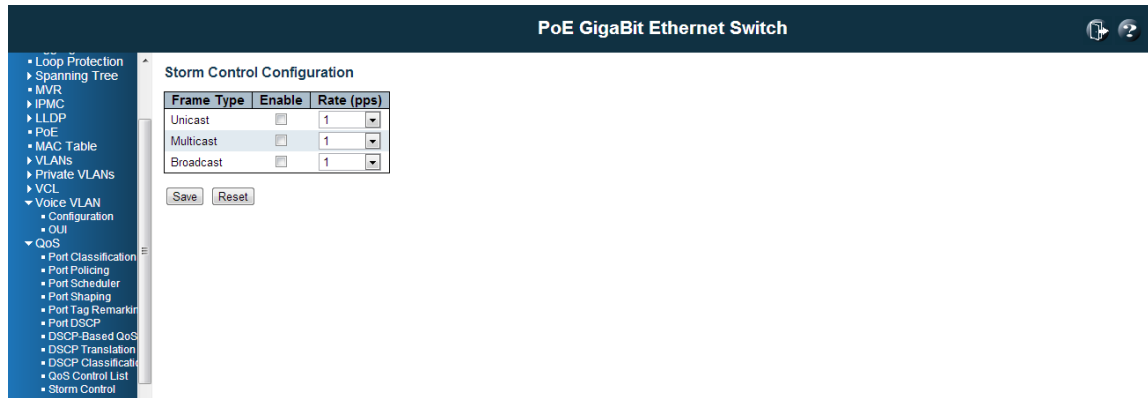
- : Inserts a new QCE before the current row.
- : Edits the QCE.
- : Moves the QCE up the list.
- : Moves the QCE down the list.
- : Deletes the QCE.
- : The lowest plus sign adds a new entry at the bottom of the QCE listings.

## Buttons

**Refresh:** Click to refresh the page. This will help to check the latest conflict status after releasing the resources.

### 4.17.11 QoS / Storm Control Configuration

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.

**Note:** Frames, which are sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.

### 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,1024K,2048K,4096K,8192K,16384K or 32768K.**

### Buttons

**Save:** Click to save changes.

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

# 4.18 Mirroring Configuration

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.

The traffic to be copied on the **mirror port** is selected as follows:

All frames received on a given port (also known as ingress or source mirroring).

All frames transmitted on a given port (also known as egress or destination mirroring).

## Port to mirror on

**Port to mirror** also known as the **mirror port**. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. **Disabled** disables mirroring.

## Mirror Port Configuration

The following table is used for Rx and Tx enabling.

Port	Mode
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled

## 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 Tx frames on the **mirror port**. 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.

## 4.19 UPnP Configuration

Configure UPnP on this page.

The screenshot shows the configuration interface for a PoE GigaBit Ethernet Switch. On the left is a navigation tree with categories like Configuration, Monitor, Diagnostics, and Maintenance. Under Configuration, various settings like System, Power Reduction, Ports, Security, and others are listed. The main area is titled 'UPnP Configuration'. It contains three fields: 'Mode' set to 'Disabled', 'TTL' set to '4', and 'Advertising Duration' set to '100'. Below these fields are 'Save' and 'Reset' buttons.

### 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**

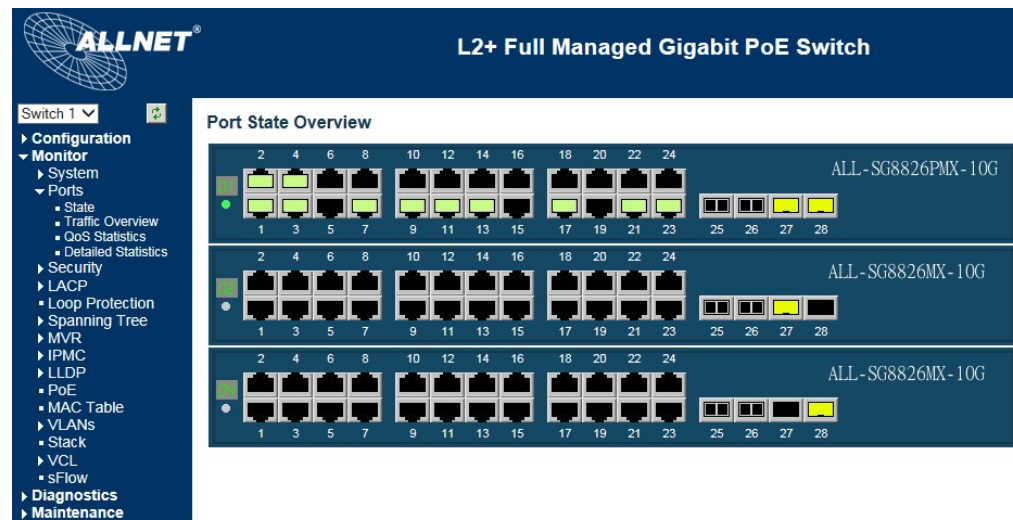
**Save:** Click to save changes.

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



## 4.20 Stack Configuration

Overview: Monitor - Ports – State



Configuration – Stack

### Stack Configuration

Stacking State	Enabled
Stacking Enabled	<input checked="" type="checkbox"/>

Delete	Stack Member	Switch ID	Master		Stack Ports	Switch Status	Switch Type
			Capable	Priority			
<input type="checkbox"/>	00:0F:C9:09:09:B4	1	Yes	1	27,28	Active	PoE Switch
<input type="checkbox"/>	00:0F:C9:78:36:E3	2	Yes	3	27,28	Active	Managed Switch
<input type="checkbox"/>	00:0F:C9:52:22:D5	4	Yes	3	27,28	Active	Managed Switch

☐ Start Master Election

Save Reset

## Monitor - Stack

### Stack Topology

Auto-refresh ☐ Refresh

State	Stacking Enabled
Topology	Chain
Member Count	3
Last Topology Change	2014-12-11T08:30:55+01:00
Master Switch	00:0F:C9:09:09:B4
Last Master Change	2014-12-11T08:30:55+01:00

### Stack List

Stack Member	Switch ID	Product		Master		
		Name	Version	Priority	Time	Reelect
00:0F:C9:09:09:B4	1	PoE Switch	PoE (stackable) dev-build by allan@localhost.localdomain 2014-10-20T17:44:04+08:00 Config.smb_switch_stackable_jr1_ref.	1	0d 05:22:22	No
00:0F:C9:78:36:E3	2	Managed Switch	Managed (stackable) dev-build by allan@localhost.localdomain 2014-10-16T15:28:29+08:00 Config.smb_switch_stackable_jr1_	3	-	No
00:0F:C9:52:22:D5	4	Managed Switch	Managed (stackable) dev-build by allan@localhost.localdomain 2014-10-16T14:43:46+08:00 Config.smb_switch_stackable_jr1_	3	-	No

### Master Forwarding Table

Stack Member	Switch ID	Ports	Distance		Forwarding	
			Port 27	Port 28	Port 27	Port 28
00:0F:C9:09:09:B4	1	1-26	0	0	Local	Local
00:0F:C9:78:36:E3	2	1-26	1	-	Active	-
00:0F:C9:52:22:D5	4	1-26	-	1	-	Active

The ALL-SG8826MX-10G includes a stacking feature by using two SFP+ ports. This allows multiple switches (up to 16) to operate as a single unit. You can set the stack configuration here.

Within a managed stack, one master switch (or just "master") must be elected. Any switch not being master is a slave switch (or just "slave").

To elect a master, the following criteria are evaluated sequentially:

1. If any switch already claims to have been master for more than 30 seconds, then that switch will become master.
2. If multiple switches claim to have been master for more than 30 seconds, then the switch which has been master for the longest period of time will become master.
3. **The switch with the highest stack priority.**
4. The switch with the smallest MAC address.

The above algorithm ensures that once a master has been elected and has been master for more than 30 seconds, it will remain master. However in some cases the user may want to enforce a new master election. This is done by clicking "Start Master Election", followed by "Save". This causes the first two criteria to be ignored, thereby basing master election only on master priority and MAC address. When master election is enforced, the first two criteria are ignored for a period of 10-15 seconds. On the Stack State Monitor web page, this is shown by "Reelect" being set to "Yes" for one of the switches in the stack.

### NOTE:

**When stacking a PoE switch with a non-PoE switch, one PoE switch must always be the master. This switch should have the highest priority in the stack (highest priority is number "1").**

### Stacking State

Indicates the stacking operation mode. Possible modes are:

**Enabled:** Enable stacking mode operation.

**Disabled:** Disable stacking mode operation.

When the stacking mode is enabled, multiple switches will operate as one single unit.

### Stacking Unit Table

This table displays all the switches (ALL-SG8826MX-10G) stacked. You can check the **Delete** checkbox to delete the selected switch, change the Switch ID, change the Priority, or change the Stack Ports here with the scroll-down menus. Also, you can view the status of all the switches that are stacked here.

### Buttons

**Save:** Click to save changes.

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

## 5. Feature Configuration - CLI

The Command Line Interface (CLI) is the user interface to the switch's embedded software system. You can view the system information, show the status, configure the switch and receive a response back from the system by keying in a command.

After login the switch through console CLI, you can see the ">" mark. You can type the command after it. There are some useful command, such as:

Type '<group>' to enter command group, e.g. 'port' to the port configuration.

Type '<group> ?' to get list of group commands, e.g. 'port ?'. You can follow the instruction step by step to finish the command.

Type '<command> ?' to get help on a command, e.g. 'port mode ?'.

Type 'up' to move up one level or '/' to go to root level

Type "logout" in root level to leave the command line interface

Click "Enter" key after finish the command.

Click "Up" key to repeat the previous commands

Commands may be abbreviated, e.g. 'por co' instead of 'port configuration'. For quick configuration, the abbreviated typo is helpful.

### Example: Configure the System Contact to Orwell

You can go to system group or type the full name in root level. Both of the methods can meet your need.

In system group mode:

```
System>contact Orwell
```

In root level:

```
>sys contact Orwell
```

**Note:** This chapter just lists the relevant command lines of the feature settings for your reference. You can see the detail explanation of the commands and features through the chapter 4.

### 5.1 System Configuration

Feature	Command Line
<b>System Information</b>	
System Group	Enter the System Configuration Group to do further configuration.  >system Type 'up' to move up one level or '/' to go to root level System>
System Contact	<b>Syntax:</b> System Name [<name>]  <b>Parameters:</b>

	<p>&lt;name&gt;: System name string. (1-255)</p> <p><b>Example:</b> Contact Name = Orwell System&gt;contact Orwell</p>
System Name	<p><b>Syntax:</b> System Name [&lt;name&gt;]</p> <p><b>Parameters:</b> &lt;name&gt;: System name string. (1-255)</p> <p><b>Example:</b> Contact Name = switch System&gt;name switch switch:/&gt; <i>(After given system name, the prompt character will be changed automatically.)</i></p>
System Location	<p><b>Syntax:</b> System Location [&lt;location&gt;]</p> <p><b>Parameters:</b> &lt;location&gt;: System location string. (1-255)</p> <p><b>Example:</b> Location Name switch:/System&gt;loca fil_01</p>
Time Zone Offset	<p><b>Syntax:</b> System Time zone [&lt;offset&gt;]</p> <p><b>Parameters:</b> &lt;offset&gt;: Time zone offset in minutes (-720 to 720) relative to UTC</p> <p><b>Example:</b> Time Zone = 100 switch:/System&gt;time 100</p>
<b>IP Configuration</b>	
IP Group	<p>Enter the IP Configuration Group</p> <p>switch:/&gt;ip Type 'up' to move up one level or '/' to go to root level switch:/IP&gt;</p>
DHCP Client	<p><b>Syntax:</b> IP DHCP [enable disable]</p> <p>switch:/IP&gt;dhcp en</p>
IP Setting (Address, Mask, Gateway, Managed VID)	<p><b>Syntax:</b> IP Setup [&lt;ip_addr&gt;] [&lt;ip_mask&gt;] [&lt;ip_router&gt;] [&lt;vid&gt;]</p> <p><b>Example:</b> IP=192.168.2.2, Mask=255.255.255.0, Gateway: 192.168.2.254, VID=1 switch:/IP&gt;setup 192.168.2.2 255.255.255.0 192.168.2.254 1</p>
NTP	<p>Enable NTP Mode by below command:</p> <p>switch:/IP&gt;ntp mode en</p> <p>Type the NTP Server address settings by below command:</p>

	<p><b>Syntax:</b></p> <p>IP NTP Server Add &lt;server_index&gt; &lt;ip_addr_string&gt;</p> <p>IP NTP Server Ipv6 Add &lt;server_index&gt; &lt;server_ipv6&gt;</p> <p>IP NTP Server Delete &lt;server_index&gt;</p> <p><b>Example:</b></p> <p>switch:/IP&gt;ntp ser add 1 192.168.100.1</p> <p>switch:/IP&gt;ntp ser add 2 168.95.1.1</p> <p>Check the NTP Server settings by below command:</p> <p>switch:/IP&gt;ntp conf</p> <p>IP NTP Configuration:</p> <p>=====</p> <p>NTP Mode : Enabled</p> <table> <tr> <th>Idx</th><th>Server IP host address (a.b.c.d) or a host name string</th></tr> <tr> <td>---</td><td>-----</td></tr> <tr> <td>1</td><td>192.168.100.1</td></tr> <tr> <td>2</td><td>168.95.1.1</td></tr> <tr> <td>3</td><td></td></tr> <tr> <td>4</td><td></td></tr> <tr> <td>5</td><td></td></tr> </table>	Idx	Server IP host address (a.b.c.d) or a host name string	---	-----	1	192.168.100.1	2	168.95.1.1	3		4		5	
Idx	Server IP host address (a.b.c.d) or a host name string														
---	-----														
1	192.168.100.1														
2	168.95.1.1														
3															
4															
5															
DNS Server	<p><b>Syntax:</b></p> <p>IP DNS [&lt;ip_addr&gt;]</p> <p><b>Parameters:</b></p> <p>&lt;ip_addr&gt;: IP address (a.b.c.d), default: Show IP address</p> <p><b>Example:</b></p> <p>switch:/IP&gt;dns 168.95.1.1</p>														
DNS Proxy	<p><b>Syntax:</b> IP DNS_Proxy [enable disable]</p> <p>switch:/IP&gt;dns_proxy en</p>														
<b>IPv6 Configuration</b>															
IPv6 Commands	<p><b>Syntax:</b></p> <p>IP IPv6 AUTOCONFIG [enable disable]</p> <p>IP IPv6 Setup [&lt;ipv6_addr&gt;] [&lt;ipv6_prefix&gt;] [&lt;ipv6_router&gt;]</p> <p>IP IPv6 State &lt;ipv6_addr&gt; [enable disable]</p> <p>IP IPv6 Ping6 &lt;ipv6_addr&gt; [(Length &lt;ping_length&gt;)] [(Count &lt;ping_count&gt;)] [(Interval &lt;ping_interval&gt;)]</p>														
Auto Configuration	<p><b>Syntax:</b></p> <p>IP IPv6 AUTOCONFIG [enable disable]</p> <p><b>Example:</b></p> <p>switch:/IP&gt;ipv6 auto en</p>														
IPv6 Address Setting (Address, Prefix,	<p><b>Syntax:</b></p> <p>IP IPv6 Setup [&lt;ipv6_addr&gt;] [&lt;ipv6_prefix&gt;] [&lt;ipv6_router&gt;]</p>														

Router)	<b>Example:</b> switch:/IP>ipv6 setup 2001:DB8::250:8bff:fee8:f800 48 2001:DB8::250:8bff:fee8:f8ff
IPv6 Ping Test	<b>Syntax:</b> IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)] <b>Example:</b> switch:/IP>ipv6 ping6 2001:DB8::250:8bff:fee8:f800
<b>NTP</b>	
NTP Mode	Enable NTP Mode by below command: switch:/IP>ntp mode en
NTP Server Address Setting	<b>Syntax:</b> Type the NTP Server address settings by below command: IP NTP Server Add <server_index> <ip_addr_string> IP NTP Server Ipv6 Add <server_index> <server_ipv6> IP NTP Server Delete <server_index> <b>Example:</b> switch:/IP>ntp ser add 1 192.168.100.1 switch:/IP>ntp ser add 2 168.95.1.1
NTP Setting Status	Check the NTP Server settings by below command:  switch:/IP>ntp conf  IP NTP Configuration: ===== NTP Mode : Enabled Idx    Server IP host address (a.b.c.d) or a host name string ---    ----- 1       192.168.100.1 2       168.95.1.1 3 4 5
<b>System Log</b>	
Server Mode	<b>Syntax:</b> System Log Server Mode [enable disable] <b>Example:</b> switch:/System>log server mode en
Server Address	<b>Syntax:</b> System Log Server Address [<ip_addr_string>] <b>Example:</b> switch:/System>log server add 192.168.2.100
Syslog Level	<b>Syntax:</b> System Log Level [info warning error]

	<p><b>Information:</b> switch:/System&gt;log level inf</p> <p><b>Warning:</b> switch:/System&gt;log level war</p> <p><b>Error:</b> switch:/System&gt;log level err</p>
Clear Syslog	<p><b>Syntax:</b> System Log Clear [all info warning error]</p> <p>switch:/System&gt;log clear all</p>
System Log Configuration	<p>switch:/System&gt;log conf</p> <p>System Log Configuration: =====</p> <p>System Log Server Mode : Enabled System Log Server Address : 192.168.2.100 System Log Level : Error</p>

## 5.2 Power Reduction

Feature	Command Line
<b>LED Power Reduction</b>	
LED Intensity Times	<p><b>Syntax:</b> led_power timers [&lt;hour&gt;] [&lt;intensity&gt;]</p> <p><b>Parameters:</b> &lt;hour&gt; : The hour (0-24) at which to change LEDs intensity &lt;intensity&gt;: The LED intensity in % (0-100)</p> <p><b>Example: (Time=2:00, Intensity: 30%)</b> led_power&gt;timer 2 30</p>
Maintenance	<p><b>Syntax:</b> led_power maintenance [&lt;maintenance_time&gt;] [on_at_errors leave_at_errors]</p> <p><b>Parameters:</b> &lt;maintenance_time&gt; : Time in seconds (0-65535) that the LEDs shall be turned on, when any port changes link state on_at_errors leave_at_errors: on_at_error if LEDs shall be turned on if any errors has been detected. leave_at_errors if no LED change shall happen when errors have been detected</p> <p><b>Example:</b> led_power&gt;main 20 led_power&gt;main 20 on (20 sec., on_ad_errors enabled)</p>



EEE Configuration	
EEE Port Configuration	<p><b>Syntax:</b> EEE Mode [&lt;port_list&gt;] [enable disable]</p> <p><b>Parameters:</b> &lt;port_list&gt;: Port list or 'all', default: All ports enable : Enable EEE disable: Disable EEE</p> <p><b>Example:</b> Enable Port 1-5 EEE&gt;mode 1-5 en</p>
Urgent Queue of Port	<p><b>Syntax:</b> EEE Urgent_queues [&lt;port_list&gt;] [&lt;queue_list&gt;]</p> <p><b>Parameters:</b> &lt;port_list&gt; : Port list or 'all', default: All ports &lt;queue_list&gt;: List of queues to configure as urgent queues (1-8 or none)</p> <p><b>Example:</b> Enable Urgent_Queue on Port 1-5 EEE&gt;urge 1-5 2</p>

### 5.3 Port Configuration

Feature	Command Line
Port Configuration	
Port Group	switch:/>port Type 'up' to move up one level or '/' to go to root level switch:/Port>
Link State	<p><b>Syntax:</b> Port State [&lt;port_list&gt;] [enable disable]</p> <p><b>Example:</b> Enable/Disable Port 1 State. After port 1 disabled, the port can't access the switch.            Port&gt;state 1 en            Port&gt;state 1 dis</p>
Link Speed and Duplex	<p><b>Syntax:</b> Port Mode [&lt;port_list&gt;]            [auto 10hdx 10fdx 100hdx 100fdx 1000fdx sfp_auto_ams 100x_ams 100fx_ams 1000x 100fx]</p> <p><b>Example:</b>            Port&gt;mode 2 1000fdx (Configure port 2 to 1000 Full Duplex)            Port&gt;mode 1-4 1000fdx (Configure port 1-4 to 1000 Full Duplex)</p>
Flow Control	<p><b>Syntax:</b> Port Flow Control [&lt;port_list&gt;] [enable disable]</p>

	<b>Example:</b> Port>flow cont 1 en    (Enable Flow Control on Port 1) Port>flow cont 1 dis   (Disable Flow Control on Port 2)																																																
Maximum Frame Size	<b>Syntax:</b> Port MaxFrame [<port_list>] [<max_frame>]  <b>Example:</b> Set port 1-24's maximum frame size to 9K jumbo frame  Port>maxf 1-24 9600																																																
Port Status																																																	
Port Status	Port>conf 1-2  Port Configuration: =====																																																
	<table><tr><td>Port</td><td>State</td><td>Mode</td><td>Flow Control</td><td>MaxFrame</td><td>Power</td><td>Excessive</td><td>Link</td></tr><tr><td>---</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>---</td><td></td><td></td></tr><tr><td>1</td><td>Enabled</td><td>Auto</td><td>Disabled</td><td>9600</td><td>Disabled</td><td>Discard</td><td>Down</td></tr><tr><td>2</td><td>Enabled</td><td>Auto</td><td>Disabled</td><td>9600</td><td>Disabled</td><td>Discard</td><td>1Gfdx</td></tr><tr><td colspan="8">.....</td></tr></table>	Port	State	Mode	Flow Control	MaxFrame	Power	Excessive	Link	---	-----	-----	-----	-----	---			1	Enabled	Auto	Disabled	9600	Disabled	Discard	Down	2	Enabled	Auto	Disabled	9600	Disabled	Discard	1Gfdx	.....															
Port	State	Mode	Flow Control	MaxFrame	Power	Excessive	Link																																										
---	-----	-----	-----	-----	---																																												
1	Enabled	Auto	Disabled	9600	Disabled	Discard	Down																																										
2	Enabled	Auto	Disabled	9600	Disabled	Discard	1Gfdx																																										
.....																																																	
Port Mode	Port>mode 2  Port    Mode            Link ----   -----   ----  2       Auto            1Gfdx																																																
Port Status - All Information	switch:/Port>config  Port Configuration: =====																																																
	<table><tr><td>Port</td><td>State</td><td>Mode</td><td>Flow Control</td><td>MaxFrame</td><td>Power</td><td>Excessive</td><td>Link</td></tr><tr><td>---</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>---</td><td></td><td></td></tr><tr><td>1</td><td>Enabled</td><td>Auto</td><td>Disabled</td><td>9600</td><td>Disabled</td><td>Discard</td><td>Down</td></tr><tr><td>2</td><td>Enabled</td><td>Auto</td><td>Disabled</td><td>9600</td><td>Disabled</td><td>Discard</td><td>1Gfdx</td></tr><tr><td>3</td><td>Enabled</td><td>Auto</td><td>Disabled</td><td>9600</td><td>Disabled</td><td>Discard</td><td>Down</td></tr><tr><td colspan="8">.....</td></tr></table>	Port	State	Mode	Flow Control	MaxFrame	Power	Excessive	Link	---	-----	-----	-----	-----	---			1	Enabled	Auto	Disabled	9600	Disabled	Discard	Down	2	Enabled	Auto	Disabled	9600	Disabled	Discard	1Gfdx	3	Enabled	Auto	Disabled	9600	Disabled	Discard	Down	.....							
Port	State	Mode	Flow Control	MaxFrame	Power	Excessive	Link																																										
---	-----	-----	-----	-----	---																																												
1	Enabled	Auto	Disabled	9600	Disabled	Discard	Down																																										
2	Enabled	Auto	Disabled	9600	Disabled	Discard	1Gfdx																																										
3	Enabled	Auto	Disabled	9600	Disabled	Discard	Down																																										
.....																																																	
Status of Link UP ports	switch:/Port>conf all up  Port Configuration: =====																																																
	<table><tr><td>Port</td><td>State</td><td>Mode</td><td>Flow Control</td><td>MaxFrame</td><td>Power</td><td>Excessive</td><td>Link</td></tr><tr><td>---</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>---</td><td></td><td></td></tr><tr><td>2</td><td>Enabled</td><td>Auto</td><td>Disabled</td><td>9600</td><td>Disabled</td><td>Discard</td><td>1Gfdx</td></tr></table>	Port	State	Mode	Flow Control	MaxFrame	Power	Excessive	Link	---	-----	-----	-----	-----	---			2	Enabled	Auto	Disabled	9600	Disabled	Discard	1Gfdx																								
Port	State	Mode	Flow Control	MaxFrame	Power	Excessive	Link																																										
---	-----	-----	-----	-----	---																																												
2	Enabled	Auto	Disabled	9600	Disabled	Discard	1Gfdx																																										
Port Statistic	switch:/Port>statistic 1  Port 1 Statistics:  Rx Packets:																																																

## 5.4 Security Configuration

Feature	Command Line				
<b>Security-Switch Configuration</b>					
Security -Switch Group	<p>&gt;securi swi Type 'up' to move up one level or '/' to go to root level Security/Switch&gt;?</p> <p>Command Groups: -----</p> <p>Security Switch Users : User management Security Switch Privilege: Privilege level Security Switch Auth : Authentication Security Switch SSH : Secure Shell Security Switch HTTPS : Hypertext Transfer Protocol over Secure Socket Layer Security Switch Access : Access management Security Switch SNMP : Simple Network Management Protocol Security Switch RMON : Remote Network Monitoring</p>				
User Configuration	<p>Security/Switch&gt;user ? Available Commands:</p> <p>Security Switch Users Configuration Security Switch Users Add &lt;user_name&gt; &lt;password&gt; &lt;privilege_level&gt; Security Switch Users Delete &lt;user_name&gt;</p>				
Add New User	<p><b>Syntax:</b> Security Switch Users Add &lt;user_name&gt; &lt;password&gt; &lt;privilege_level&gt;</p> <p><b>Example:</b> Add New User Name, Password with highest privilege, Name: Orwell, Password: password, Privilege: 15</p> <p>Security/Switch&gt;users add Orwell password 15</p>				
Delete the User	<p><b>Syntax:</b> Security Switch Users Delete &lt;user_name&gt;</p> <p><b>Example:</b> Delete the User, Orwell from User Name database</p> <p>Security/Switch&gt;users del Orwell</p>				
User Name Database	<p>Security/Switch&gt;users conf</p> <p>Users Configuration: =====</p> <table> <tr> <td>User Name</td><td>Privilege Level</td></tr> <tr> <td>-----</td><td>-----</td></tr> </table>	User Name	Privilege Level	-----	-----
User Name	Privilege Level				
-----	-----				



	<p>Security/Switch&gt;https mode dis</p> <p>Security Switch HTTPS Redirect [enable disable]  Security/Switch&gt;https mode en (Must enabled HTTPS)  Security/Switch&gt;https redi en</p> <p><b>Result:</b>  Security/Switch&gt;https conf</p> <p>HTTPS Configuration:  =====</p> <p>HTTPS Mode : Enabled  HTTPS Redirect Mode : Enabled</p>
Access Management	<p><b>Syntax:</b>  Security Switch Access Add &lt;access_id&gt; &lt;start_ip_addr&gt;  &lt;end_ip_addr&gt; [web] [snmp  ] [telnet]</p> <p><b>Example:</b> Limit the IP range from the 192.168.2.1 to  192.168.2.10 can access the web UI.</p> <p>Security/Switch&gt;access add 1 192.168.2.1 192.168.2.10 web</p>
SNMP System Configuration (Mode, Version, Read /Write Community)	<p><b>Syntax:</b>  Security Switch SNMP Mode [enable disable]  Security Switch SNMP Version [1 2c 3]  Security Switch SNMP Read Community [&lt;community&gt;]  Security Switch SNMP Write Community [&lt;community&gt;]</p> <p><b>Example:</b>  Security/Switch&gt;snmp mode en  Security/Switch&gt;snmp ver 2c  Security/Switch/SNMP&gt;read com abc  Security/Switch/SNMP&gt;write com orwell</p> <p><b>Result:</b>  SNMP Configuration:  =====</p> <p>SNMP Mode : Enabled  SNMP Version : 2c  Read Community : abc  Write Community : orwell</p>
SNMP Community	<p><b>Syntax:</b>  Security Switch SNMP Community Add &lt;community&gt;  [&lt;ip_addr&gt;] [&lt;ip_mask&gt;]  Security Switch SNMP Community Delete &lt;index&gt;  Security Switch SNMP Community Lookup [&lt;index&gt;]</p> <p><b>Example:</b>  Security/Switch&gt;snmp commu add abc  Security/Switch&gt;snmp commu add test 192.168.2.100  255.255.255.0</p>

SNMP Trap Server Setting	<p>Enter the SNMP Trap Configuration Group</p> <p>Security/Switch/SNMP&gt;trap Type 'up' to move up one level or '/' to go to root level Security/Switch/SNMP/Trap&gt;</p> <p><b>Syntax:</b> Security Switch SNMP Trap Mode [enable disable] Security Switch SNMP Trap Version [1 2c 3] Security Switch SNMP Trap Community [&lt;community&gt;] Security Switch SNMP Trap Destination [&lt;ip_addr_string&gt;] Security Switch SNMP Trap IPv6 Destination [&lt;ipv6_addr&gt;]</p> <p><b>Example:</b> Security/Switch/SNMP/Trap&gt;mode ena Security/Switch/SNMP/Trap&gt;version 2c Security/Switch/SNMP/Trap&gt;community public Security/Switch/SNMP/Trap&gt;destination 192.168.2.100</p> <p><b>Result:</b></p> <pre> Trap Mode                : Enabled Trap Version              : 2c Trap Community            : public Trap Destination          : 192.168.2.100 Trap IPv6 Destination     : :: </pre>
SNMP Trap Event Setting	<p><b>Syntax:</b> Security Switch SNMP Trap Authentication Failure [enable disable] Security Switch SNMP Trap Link-up [enable disable] Security Switch SNMP Trap Inform Mode [enable disable] Security Switch SNMP Trap Inform Timeout [&lt;timeout&gt;] Security Switch SNMP Trap Inform Retry Times [&lt;retries&gt;]</p> <p><b>Example:</b> Security/Switch/SNMP&gt;trap auth fai en Security/Switch/SNMP&gt;trap link-up en Security/Switch/SNMP&gt;trap info mode en Security/Switch/SNMP&gt;trap info time 5 Security/Switch/SNMP&gt;trap info ret times 5</p> <p><b>Result:</b></p> <pre> Trap Authentication Failure : Enabled Trap Link-up and Link-down  : Enabled Trap Inform Mode            : Enabled Trap Inform Timeout (seconds) : 5 Trap Inform Retry Times     : 5 </pre>
SNMPv3 User	<p><b>Syntax:</b> Security Switch SNMP User Add &lt;engineid&gt; &lt;user_name&gt; [MD5 SHA] [&lt;auth_password&gt;] [DES] [&lt;priv_password&gt;]</p> <p><b>Example:</b> Security/Switch/SNMP&gt;user add 800007e5017f000001 orwell Security/Switch/SNMP&gt;user add 800007e5017f000001 andy</p>

	<div>md5 andy123</div> <div><b>Result:</b> SNMPv3 Users Table:<table><thead><tr><th>Idx</th><th>Engine ID</th><th>User Name</th><th>Level</th><th>Auth Priv</th></tr></thead><tbody><tr><td>1</td><td>Local</td><td>default_user</td><td>NoAuth, NoPriv</td><td>None</td></tr><tr><td>2</td><td>Local</td><td>orwell</td><td>NoAuth, NoPriv</td><td>None</td></tr><tr><td>3</td><td>Local</td><td>andy</td><td>Auth, NoPriv</td><td>MD5 None</td></tr></tbody></table><div>Number of entries: 3</div></div>	Idx	Engine ID	User Name	Level	Auth Priv	1	Local	default_user	NoAuth, NoPriv	None	2	Local	orwell	NoAuth, NoPriv	None	3	Local	andy	Auth, NoPriv	MD5 None
Idx	Engine ID	User Name	Level	Auth Priv																	
1	Local	default_user	NoAuth, NoPriv	None																	
2	Local	orwell	NoAuth, NoPriv	None																	
3	Local	andy	Auth, NoPriv	MD5 None																	
RMON	<div>In Security/Switch Group, the system supports 4 types RMON groups, please follow the RMON Syntax to add the entries.</div> <div><b>Syntax:</b> Security/Switch&gt;rmon ?</div> <div><b>Statistics:</b> Security Switch RMON Statistics Add &lt;stats_id&gt; &lt;data_source&gt; Security Switch RMON Statistics Delete &lt;stats_id&gt; Security Switch RMON Statistics Lookup [&lt;stats_id&gt;]</div> <div><b>Histroy:</b> Security Switch RMON History Add &lt;history_id&gt; &lt;data_source&gt; [&lt;interval&gt;] [&lt;buckets&gt;] Security Switch RMON History Delete &lt;history_id&gt; Security Switch RMON History Lookup [&lt;history_id&gt;]</div> <div><b>Alarm:</b> Security Switch RMON Alarm Add &lt;alarm_id&gt; &lt;interval&gt; &lt;alarm_vairable&gt; [absolute delta] &lt;rising_threshold&gt; &lt;rising_event_index&gt; &lt;falling_threshold&gt; &lt;falling_event_index&gt; [rising falling both] Security Switch RMON Alarm Delete &lt;alarm_id&gt; Security Switch RMON Alarm Lookup [&lt;alarm_id&gt;]</div> <div><b>Event:</b> Security Switch RMON Event Add &lt;event_id&gt; [none log trap log_trap] [&lt;community&gt;] [&lt;description&gt;] Security Switch RMON Event Delete &lt;event_id&gt; Security Switch RMON Event Lookup [&lt;event_id&gt;]</div>																				
Security-Network Configuration																					
Limit Control																					
Limit Control - System Configuration	<div><b>Syntax:</b> Security Network Limit Configuration [&lt;port_list&gt; Security Network Limit Mode [enable disable] Security Network Limit Aging [enable disable] Security Network Limit Agetime [&lt;age_time&gt;]</div> <div><b>Example:</b> Security/Network&gt;limit mode enable Security/Network&gt;limit agin enable Security/Network&gt;limit agetim 1000</div> <div><b>Result:</b></div>																				

	Port Security Limit Control Configuration: ===== Mode : Enabled Aging : Disabled Age Period: 3600
Limit Control - Port Configuration	<b>Syntax:</b> Security Network Limit Port [<port_list>] [enable disable] Security Network Limit [<port_list>] [<limit>] Security Network Limit Action [<port_list>] [none trap shut trap_shut] Security Network Limit Reopen [<port_list>]  <b>Example:</b> Security/Network>limit port 1 enabl Security/Network>limit 1 5 Security/Network>limit action 1 trap
<b>Network Access Server Configuration (also known as IEEE 802.1X)</b>	
NAS System Configuration	<b>Syntax:</b> <b>Mode:</b> Security Network NAS Mode [enable disable] Security Network NAS Reauthentication [enable disable]  <b>Time Settings</b> Security Network NAS ReauthPeriod [<reauth_period>] Security Network NAS EapolTimeout [<eapol_timeout>] Security Network NAS Agetime [<age_time>] Security Network NAS Holdtime [<hold_time>]  <b>Radius-Assigned</b> Security Network NAS RADIUS_QoS [global <port_list>] [enable disable] Security Network NAS RADIUS_VLAN [global <port_list>] [enable disable]  <b>Guest VLAN</b> Security Network NAS Guest_VLAN [global <port_list>] [enable disable] [<vid>] [<reauth_max>] [<allow_if_eapol_seen>]  <b>Example:</b> Guest_VLAN Global Enabled, Guest VLAN ID=100, Max. Re-Authentication Count = 10, Allow Guest VLAN if EAPOL See = Enable  Security/Network>nas gues glob en 100 10 en
NAS Port Configuration	<b>Syntax:</b> Security Network NAS State [<port_list>] [auto authorized unauthorized single multi macbased]  auto= Port-based 802.1X authorized = Force Authorized unauthorized = Force Unauthorized single = Single 802.1X



	multi= Multi 802.1X macbased = MAC_Based Authentication  <b>Example:</b> Security/Network>nas state 2 auto																											
<b>ACL (Access Control List)</b>																												
ACL Port Configuration	<b>Syntax:</b> Security Network ACL Action [<port_list>] [permit deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>]  <b>Parameters:</b> <port_list> : Port list or 'all', default: All ports permit : Permit forwarding (default) deny : Deny forwarding <rate_limiter> : Rate limiter number (1-15) or 'disable' <port_redirect>: Port list for copy of frames or 'disable' <mirror> : Mirror of frames: enable disable <logging> : System logging of frames: log log_disable <shutdown> : Shut down ingress port: shut shut_disable  <b>Example:</b> Security/Network/ACL>Action 1 permit 10 dis en log shut  <b>Result:</b> ACL Configuration: =====																											
	<table><tr><td>Port</td><td>Policy</td><td>Action</td><td>Rate L.</td><td>Port C.</td><td>Mirror</td><td>Logging</td><td>Shutdown</td><td>Counter</td></tr><tr><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>1</td><td>0</td><td>Permit</td><td>10</td><td>Disabled</td><td>Enabled</td><td>Enabled</td><td>Enabled</td><td>0</td></tr></table>	Port	Policy	Action	Rate L.	Port C.	Mirror	Logging	Shutdown	Counter	-----	-----	-----	-----	-----	-----	-----	-----	-----	1	0	Permit	10	Disabled	Enabled	Enabled	Enabled	0
Port	Policy	Action	Rate L.	Port C.	Mirror	Logging	Shutdown	Counter																				
-----	-----	-----	-----	-----	-----	-----	-----	-----																				
1	0	Permit	10	Disabled	Enabled	Enabled	Enabled	0																				
Rate Limiter	<b>Syntax:</b> Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]  <b>Parameters:</b> <rate_limiter_list>: Rate limiter list (1-16), default: All rate limiters <rate_unit> : IP flags: pps kbps, default: pss <rate>: Rate in pps (0-100) or kbps (0, 100, 2*100, 3*100, ..., 1000000)  <b>Example: Rate Limiter ID=10, Rate = 300kbps</b> Security/Network/ACL>rate 10 kbps 300  <b>Result:</b> Rate Limiter    Rate -----    ----  ..... 9                    1 PPS 10                   300 KBPS .....																											
ACL Policy	<b>Syntax:</b> Security Network ACL Policy [<port_list>] [<policy>]  <b>Example:</b> Security/Network/ACL>policy 1 2																											

Access Control List	<p><b>Syntax:</b>  Security Network ACL Add [&lt;ace_id&gt;] [&lt;ace_id_next&gt;]  [(port &lt;port_list&gt;)] [(policy &lt;policy&gt; &lt;policy_bitmask&gt;)]  [&lt;tagged&gt;] [&lt;vid&gt;] [&lt;tag_prio&gt;] [&lt;dmac_type&gt;] [(etype  [&lt;etype&gt;] [&lt;smac&gt;] [&lt;dmac&gt;])]    (arp [&lt;sip&gt;] [&lt;dip&gt;] [&lt;smac&gt;] [&lt;arp_opcode&gt;]  [&lt;arp_flags&gt;])    (ip [&lt;sip&gt;] [&lt;dip&gt;] [&lt;protocol&gt;] [&lt;ip_flags&gt;])    (icmp [&lt;sip&gt;] [&lt;dip&gt;] [&lt;icmp_type&gt;] [&lt;icmp_code&gt;]  [&lt;ip_flags&gt;])    (udp [&lt;sip&gt;] [&lt;dip&gt;] [&lt;sport&gt;] [&lt;dport&gt;] [&lt;ip_flags&gt;])    (tcp [&lt;sip&gt;] [&lt;dip&gt;] [&lt;sport&gt;] [&lt;dport&gt;] [&lt;ip_flags&gt;]  [&lt;tcp_flags&gt;])    [permit deny] [&lt;rate_limiter&gt;] [&lt;port_redirect&gt;] [&lt;mirror&gt;]  [&lt;logging&gt;][&lt;shutdown&gt;]</p> <p><b>Parameters:</b>  &lt;ace_id&gt; : ACE ID (1-256), default: Next available ID  &lt;ace_id_next&gt; : Next ACE ID (1-256), default: Add ACE last  port : Port ACE keyword  &lt;port_list&gt; : Port list or 'all', default: All ports  policy : Policy ACE keyword  &lt;policy&gt; : Policy number (0-255)  &lt;policy_bitmask&gt;: Policy number bitmask (0x0-0xFF)  &lt;tagged&gt; : Tagged of frames: any enable disable  &lt;vid&gt; : VLAN ID (1-4095) or 'any'  &lt;tag_prio&gt; : VLAN tag priority (0-7) or 'any'  &lt;dmac_type&gt; : DMAC type:  any unicast multicast broadcast  etype : Ethernet Type keyword  &lt;etype&gt; : Ethernet Type: 0x600 - 0xFFFF or 'any'  but excluding 0x800(IPv4) 0x806(ARP) and 0x86DD(IPv6)  &lt;smac&gt; : Source MAC address ('xx-xx-xx-xx-xx-xx'  or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal  digit) or 'any'  &lt;dmac&gt; : Destination MAC address  ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x  is a hexadecimal digit) or 'any'  arp : ARP keyword  &lt;sip&gt; : Source IP address (a.b.c.d/n) or 'any'  &lt;dip&gt; : Destination IP address (a.b.c.d/n) or 'any'  &lt;arp_opcode&gt; : ARP operation code: any arp rarp other  &lt;arp_flags&gt; : ARP flags: request smac tmac len ip ether  [0 1 any]  ip : IP keyword  &lt;protocol&gt; : IP protocol number (0-255) or 'any'  &lt;ip_flags&gt; : IP flags: ttl options fragment [0 1 any]  icmp : ICMP keyword  &lt;icmp_type&gt; : ICMP type number (0-255) or 'any'  &lt;icmp_code&gt; : ICMP code number (0-255) or 'any'  udp : UDP keyword  &lt;sport&gt; : Source UDP/TCP port range (0-65535) or  'any'  &lt;dport&gt; : Destination UDP/TCP port range  (0-65535) or 'any'</p>
---------------------	--

	<p>tcp : TCP keyword</p> <p>&lt;tcp_flags&gt; : TCP flags: fin syn rst psh ack urg [0 1 any]</p> <p>permit : Permit forwarding (default)</p> <p>deny : Deny forwarding</p> <p>&lt;rate_limiter&gt; : Rate limiter number (1-15) or 'disable'</p> <p>&lt;port_redirect&gt; : Port list for copy of frames or 'disable'</p> <p>&lt;mirror&gt; : Mirror of frames: enable disable</p> <p>&lt;logging&gt; : System logging of frames:</p> <p>log log_disable</p> <p>&lt;shutdown&gt; : Shut down ingress port:</p> <p>shut shut_disable</p> <p><b>Example:</b></p> <p><b>Add one ACE:</b></p> <p>Security/Network/ACL&gt;add 2 port 6-10 policy 3 8 ip</p> <p>ACE ID 2 added last</p> <p><b>Edit one ACE:</b></p> <p>Security/Network/ACL&gt;add 1 port 1-5 policy 2 8 any</p> <p>ACE ID 1 modified last</p> <p><b>Result:</b></p> <table><tr><th>ID</th><th>Type</th><th>Port</th><th>Policy</th><th>Frame</th><th>Action</th><th>Rate L.</th><th>Port C.</th><th>Mirror</th><th>Counter</th></tr><tr><td>1</td><td>User</td><td>1-5</td><td>2 /0x8</td><td>Any</td><td>Permit</td><td>Disabled</td><td>Disabled</td><td>Disabled</td><td>0</td></tr><tr><td>2</td><td>User</td><td>6-10</td><td>3 /0x8</td><td>IP</td><td>Permit</td><td>Disabled</td><td>Disabled</td><td>Disabled</td><td>0</td></tr></table>	ID	Type	Port	Policy	Frame	Action	Rate L.	Port C.	Mirror	Counter	1	User	1-5	2 /0x8	Any	Permit	Disabled	Disabled	Disabled	0	2	User	6-10	3 /0x8	IP	Permit	Disabled	Disabled	Disabled	0
ID	Type	Port	Policy	Frame	Action	Rate L.	Port C.	Mirror	Counter																						
1	User	1-5	2 /0x8	Any	Permit	Disabled	Disabled	Disabled	0																						
2	User	6-10	3 /0x8	IP	Permit	Disabled	Disabled	Disabled	0																						
<b>DHCP</b>																															
DHCP Snooping	<p><b>Syntax:</b></p> <p>Security Network DHCP Snooping Mode [enable disable]</p> <p>Security Network DHCP Snooping Port Mode [&lt;port_list&gt;]</p> <p>[trusted untrusted]</p> <p>Security Network DHCP Snooping Statistics [&lt;port_list&gt;]</p> <p>[clear]</p> <p><b>Example:</b></p> <p>Security/Network&gt;dhcp snooping mode en</p> <p>Security/Network&gt;dhcp snooping port mode 1 tru (Port 1)</p> <p>Security/Network&gt;dhcp snooping port mode 1-10 tru (Port 1-10)</p>																														
DHCP Relay	<p><b>Syntax:</b></p> <p>Security Network DHCP Relay Mode [enable disable]</p> <p>Security Network DHCP Relay Server [&lt;ip_addr&gt;]</p> <p>Security Network DHCP Relay Information Mode [enable disable]</p> <p>Security Network DHCP Relay Information Policy [replace keep drop]</p> <p><b>Example:</b></p> <p>Security/Network&gt;dhcp relay server 192.168.2.100</p> <p>Security/Network&gt;dhcp relay mode en</p> <p>(Assign one Server IP before enable the Relay mode)</p> <p>Security/Network&gt;dhcp rel info mode en</p> <p>Security/Network&gt;dhcp rel info policy keep</p>																														

IP Source Guard																
IP Source Guard Configuration	<p><b>Syntax:</b> Security Network IP Source Guard Configuration Security Network IP Source Guard Mode [enable disable] Security Network IP Source Guard Port Mode [&lt;port_list&gt;] [enable disable] Security Network IP Source Guard limit [&lt;port_list&gt;] [&lt;dynamic_entry_limit&gt; unlimited] Security Network IP Source Guard Entry [&lt;port_list&gt;] add delete &lt;vid&gt; &lt;allowed_ip&gt; &lt;allowed_mac&gt; Security Network IP Source Guard Status [&lt;port_list&gt;] Security Network IP Source Guard Translation</p> <p><b>Example:</b> Security/Network&gt;ip source guard mode en Security/Network&gt;ip source guard port mode 1-10 en (Port 1-10) Security/Network&gt;ip source guard limit 1-10 2 (limit 2 MAC Address)</p>															
IP Source Guard Static Table	<p><b>Syntax:</b> Security Network IP Source Guard Entry [&lt;port_list&gt;] add delete &lt;vid&gt; &lt;allowed_ip&gt; &lt;allowed_mac&gt;</p> <p><b>Example:</b> Security/Network&gt;ip source guard entry 5 add 2 192.168.2.101 001122334455</p> <p><b>Result:</b> IP Source Guard Entry Table:</p> <table><thead><tr><th>Type</th><th>Port</th><th>VLAN</th><th>IP Address</th><th>MAC Address</th></tr></thead><tbody><tr><td>Static</td><td>1</td><td>1</td><td>192.168.2.10</td><td>11-22-33-44-55-66</td></tr><tr><td>Static</td><td>5</td><td>2</td><td>192.168.2.101</td><td>00-0b-16-21-2c-37</td></tr></tbody></table>	Type	Port	VLAN	IP Address	MAC Address	Static	1	1	192.168.2.10	11-22-33-44-55-66	Static	5	2	192.168.2.101	00-0b-16-21-2c-37
Type	Port	VLAN	IP Address	MAC Address												
Static	1	1	192.168.2.10	11-22-33-44-55-66												
Static	5	2	192.168.2.101	00-0b-16-21-2c-37												
ARP Inspection																
ARP Inspection	<p><b>Syntax:</b> Security Network ARP Inspection Configuration Security Network ARP Inspection Mode [enable disable] Security Network ARP Inspection Port Mode [&lt;port_list&gt;] [enable disable] Security Network ARP Inspection Entry [&lt;port_list&gt;] add delete &lt;vid&gt; &lt;allowed_mac&gt; &lt;allowed_ip&gt; Security Network ARP Inspection Status [&lt;port_list&gt;] Security Network ARP Inspection Translation</p> <p><b>Example:</b> Security/Network&gt;arp inspection mode en Security/Network&gt;arp inspection port mode 1-10 en Security/Network&gt;arp inspection entry 1 add 10 112233445566 192.168.2.10</p> <p>Security/Network&gt;arp inspection status</p> <p>ARP Inspection Entry Table:</p>															

	<div> <div>TypePortVLANMAC AddressIP Address</div> <div>-----</div> <div>Static1100b-16-21-2c-37-42192.168.2.10</div> </div>
<b>Security-AAA Configuration</b>	
Common Server Configuration	<b>Syntax:</b> Security AAA Timeout [<timeout>] Security AAA Deadtime [<dead_time>]
RADIUS Authentication Server	<b>Syntax:</b> Security AAA RADIUS [<server_index>] [enable disable] [<ip_addr_string>] [<secret>] [<server_port>]  <b>Example:</b> Security>aaa radi 1 en 192.168.2.200 password 1812
RADIUS Accounting Server	<b>Syntax:</b> Security AAA ACCT_RADIUS [<server_index>] [enable disable] [<ip_addr_string>] [<secret>] [<server_port>]  <b>Example:</b> Security>aaa ACCT_radi 1 en 192.168.2.200 password 1813
TACACS+ Authentication Server	<b>Syntax:</b> Security AAA TACACS+ [<server_index>] [enable disable] [<ip_addr_string>] [<secret>] [<server_port>]  <b>Example:</b> Security>aaa tacacs+ 1 en 192.168.2.200 password 49
AAA Configuration	Security>aaa con  AAA Configuration: ===== <div> <div>Server Timeout : 15 seconds</div> <div>Server Dead Time : 300 seconds</div> </div> RADIUS Authentication Server Configuration: ===== <div> <div> <div>ServerModeIP AddressSecretPort</div> <div>-----</div> <div> 1Enabled192.168.2.200*****1812 2Disabled1812 3Disabled1812 4Disabled1812 5Disabled1812 </div> </div> </div> RADIUS Accounting Server Configuration: ===== <div> <div> <div>ServerModeIP AddressSecretPort</div> <div>-----</div> <div> 1Enabled192.168.2.200*****1813 2Disabled1813 3Disabled1813 4Disabled1813 </div> </div> </div>

	5	Disabled		1813
TACACS+ Authentication Server Configuration:				
=====				
Server	Mode	IP Address	Secret	Port
-----				
1	Enabled	192.168.2.200	*****	49
2	Disabled			49
3	Disabled			49
4	Disabled			49
5	Disabled			49
Security>				

## 5.5 Aggregation Configuration

Feature	Command Line
<b>Static Aggregation Configuration</b>	
Aggregation Group Configuration	<p><b>Syntax:</b> Aggr Add &lt;port_list&gt; [&lt;aggr_id&gt;]</p> <p><b>Example:</b> Add port 5-8 to Group 1 &gt;aggr add 5-8 1</p> <p>&gt;aggr del 1    (Delete the group 1)</p>
Hash Code Contributors	<p><b>Syntax:</b> Aggr Mode [smac dmac ip port] [enable disable]</p> <p>smac = Source MAC Address dmac = Destination MAC Address ip = IP Address port = TCP/UDP Port Number</p> <p><b>Example:</b> Only the Source MAC Hash is enabled. The rest mode are disabled.</p> <p>&gt;aggr mode smac en &gt;aggr mode dmac dis &gt;aggr mode ip dis &gt;aggr mode port dis</p>
<b>LACP</b>	
LACP Port Configuration	<p><b>Syntax:</b> LACP Configuration [&lt;port_list&gt; LACP Mode [&lt;port_list&gt;] [enable disable] LACP Key [&lt;port_list&gt;] [&lt;key&gt;] LACP Role [&lt;port_list&gt;] [active passive] LACP Status [&lt;port_list&gt;] LACP Statistics [&lt;port_list&gt;] [clear]</p> <p><b>Example:</b> Configure port 5-8 to a LACP group &gt;lacp mode 5-8 en    (Mode = Enable)</p>

	>lacp key 5-8 100      (Key = 100) >lacp role 5-8 act      (Role = Enable)
--	---

## 5.6 Loop Protection

Feature	Command Line
<b>General Settings</b>	
Enable Loop Protection	<b>Syntax:</b> Loop Protect Mode [enable disable] Loop Protect Transmit [<transmit-time>] Loop Protect Shutdown [<shutdown-time>]  <b>Example:</b> >loop protect mode en
Transmission Time	>loop protect trans 10      (10 seconds)
Shutdown Time	>loop protect shut 200      (200 seconds)
<b>Port Configuration</b>	
Loop Protection - Port Configuration	<b>Syntax:</b> Loop Protect Port Mode [<port_list>] [enable disable] Loop Protect Port Action [<port_list>] [shutdown shut_log log] Loop Protect Port Transmit [<port_list>] [enable disable]  <b>Example:</b> Loop/Protect>port mode 1 en Loop/Protect>port action 1 shut_log (Shutdown Port and Log) Loop/Protect>port transmit 1 en

## 5.7 Spanning Tree

Feature	Command Line
<b>Bridge Configuration</b>	
Protocol Version	<b>Syntax:</b> STP Version [<stp_version>]  <b>Parameters:</b> <stp_version>: mstp rstp stp  <b>Example:</b> STP>ver rstp
Bridge Priority	<b>Syntax:</b> STP Msti Priority [<msti>] [<priority>]

	<p><b>Example:</b>  STP&gt;msti pri  MSTI# Bridge Priority  -----  CIST 32768</p> <p>STP&gt;msti pri 4096</p> <p>(The available priority parameter includes: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)</p>
Forward Delay	<p><b>Syntax:</b>  STP FwdDelay [&lt;delay&gt;]  (Valid values are in the range 4 to 30 seconds)</p>
Max. Age	<p><b>Syntax:</b>  STP MaxAge [&lt;max_age&gt;]  (Valid values are in the range 6 to 40 seconds, and MaxAge must be &lt;= (FwdDelay-1)*2.)</p>
Maximum Hop Count	<p><b>Syntax:</b>  STP MaxHops [&lt;maxhops&gt;]  (Valid values are in the range 6 to 40 hops)</p>
Transmit Hold Count	<p><b>Syntax:</b>  STP Txhold [&lt;holdcount&gt;]  (Valid values are in the range 1 to 10 BPDU's per second.)</p>
Advanced Setting	<p><b>Syntax:</b>  STP bpduFilter [enable disable]  STP bpduGuard [enable disable]  STP recovery [&lt;timeout&gt;]  (After recovery timeout time is set, the recovery is enabled automatically.)</p>
<b>MSTI Mapping</b>	
MSTI/VLAN Mapping	<p><b>Syntax:</b>  STP Msti Add &lt;msti&gt; &lt;vid-range&gt;</p> <p><b>Example:</b>  STP&gt;mst add 1 100  Add VLAN 100 to MSTI1</p> <p>STP&gt;mst map  MSTI VLANs mapped to MSTI  -----  MSTI1 100  MSTI2 No VLANs mapped  MSTI3 No VLANs mapped  MSTI4 No VLANs mapped  MSTI5 No VLANs mapped  MSTI6 No VLANs mapped  MSTI7 No VLANs mapped</p>
<b>Port Setting</b>	
STP Port Mode	<p><b>Syntax:</b></p>



	<p>STP Port Mode [&lt;port_list&gt;] [enable disable]  STP Port Edge [&lt;port_list&gt;] [enable disable]  STP Port AutoEdge [&lt;port_list&gt;] [enable disable]  STP Port P2P [&lt;port_list&gt;] [enable disable auto]  STP Port RestrictedRole [&lt;port_list&gt;] [enable disable]  STP Port RestrictedTcn [&lt;port_list&gt;] [enable disable]  STP Port bpdGuard [&lt;port_list&gt;] [enable disable]  STP Port Statistics [&lt;port_list&gt;] [clear]</p> <p><b>Example:</b>  STP&gt;port mode 1-24 dis (Disable STP on port 1-24)  STP&gt;port edge 1-24 en (Enable Edge port on port 1-24)  STP&gt;port autoedge 1-24 en (Enable Auto Edge on P1-24)  STP&gt;port p2p 1-24 en (Enable P2P mode on P1-24)  STP&gt;port p2p 1-24 auto (Enable Automatic P2P detection)  STP&gt;port bpd 1-24 en (Enable BPDUGuard on P1-24)</p>
Port Path Cost	<p><b>Syntax:</b>  STP Msti Port Cost [&lt;msti&gt;] [&lt;port_list&gt;] [&lt;path_cost&gt;]</p> <p><b>Parameters:</b>  &lt;msti&gt; : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)  &lt;port_list&gt;: Port list or 'all'. Port zero means aggregations.  &lt;path_cost&gt;: STP port path cost (1-200000000) or 'auto'</p> <p><b>Example: Configure CIST 0 Port Path Cost</b>  STP&gt;msti port cost 0 all auto (Path cost = auto)  STP&gt;msti port cost 0 all 100000 (Path cost = 100000)</p>
Port Priority	<p><b>Syntax:</b>  STP Msti Port Priority [&lt;msti&gt;] [&lt;port_list&gt;] [&lt;priority&gt;]</p> <p><b>Parameters:</b>  &lt;msti&gt; : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)  &lt;port_list&gt;: Port list or 'all'. Port zero means aggregations.  &lt;priority&gt; : STP port priority (0/16/32/48/.../224/240)</p> <p><b>Example: Configure CIST 0 Port Priority</b>  STP Msti Port Priority [&lt;msti&gt;] [&lt;port_list&gt;] [&lt;priority&gt;]  STP&gt;msti port priority 0 5 240 (Port 5 Priority = 240)  STP&gt;msti port priority 0 all 128 (All Ports' priority = 128)</p> <p><b>Example: Configure MSTI 1 Port Priority</b>  STP&gt;msti port priority 1 5 240 (MSTI1 port 5 priority=240)</p>

## 5.8 MVR

Feature	Command Line
<b>MVR Configuration</b>	
MVR Mode	<p><b>Syntax:</b>  MVR Mode [enable disable]</p>

MVR - VLAN Interface Setting	<b>Syntax:</b> MVR VLAN Setup [<mvid>] [add del upd] [(Name <mvr_name>)] <b>Example:</b> MVR VLAN 2, MVR Name = Source2 MVR>vlan setup 2 add Name Source2																																				
MVR - Port Role	<b>Syntax:</b> MVR VLAN Port [<vid> <mvr_name>] [<port_list>] [source receiver inactive] <b>Example:</b> Port 2 = Source Port, Port 6-7 = Receiver Port MVR>vlan port 2 2 source MVR>vlan port 2 6-7 rec																																				
Immediately Leave	<b>Syntax:</b> MVR Immediate Leave [<port_list>] [enable disable] <b>Example:</b> MVR>immedi leave 1-10 en																																				
MVR Configuration	MVR>conf (View the settings of above configuration)  MVR Configuration: ===== MVR Mode: Enabled MVR Interface Setting <table><tr><th>VID</th><th>Name</th><th>Mode</th><th>Tagging</th><th>Priority</th><th>LLQI</th></tr><tr><td>2</td><td>Source2</td><td>Dynamic</td><td>Tagged</td><td>0</td><td>5</td></tr></table> [Port Setting of Source2(VID-2)] Source Port : 2 Receiver Port: 6,7 Inactive Port: 1,3-5,8-26 [Channel Setting of Source2(VID-2)] <Empty Channel Table> MVR Immediate Leave Setting Port Immediate Leave <table><tr><td>1</td><td>Enabled</td></tr><tr><td>2</td><td>Enabled</td></tr><tr><td>3</td><td>Enabled</td></tr><tr><td>4</td><td>Enabled</td></tr><tr><td>5</td><td>Enabled</td></tr><tr><td>6</td><td>Enabled</td></tr><tr><td>7</td><td>Enabled</td></tr><tr><td>8</td><td>Enabled</td></tr><tr><td>9</td><td>Enabled</td></tr><tr><td>10</td><td>Enabled</td></tr><tr><td>11</td><td>Disabled</td></tr><tr><td>12</td><td>Disabled</td></tr></table>	VID	Name	Mode	Tagging	Priority	LLQI	2	Source2	Dynamic	Tagged	0	5	1	Enabled	2	Enabled	3	Enabled	4	Enabled	5	Enabled	6	Enabled	7	Enabled	8	Enabled	9	Enabled	10	Enabled	11	Disabled	12	Disabled
VID	Name	Mode	Tagging	Priority	LLQI																																
2	Source2	Dynamic	Tagged	0	5																																
1	Enabled																																				
2	Enabled																																				
3	Enabled																																				
4	Enabled																																				
5	Enabled																																				
6	Enabled																																				
7	Enabled																																				
8	Enabled																																				
9	Enabled																																				
10	Enabled																																				
11	Disabled																																				
12	Disabled																																				

## 5.9 IPMC

Feature	Command Line
<b>IGMP Snooping Configuration</b>	
IGMP Snooping Enable	<b>Syntax:</b> IPMC Mode [mld igmp] [enable disable]

	<b>Example:</b> IPMC>mode igmp en
Unregistered IPMCv4 Flooding Enabled	<b>Syntax:</b> IPMC Flooding [mld igmp] [enable disable] <b>Example:</b> IPMC>flood igmp en
IGMP SSM Range (Source-Specific Multicast)	<b>Syntax:</b> IPMC SSM [mld igmp] [(Range <prefix> <mask_len>)] <b>Example:</b> IPMC>ssm igmp range 239.0.0.0 8 (Range from 239.0.0.0, mask length=8)
Leave Proxy Enable	<b>Syntax:</b> IPMC Leave Proxy [mld igmp] [enable disable] <b>Example:</b> IPMC>leave proxy igmp en      (Enable) IPMC>leave proxy igmp dis      (Disable)
Proxy Enable	<b>Syntax:</b> IPMC Proxy [mld igmp] [enable disable] <b>Example:</b> IPMC>proxy igmp en      (Enable) IPMC>proxy igmp dis      (Disable)
<b>Port Related Configuration</b> (Router Port, Fast Leave, Throttling)	<b>Syntax:</b> IPMC Router [mld igmp] [<port_list>] [enable disable] IPMC Fastleave [mld igmp] [<port_list>] [enable disable] IPMC Throttling [mld igmp] [<port_list>] [limit_group_number] <b>Example:</b> IPMC>router igmp 25-26 en    (Port 25-26 are router ports) IPMC>Fast igmp 1-24 en (Enable IGMP Fast Leave on P1-24) IPMC>thro igmp 1-2 5    (Throtting of Port 1, 2 is 5 groups.)
VLAN Configuration	<b>Syntax:</b> IPMC State [mld igmp] [<vid>] [enable disable] IPMC Querier [mld igmp] [<vid>] [enable disable] IPMC Compatibility [mld igmp] [<vid>] [auto v1 v2 v3]  IPMC Parameter RV [mld igmp] [<vid>] [ipmc_param_rv] IPMC Parameter QI [mld igmp] [<vid>] [ipmc_param_qi] IPMC Parameter QRI [mld igmp] [<vid>] [ipmc_param_qri] IPMC Parameter LLQI [mld igmp] [<vid>] [ipmc_param_llqi] IPMC Parameter URI [mld igmp] [<vid>] [ipmc_param_uri]  <b>Example:</b> IPMC>state igmp 2 en    (Enable IGMP Snooping on VLAN 2)

	IPMC>quer igmp 2 en (Enable IGMP Querier on VLAN 2) IPMC>compa igmp 2 v2 (Enable IGMPv2 on VLAN 2)
<b>MLD Snooping</b>	
MLD Snooping	Note: The MLD Snooping is applied to IPv6 Multicast. The commands are the same as above IGMP Snooping (IPv4) Commands. Just chooses mld instead of igmp when seeing [mld igmp] in the syntax. The IP Address should be IPv6 format for sure.

## 5.10 LLDP Configuration

Feature	Command Line
<b>LLDP Parameters</b>	
LLDP Timers	<b>Syntax:</b> LLDP Interval [<interval>] LLDP Hold [<hold>] LLDP Delay [<delay>] LLDP Reinit [<reinit>]  <b>Example:</b> LLDP>interval 30 LLDP>hold 4 LLDP>delay 2 LLDP>reini 2
LLDP Mode	<b>Syntax:</b> LLDP Mode [<port_list>] [enable disable rx tx] (rx=RX Only, tx=TX Only)  <b>Example:</b> Enable LLDP on Ports LLDP>mode 1-10 en (Port 1-10 are enabled) LLDP>mode 1-26 en (Port 1-26 are enabled)
CDP aware	<b>Syntax:</b> LLDP cdp_aware [<port_list>] [enable disable]  <b>Example:</b> Enable CDP on Port 1-5 LLDP>cdp_a 1-5 en (CDP on Port 1-5 are enabled)
LLDP Optional_TLV Parameters	<b>Syntax:</b> LLDP optional_TLV [<port_list>] [port_descr sys_name sys_descr sys_capa mgmt_addr] [enable disable]  <b>Example:</b> LLDP>option 1-3 port en LLDP>option 1-3 sys_name en LLDP>option 1-3 sys_desc en LLDP>option 1-3 sys_capa en LLDP>option 1-3 mgmt_add en

## 5.11 sFlow Configuration

Feature	Command Line												
sFlow Configuration													
Receiver Configuration	<p><b>Syntax:</b> sFlow Receiver [release] [&lt;timeout&gt;] [&lt;ip_addr_host&gt;] [&lt;udp_port&gt;] [&lt;datagram_size&gt;]</p> <p><b>Example:</b> sFlow&gt;receiver 10 192.168.2.100 6343 1400</p> <p><b>Result:</b> Receiver Configuration: =====</p> <p>Owner : &lt;none&gt; Receiver : 192.168.2.100 UDP Port : 6343 Max. Datagram: 1400 bytes Time left : 0 seconds</p>												
Receiver Release	sFlow>receiver												
Port Configuration	<p><b>Syntax:</b> sFlow Receiver [release] [&lt;timeout&gt;] [&lt;ip_addr_host&gt;] [&lt;udp_port&gt;] [&lt;datagram_size&gt;] sFlow FlowSampler [&lt;port_list&gt;] [&lt;sampling_rate&gt;] [&lt;max_hdr_size&gt;] sFlow CounterPoller [&lt;port_list&gt;] [&lt;interval&gt;] sFlow Statistics Receiver [clear] sFlow Statistics Samplers [&lt;port_list&gt;] [clear]</p> <p><b>Example:</b></p> <p>sFlow&gt;flow 1-2 10 128 (Enable FlowSample on port 1-2, rate=10, max. size=128)</p> <p>sFlow&gt;coun 1-2 5 (Enable CounterPoller of port 1-2, and set interval to 5)</p> <p>sFlow&gt;statistic sample 1-2</p> <p>Per-Port Statistics: =====</p> <table><tr><th>Port</th><th>Rx Flow Samples</th><th>Tx Flow Samples</th><th>Counter Samples</th></tr><tr><td>1</td><td>0</td><td>0</td><td>0</td></tr><tr><td>2</td><td>0</td><td>0</td><td>0</td></tr></table>	Port	Rx Flow Samples	Tx Flow Samples	Counter Samples	1	0	0	0	2	0	0	0
Port	Rx Flow Samples	Tx Flow Samples	Counter Samples										
1	0	0	0										
2	0	0	0										

## 5.12 MAC Address Table Configuration

Feature	Command Line
<b>MAC Address Table Configuration</b>	
Aging Time Configuration	<p><b>Syntax:</b> MAC Agetime [&lt;age_time&gt;]</p> <p><b>Parameters:</b> &lt;age_time&gt;: MAC address age time (0,10-1000000) 0=disable</p> <p><b>Example:</b> MAC&gt;age 100 (change aging time to 100 seconds, the aging time range is 10-1000000) MAC&gt;age 0 (0 = Disable Aging time)</p>
MAC Learning Configuration	<p><b>Syntax:</b> MAC Learning [&lt;port_list&gt;] [auto disable secure]</p> <p><b>Example:</b> MAC&gt;lear 1-8 sec MAC&gt;lear 9-12 dis MAC&gt;learn 1-12 auto</p>
Static MAC Table	<p><b>Syntax:</b> MAC Add &lt;mac_addr&gt; &lt;port_list&gt; [&lt;vid&gt;]</p> <p><b>Example:</b> MAC&gt;add 0b16212c3742 1-5 1 (This type will be changed to hexadecimal automatically.) MAC&gt;add 0b-16-21-2c-37-42 1-10 1 (This type is hexadecimal, it will not be changed.)</p> <p><b>Result:</b></p> <pre> Non-volatile static: VID  MAC Address      Ports ---  - 1    00-10-15-02-25-2a  1-5 1    0b-16-21-2c-37-42  1-10 </pre>

## 5.13 VLAN Configuration

Feature	Command Line
<b>VLAN Configuration</b>	
VLAN Membership	<p><b>Syntax:</b> VLAN Add &lt;vid&gt; &lt;name&gt; [&lt;ports_list&gt;] VLAN Name Add &lt;name&gt; &lt;vid&gt;</p>

	<b>Example:</b> VLAN>add 3 5-8 (Add port 5-8 to VLAN 3) VLAN>name add vlan3 3 (vlan3 is the name of VLAN 3)
Port Configuration	<b>Syntax:</b> VLAN FrameType [<port_list>] [all tagged untagged] VLAN IngressFilter [<port_list>] [enable disable] VLAN tx_tag [<port_list>] [untag_pvid untag_all tag_all] VLAN PortType [<port_list>] [unaware c-port s-port s-custom-port] <b>Example:</b> VLAN>framety 1-3 all VLAN>ingr 1-3 en VLAN>tx_t 1-3 untag_pvid VLAN>portty 1-3 un

## 5.14 Private VLAN Configuration

Feature	Command Line								
<b>PVLAN Configuration</b>									
PVLAN Configuration	<b>Syntax:</b> PVLAN Configuration [<port_list>] PVLAN Add <pvlan_id> [<port_list>] PVLAN Delete <pvlan_id> PVLAN Lookup [<pvlan_id>] PVLAN Isolate [<port_list>] [enable disable] <b>Example:</b> PVLAN>add 10 9-12 PVLAN>add 10 1-2 PVLAN>add 20 1-2 PVLAN>add 20 13-18 PVLAN>iso 9-18 en (Enable Isolated Ports) <b>Result:</b> <table> <tr> <th>PVLAN ID</th><th>Ports</th></tr> <tr> <td>1</td><td>1-8,17-26</td></tr> <tr> <td>10</td><td>1,2</td></tr> <tr> <td>20</td><td>13-18</td></tr> </table>	PVLAN ID	Ports	1	1-8,17-26	10	1,2	20	13-18
PVLAN ID	Ports								
1	1-8,17-26								
10	1,2								
20	13-18								

## 5.15 VCL Configuration

Feature	Command Line
<b>MAC-based VLAN Configuration</b>	
MAC-based VLAN Configuration	<b>Syntax:</b> VCL Macvlan Add <mac_addr> <vid> [<port_list>] <b>Example:</b> VCL/Macvlan>add 001122334455 10 1-4

	<b>Result:</b> VCL/Macvlan>conf  <table><tr><td>MAC Address</td><td>VID</td><td>Ports</td></tr><tr><td>-----</td><td>----</td><td>----</td></tr><tr><td>00-0b-16-21-2c-37</td><td>10</td><td>1-4</td></tr></table>	MAC Address	VID	Ports	-----	----	----	00-0b-16-21-2c-37	10	1-4																					
MAC Address	VID	Ports																													
-----	----	----																													
00-0b-16-21-2c-37	10	1-4																													
Protocol-based VLAN Configuration																															
Protocol to Group	<b>Syntax:</b> VCL ProtoVlan Protocol Add Eth2 <ether_type> arp ip ipx at <group_id> <b>Example:</b> VCL/ProtoVlan>protocol add Eth2 0x0808 E4																														
Group to VLAN	<b>Syntax:</b> VCL ProtoVlan Vlan Add [<port_list>] <group_id> <vid> <b>Example:</b> VCL/ProtoVlan>vlan add 1-8 E4 10																														
Protocol VLAN Configuration	<b>Result:</b> VCL/ProtoVlan>conf <table><tr><td>Protocol Type</td><td>Protocol (Value)</td><td>Group ID</td></tr><tr><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>EthernetII</td><td>ETYPE:0x808</td><td>E4</td></tr><tr><td>LLC_Other</td><td>DSAP:0xff; SSAP:0xff</td><td>L3</td></tr><tr><td>LLC_SNAP</td><td>OUI-00:e0:2b; PID:0x1</td><td>S2</td></tr><tr><td>EthernetII</td><td>ETYPE:0x800</td><td>E1</td></tr></table> <table><tr><td>Group ID</td><td>VID</td><td>Ports</td></tr><tr><td>-----</td><td>----</td><td>----</td></tr><tr><td>E4</td><td>10</td><td>1-8</td></tr><tr><td>E1</td><td>10</td><td>5-8</td></tr></table>	Protocol Type	Protocol (Value)	Group ID	-----	-----	-----	EthernetII	ETYPE:0x808	E4	LLC_Other	DSAP:0xff; SSAP:0xff	L3	LLC_SNAP	OUI-00:e0:2b; PID:0x1	S2	EthernetII	ETYPE:0x800	E1	Group ID	VID	Ports	-----	----	----	E4	10	1-8	E1	10	5-8
Protocol Type	Protocol (Value)	Group ID																													
-----	-----	-----																													
EthernetII	ETYPE:0x808	E4																													
LLC_Other	DSAP:0xff; SSAP:0xff	L3																													
LLC_SNAP	OUI-00:e0:2b; PID:0x1	S2																													
EthernetII	ETYPE:0x800	E1																													
Group ID	VID	Ports																													
-----	----	----																													
E4	10	1-8																													
E1	10	5-8																													
IP Subnet-based VLAN Configuration																															
IP Subnet-based VLAN Configuration	<b>Syntax:</b> VCL IPVlan Add [<vce_id>] <ip_addr_mask> <vid> [<port_list>]  <b>Parameters:</b> <vce_id> : Unique VCE ID for each VCL entry <ip_addr_mask>: Source IP address and mask (Format: a.b.c.d/n). <vid> : VLAN ID (1-4095) <port_list> : Port list or 'all', default: All ports  <b>Example:</b> VCL/IPVlan>add 1 192.168.10.0/24 10 1-10  <b>Result:</b> <table><tr><td>VCE ID</td><td>IP Address</td><td>Mask Length</td><td>VID</td><td>Ports</td></tr><tr><td>-----</td><td>-----</td><td>----</td><td>----</td><td>----</td></tr><tr><td>1</td><td>192.168.10.0</td><td>24</td><td>10</td><td>1-10</td></tr></table>	VCE ID	IP Address	Mask Length	VID	Ports	-----	-----	----	----	----	1	192.168.10.0	24	10	1-10															
VCE ID	IP Address	Mask Length	VID	Ports																											
-----	-----	----	----	----																											
1	192.168.10.0	24	10	1-10																											



## 5.16 Voice VLAN Configuration

Feature	Command Line																				
Voice VLAN Configuration																					
Voice VLAN Configuration	<p><b>Syntax:</b> Voice VLAN Mode [enable disable] Voice VLAN ID [&lt;vid&gt;] Voice VLAN Agetime [&lt;age_time&gt;] Voice VLAN Traffic Class [&lt;class&gt;]</p> <p><b>Example:</b> Voice&gt;vlan mode en Voice&gt;vlan id 100 Voice&gt;vlan age 86400 Voice&gt;vlan traff class 7</p> <p><b>Result:</b> Voice VLAN Configuration: =====</p> <p>Voice VLAN Mode : Enabled Voice VLAN VLAN ID : 100 Voice VLAN Age Time(seconds) : 86400 Voice VLAN Traffic Class : 7</p>																				
Port Configuration	<p><b>Syntax:</b> Voice VLAN Port Mode [&lt;port_list&gt;] [disable auto force] Voice VLAN Security [&lt;port_list&gt;] [enable disable] Voice VLAN Discovery Protocol [&lt;port_list&gt;] [oui lldp both]</p> <p><b>Example:</b> Voice/VLAN&gt;port mode 1-4 auto Voice/VLAN&gt;security 1-4 en Voice/VLAN&gt;disco pro 1-4 both</p> <p><b>Result:</b> Voice VLAN Port Configuration: =====</p> <table><thead><tr><th>Port</th><th>Mode</th><th>Security</th><th>Discovery Protocol</th></tr></thead><tbody><tr><td>1</td><td>Auto</td><td>Enabled</td><td>Both</td></tr><tr><td>2</td><td>Auto</td><td>Enabled</td><td>Both</td></tr><tr><td>3</td><td>Auto</td><td>Enabled</td><td>Both</td></tr><tr><td>4</td><td>Auto</td><td>Enabled</td><td>Both</td></tr></tbody></table>	Port	Mode	Security	Discovery Protocol	1	Auto	Enabled	Both	2	Auto	Enabled	Both	3	Auto	Enabled	Both	4	Auto	Enabled	Both
Port	Mode	Security	Discovery Protocol																		
1	Auto	Enabled	Both																		
2	Auto	Enabled	Both																		
3	Auto	Enabled	Both																		
4	Auto	Enabled	Both																		
OUI Configuration	<p><b>Syntax:</b> Voice VLAN OUI Add &lt;oui_addr&gt; [&lt;description&gt;] Voice VLAN OUI Delete &lt;oui_addr&gt; Voice VLAN OUI Clear Voice VLAN OUI Lookup [&lt;oui_addr&gt;]</p> <p><b>Example:</b> Voice/VLAN&gt;oui add 00-12-08 hello</p> <p><b>Result:</b> Voice/VLAN&gt;oui lookup</p> <p>Voice VLAN OUI Table: =====</p> <p>Telephony OUI Description ----- 00-01-E3 Siemens AG phones</p>																				

	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
	00-12-77	e10
	00-12-08	hello

## 5.17 QoS Configuration

Feature	Command Line
<b>QoS Configuration</b>	
Port Classification	<p><b>Syntax:</b></p> <p>QoS Port Classification Class [&lt;port_list&gt;] [&lt;class&gt;]  QoS Port Classification DPL [&lt;port_list&gt;] [&lt;dpl&gt;]  QoS Port Classification PCP [&lt;port_list&gt;] [&lt;pcp&gt;]  QoS Port Classification DEI [&lt;port_list&gt;] [&lt;dei&gt;]  QoS Port Classification Tag [&lt;port_list&gt;] [enable disable]  QoS Port Classification Map [&lt;port_list&gt;] [&lt;pcp_list&gt;]  [&lt;dei_list&gt;] [&lt;class&gt;] [&lt;dpl&gt;]  QoS Port Classification DSCP [&lt;port_list&gt;] [enable disable]</p> <p><b>Range of the Value:</b></p> <p>&lt;class&gt;: QoS class (0-7)  &lt;dpl&gt;: Drop Precedence Level (0-1)  &lt;pcp&gt;: Priority Code Point (0-7)  &lt;dei&gt;: Drop Eligible Indicator (0-1)</p> <p><b>Example:</b></p> <p>QoS/Port/Classification&gt;clas 1-2 7  QoS/Port/Classification&gt;dpl 1-2 1  QoS/Port/Classification&gt;pcp 1-2 7  QoS/Port/Classification&gt;dei 1-2 1  QoS/Port/Classification&gt;tag 1-2 en  QoS/Port/Classification&gt;dscp 1-2 en</p>
QoS Ingress Port Tag Classification	<p><b>Syntax:</b></p> <p>QoS Port Classification Map [&lt;port_list&gt;] [&lt;pcp_list&gt;]  [&lt;dei_list&gt;] [&lt;class&gt;] [&lt;dpl&gt;]</p>
Port Policing	<p><b>Syntax:</b></p> <p>QoS Port Policer Mode [&lt;port_list&gt;] [enable disable]  QoS Port Policer Rate [&lt;port_list&gt;] [&lt;rate&gt;]  QoS Port Policer Unit [&lt;port_list&gt;] [kbps fps]  QoS Port Policer FlowControl [&lt;port_list&gt;] [enable disable]</p> <p>&lt;rate&gt; : Rate in kbps or fps (100-3300000)</p> <p><b>Example:</b></p> <p>QoS/Port/Policer&gt;mode 1-2 en  QoS/Port/Policer&gt;rate 1-2 300  QoS/Port/Policer&gt;unit 1-2 kbps  QoS/Port/Policer&gt;flow 1-2 en</p>

Port Scheduler	<p><b>Syntax:</b> Syntax: QoS Port Scheduler Mode [&lt;port_list&gt;] [strict weighted]</p> <p><b>Example:</b> QoS/Port/Scheduler&gt;mode 1-2 stric (Strict Priority) QoS/Port/Scheduler&gt;mode 1-2 wei (Weighted)</p> <p><b>QoS Egress Port Scheduler and Shapers</b> QoS/Port/Scheduler&gt;wei 1-2 1 30 (Port 1-2, Q1=30) QoS/Port/Scheduler&gt;wei 1-2 2 30 (Port 1-2, Q2=30)</p> <p>The diagram illustrates the QoS Egress Port Scheduler and Shapers architecture. It shows eight queues (Q0 to Q7) on the left, each with a 'Queue Shaper' table containing 'Enable', 'Rate', 'Unit', and 'Excess' fields. The 'Rate' field is set to 500 kbps. Arrows from these queues point to a 'Queue Scheduler' table with 'Weight' and 'Percent' columns. The 'Weight' column has values 10, 30, 30, 10, 10, 10, 10, and 10, while the 'Percent' column has values 10%, 30%, 30%, 10%, 10%, 10%, 10%, and 10%. The Queue Scheduler table points to a 'Port Shaper' table with 'Enable', 'Rate', and 'Unit' columns. The 'Rate' field is set to 500 kbps. The Port Shaper table points to a final output line. The Queue Scheduler table is labeled 'D W R R' and 'S T R I C T'.</p>
Port Shaping	<p><b>Syntax:</b> <b>Port Shaper:</b> QoS Port Shaper Mode [&lt;port_list&gt;] [enable disable] QoS Port Shaper Rate [&lt;port_list&gt;] [&lt;bit_rate&gt;]</p> <p><b>Queue Shaper:</b> QoS Port QueueShaper Mode [&lt;port_list&gt;] [&lt;queue_list&gt;] [enable disable] QoS Port QueueShaper Rate [&lt;port_list&gt;] [&lt;queue_list&gt;] [&lt;bit_rate&gt;] QoS Port QueueShaper Excess [&lt;port_list&gt;] [&lt;queue_list&gt;] [enable disable]</p> <p><b>Parameters:</b> &lt;port_list&gt;: Port list or 'all', default: All ports &lt;bit_rate&gt; : Rate in kilo bits per second (100-3300000)</p> <p><b>Example:</b> QoS/Port/Shaper&gt;rate 1-2 1000 QoS/Port/QueueShaper&gt;mode 1-2 all en (Queue Shaper) QoS/Port/QueueShaper&gt;rate 1-2 all 600 (Queue Shaper)</p>
DSCP Configuration	<p><b>Syntax:</b> QoS Port DSCP Translation [&lt;port_list&gt;] [enable disable] QoS Port DSCP Classification [&lt;port_list&gt;]</p>

	<p>[none zero selected all]</p> <p>QoS Port DSCP EgressRemark [&lt;port_list&gt;]</p> <p>[disable enable remap_dp_unaware remap_dp_aware]</p> <p><i>Note: DSCP is an advanced QoS setting, please follow the DSCP table of upper access/core switch to configure the table. The table of the whole network must be unified.</i></p>
<b>Storm Configuration</b>	
Storm Control	<p><b>Syntax:</b></p> <p>QoS Storm Unicast [enable disable] [&lt;packet_rate&gt;]</p> <p>QoS Storm Multicast [enable disable] [&lt;packet_rate&gt;]</p> <p>QoS Storm Broadcast [enable disable] [&lt;packet_rate&gt;]</p> <p>&lt;packet_rate&gt;: Rate in fps (1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k, 1024k, 2048k, 4096k, 8192k, 16384k, 32768k)</p> <p><b>Example:</b></p> <p>QoS/Storm&gt;unic en 32768k</p> <p>QoS/Storm&gt;multi en 4096k</p> <p>QoS/Storm&gt;broad en 4k</p>

## 5.18 Mirroring Configuration

Feature	Command Line																				
<b>Mirroring Configuration</b>																					
Mirror Configuration	<p><b>Syntax:</b></p> <p>Mirror Port [&lt;port&gt; disable]</p> <p>Mirror Mode [&lt;port_cpu_list&gt;] [enable disable rx tx]</p> <p><b>Example:</b></p> <p>Mirror&gt;port 5</p> <p>Mirror&gt;mode 6-8 en</p> <p><b>Result:</b></p> <p>Mirror Configuration:</p> <p>=====</p> <p>Mirror Port: 5</p> <table> <tr> <th>Port</th><th>Mode</th></tr> <tr> <td>----</td><td>-----</td></tr> <tr> <td>1</td><td>Disabled</td></tr> <tr> <td>2</td><td>Disabled</td></tr> <tr> <td>3</td><td>Disabled</td></tr> <tr> <td>4</td><td>Disabled</td></tr> <tr> <td>5</td><td>Disabled</td></tr> <tr> <td>6</td><td>Enabled</td></tr> <tr> <td>7</td><td>Enabled</td></tr> <tr> <td>8</td><td>Enabled</td></tr> </table>	Port	Mode	----	-----	1	Disabled	2	Disabled	3	Disabled	4	Disabled	5	Disabled	6	Enabled	7	Enabled	8	Enabled
Port	Mode																				
----	-----																				
1	Disabled																				
2	Disabled																				
3	Disabled																				
4	Disabled																				
5	Disabled																				
6	Enabled																				
7	Enabled																				
8	Enabled																				

## 5.19 UPnP Configuration

Feature	Command Line
<b>UPnP Configuration</b>	
UPnp Configuration	<p><b>Syntax:</b>  UPnP Configuration  UPnP Mode [enable disable]  UPnP TTL [&lt;ttl&gt;]  UPnP AdvertisingDuration [&lt;duration&gt;]</p> <p><b>Example:</b>  UPnP&gt;mode en  UPnP&gt;ttl 5 (Default=4)  UPnP&gt;adver 200 (Default=100)</p> <p><b>Result:</b>  UPnP Configuration:  =====</p> <p>UPnP Mode : Enabled  UPnP TTL : 5  UPnP Advertising Duration : 200</p>

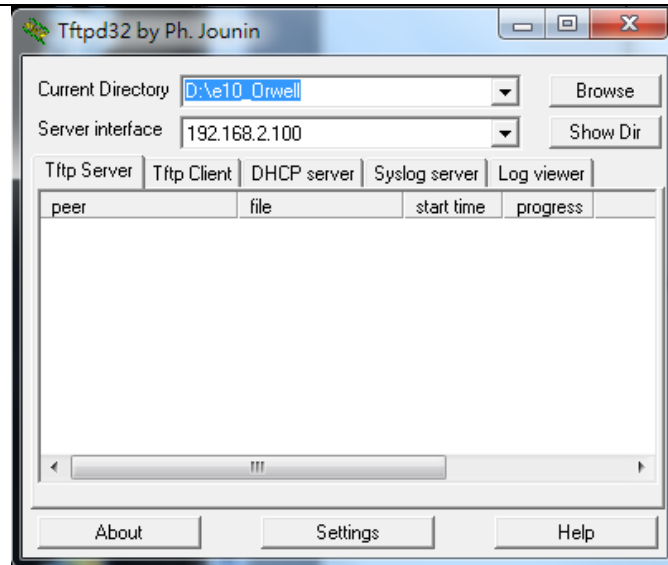
## 5.20 Diagnostic Commands

Feature	Command Line
<b>Ping</b>	
Ping Test	<p><b>Syntax:</b>  IP Ping &lt;ip_addr_string&gt; [(Length &lt;ping_length&gt;)] [(Count &lt;ping_count&gt;)] [(Interval &lt;ping_interval&gt;)]</p> <p><b>Parameters:</b>  &lt;ip_addr_string&gt;: IPv4 host address (a.b.c.d) or a host name string  length : PING Length keyword  &lt;ping_length&gt; : Ping ICMP data length (2-1452; Default is 56), excluding MAC, IP and ICMP headers  count : PING Count keyword  &lt;ping_count&gt; : Transmit ECHO_REQUEST packet count (1-60; Default is 5)  interval : PING Interval keyword  &lt;ping_interval&gt; : Ping interval (0-30; Default is 0)</p> <p><b>Example:</b> Ping IP 192.168.2.100  IP&gt;ping 192.168.2.100  PING server 192.168.2.100, 56 bytes of data.  64 bytes from 192.168.2.100: icmp_seq=0, time=0ms  64 bytes from 192.168.2.100: icmp_seq=1, time=0ms  64 bytes from 192.168.2.100: icmp_seq=2, time=0ms  64 bytes from 192.168.2.100: icmp_seq=3, time=0ms  64 bytes from 192.168.2.100: icmp_seq=4, time=0ms  Sent 5 packets, received 5 OK, 0 bad</p>
IPv6 Ping Test	<p><b>Syntax:</b>  IP IPv6 Ping6 &lt;ipv6_addr&gt; [(Length &lt;ping_length&gt;)]</p>

	<p>[(Count &lt;ping_count&gt;)] [(Interval &lt;ping_interval&gt;)]</p> <p><b>Example:</b></p> <p>switch:/IP&gt;ipv6 ping6 2001:DB8::250:8bff:fee8:f800</p>																											
VeriPHY	<p><b>Syntax:</b></p> <p>Port VeriPHY [&lt;port_list&gt;]</p> <p><b>Example:</b></p> <p>Port&gt;veriphy 24</p> <p>Starting VeriPHY, please wait</p> <table><tr><th>Port</th><th>Pair A</th><th>Length</th><th>Pair B</th><th>Length</th><th>Pair C</th><th>Length</th><th>Pair D</th><th>Length</th></tr><tr><td>----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>24</td><td>OK</td><td>0</td><td>OK</td><td>0</td><td>OK</td><td>0</td><td>OK</td><td>0</td></tr></table>	Port	Pair A	Length	Pair B	Length	Pair C	Length	Pair D	Length	----	-----	-----	-----	-----	-----	-----	-----	-----	24	OK	0	OK	0	OK	0	OK	0
Port	Pair A	Length	Pair B	Length	Pair C	Length	Pair D	Length																				
----	-----	-----	-----	-----	-----	-----	-----	-----																				
24	OK	0	OK	0	OK	0	OK	0																				

## 5.21 Maintenance Commands

Feature	Command Line
<b>Maintenance Commands</b>	
Restart Device	<p><b>Syntax:</b></p> <p>System Reboot</p> <p><b>Example:</b></p> <p>System&gt;reb</p> <p>System will reboot in a few seconds</p>
Factory Defaults	<p><b>Syntax:</b></p> <p>System Restore Default [keep_ip]</p> <p><b>Example:</b></p>
Software/Firmware (Firmware Version, Firmware Swapping, Firmware Update)	<p><b>Syntax:</b></p> <p>Firmware Information Firmware Swap Firmware Load &lt;ip_addr_string&gt; &lt;file_name&gt;</p> <p><b>Parameters of Firmware Load:</b></p> <p>&lt;ip_addr_string&gt;: IP host address (a.b.c.d) or a host name string &lt;file_name&gt; : Firmware file name</p> <p><b>Example:</b></p> <p><b>Firmware Swapping</b></p> <p>Firmware&gt;sw</p> <p>... Erase from 0x40fd0000-0x40fdffff: .</p> <p>... Program from 0x87ff0000-0x88000000 to 0x40fd0000: .</p> <p>... Program from 0x87ff000a-0x87ff000c to 0x40fd000a: .</p> <p>Alternate image activated, now rebooting.</p> <p><b>Firmware Update</b></p> <p>Firmware&gt;load 192.168.2.100 SMBStaX.dat</p> <p>Downloaded "SMBStaX.dat", 3415213 bytes</p> <p>Master initiated software updating starting</p> <p>Waiting for firmware update to complete</p> <p>Starting flash update - do not power off device!</p>



Erasing image...  
Programming image...

**Note 1:**

The switch process the firmware upgrading through TFTP protocol. When running firmware upgrading, please open the TFTP tool as TFTP server for the switch.

For example: TFTPd32 is a freeware TFTP server, you can download it from the internet. Browse the directory of the firmware file and select correct server interface.

If you failed to upload file, remember to shut down the firewall of your computer. The process may be terminated by your firewall.

**Note 2: While firmware uploading process is started, please don't shutdown the switch!**

## 6. Web Configuration - Monitor, Diagnostic, Maintenance

### 6.1 Monitor

#### 6.1.1 Monitor / System

##### 6.1.1.1 Monitor / System / Information

The switch system information is provided here.

The screenshot displays the 'System Information' page of a 'PoE GigaBit Ethernet Switch'. The interface includes a left-hand navigation menu with options like Configuration, Monitor, System, CPU Load, Log, Detailed Log, Ports, Security, LACP, Loop Protection, Spanning Tree, RSTP, LLDP, PoE, MAC Table, VLANs, Stack, VCL, and Diagnostics. The main content area shows system details organized into sections: System (Contact Name, Location), Hardware (MAC Address: 00-03-ce-22-65-88), Time (System Date: 1970-01-01T00:25:36+00:00, System Uptime: 0d 00:25:36), and Software (Software Version: PoE (stackable) dev-build by root@virtual-centos 2013-08-07T15:34:44+08:00 Config smb\_switch\_stackable\_j1\_ref.mk, Software Date: 2013-08-07T15:34:44+08:00, Acknowledgments: Details). A table at the bottom lists the switch ID (1) and chip ID (VSC7434). An 'Auto-refresh' checkbox and a 'Refresh' button are located in the top right corner.

System Information	
<strong>System</strong>	
Contact Name	
Contact Location	
<strong>Hardware</strong>	
MAC Address	00-03-ce-22-65-88
<strong>Time</strong>	
System Date	1970-01-01T00:25:36+00:00
System Uptime	0d 00:25:36
<strong>Software</strong>	
Software Version	PoE (stackable) dev-build by root@virtual-centos 2013-08-07T15:34:44+08:00 Config smb_switch_stackable_j1_ref.mk
Software Date	2013-08-07T15:34:44+08:00
Acknowledgments	Details
<strong>Software Version</strong>	
Switch ID	1
Chip ID	VSC7434

### 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.

### Chip ID

The Chip ID of this switch.

### System Date

The current (GMT) system time and date. The system time is obtained through the configured SNTP Server, if any.



## System Uptime

The period of time the device has been operational.

## Software Version

The software version of this switch.

## Software Date

The date of the switch software was produced.

## Buttons

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

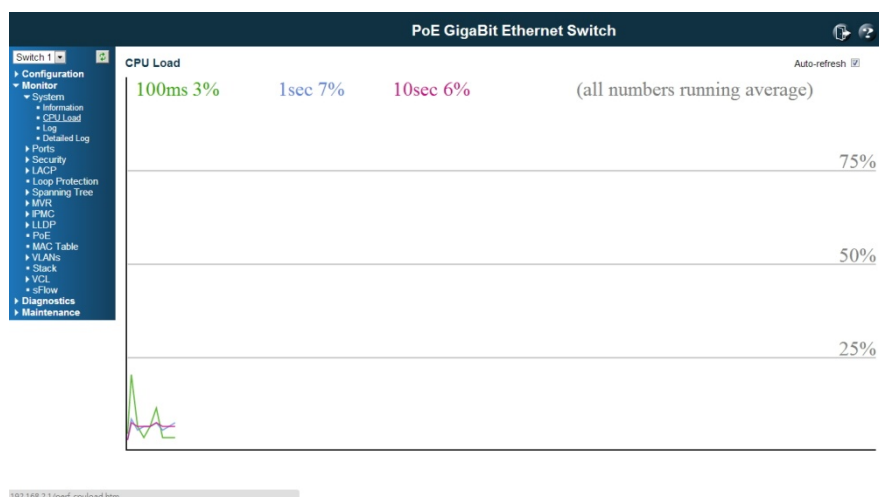
**Refresh:** Click to refresh the page; any changes made locally will be undone.

### 6.1.1.2 CPU Load

This page displays the CPU load, using an SVG graph.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.



## Buttons:

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

### 6.1.1.3 System Log Information

The switch system log information can be found here.

PoE GigaBit Ethernet Switch

Switch 1

System Log Information for Switch 1

Auto-refresh ☐ Refresh Clear << << >> >>

Level All

Clear Level All

The total number of entries is 5 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Warning	1970-01-01T00:00:00+00:00	version_string too long for SPROUT: ...
2	Info	1970-01-01T00:00:03+00:00	Switch just made a cold boot.
3	Info	1970-01-01T00:00:05+00:00	Link up on switch 1, port 2
4	Info	1970-01-01T00:00:07+00:00	Link down on switch 1, port 2
5	Info	1970-01-01T00:00:39+00:00	Link up on switch 1, port 2

352.168.2.1/syslog.htm

#### ID

The ID ( $\geq 1$ ) of the system log entry.

PoE GigaBit Ethernet Switch

Switch 1

System Log Information for Switch 1

Auto-refresh ☐ Refresh Clear << << >> >>

Level All

Clear Level All

The total number of entries is 5 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Warning	1970-01-01T00:00:00+00:00	version_string too long for SPROUT: ...
2	Info	1970-01-01T00:00:03+00:00	Switch just made a cold boot.
3	Info	1970-01-01T00:00:05+00:00	Link up on switch 1, port 2
4	Info	1970-01-01T00:00:07+00:00	Link down on switch 1, port 2
5	Info	1970-01-01T00:00:39+00:00	Link up on switch 1, port 2

352.168.2.1/syslog.htm

#### 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 enable an automatic refresh of the page at regular intervals.

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

**Clear**: Flushes all system log entries.

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

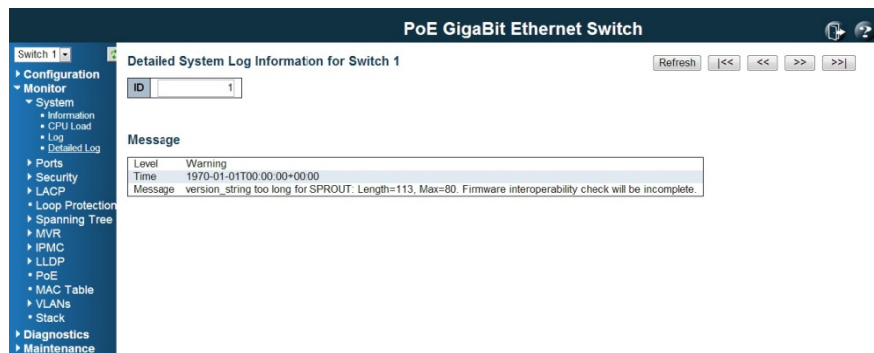
**<<**: Updates the system log entries, ending at the last entry currently displayed.

**>>**: Updates the system log entries, starting from the last entry currently displayed.

**>>**: Updates the system log entries, ending at the last available entry ID.

### 6.1.1.4 System / Detailed Log

The switch system detailed log information is provided here.



## ID

The ID ( $\geq 1$ ) 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.

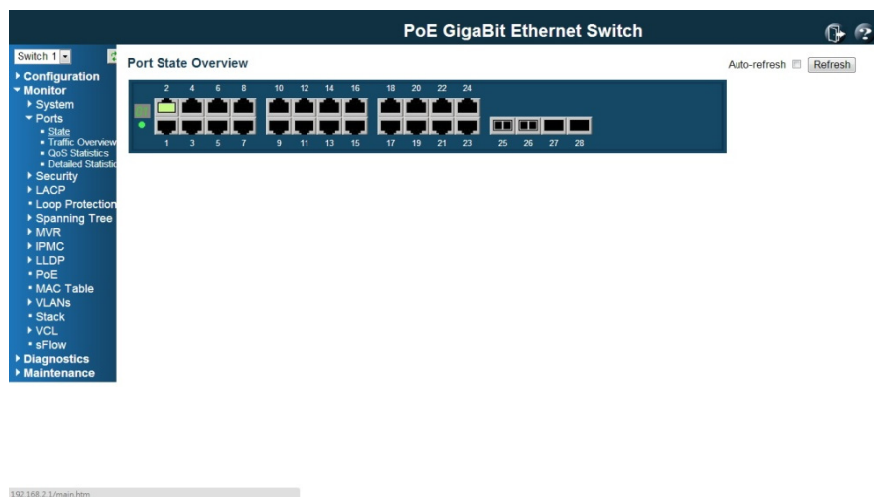
**>>:** Updates the system log entry to the next available entry ID.

**>>/:** Updates the system log entry to the last available entry ID.

## 6.1.2 Monitor / Port State

### 6.1.2.1 Port State

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



The port states are illustrated as follows:

#### RJ45 ports

#### SFP ports

#### State



## Buttons

**Auto-refresh** ☐ : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.

**Refresh:** Click to refresh the page; any changes made locally will be undone.

### 6.1.2.2 Traffic Overview

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

The displayed counters are:

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	858	1088	129942	154857	0	0	360	0	360
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	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0
27	0	12	0	912	0	0	0	0	0
28	31	12	24628	912	31	0	30	0	30

#### 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.

#### Errors

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for all ports.

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

### 6.1.2.3 QoS Statistics

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

The displayed counters are:

PoE GigaBit Ethernet Switch

Switch 1

Queuing Counters for Switch 1

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	503	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1097
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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13

190.168.2.1/qos\_counters.htm

#### 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

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for all ports.

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

### 6.1.2.4 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.

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

## 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.

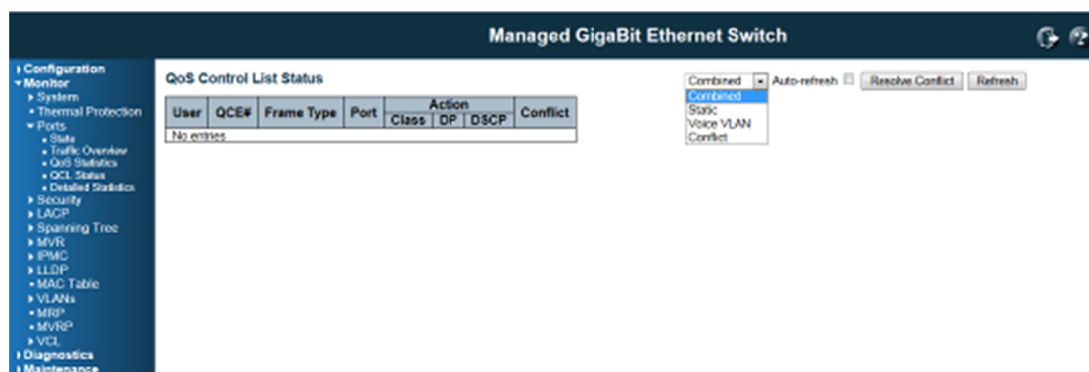
**Class:** Classified [QoS class](#); if a frame matches the QCE it will be put in the queue.

**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 at regular intervals.

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

**Refresh:** Click to refresh the page; any changes made locally will be undone

### 6.1.2.5 Detailed Port 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.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.



PoE GigaBit Ethernet Switch			
Switch 1		Port 1	
Detailed Port Statistics for Switch 1 Port 1		Auto-refresh <input type="checkbox"/> Refresh Clear	
Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
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	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	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	0		

## Receive Total and Transmit Total

### 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.

## Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

## Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

## Receive Error Counters

### 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<sup>1</sup> frames received with valid CRC.

### Rx Oversize

The number of long<sup>2</sup> frames received with valid CRC.

### Rx Fragments

The number of short<sup>1</sup> frames received with invalid CRC.

### Rx Jabber

The number of long<sup>2</sup> frames received with invalid CRC.

### Rx Filtered

The number of received frames filtered by the forwarding process.

<sup>1</sup> Short frames are frames that are smaller than 64 bytes.

<sup>2</sup> Long frames are frames that are longer than the configured maximum frame length for this port.

## Transmit Error Counters

### Tx Drops

The number of frames dropped due to output buffer congestion.

### Tx Late/Exc. Coll.

The number of frames dropped due to excessive or late collisions.

PoE GigaBit Ethernet Switch			
Switch 1	Detailed Port Statistics for Switch 1 Port 1		
Port 1	Auto-refresh	Refresh	Clear
Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
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	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	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	0		

## Buttons

The port select box determines which port is affected by clicking the buttons.

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for the selected port.

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

## 6.1. 3 Monitor / Security

### 6.1.3.1 Security / Access Management Statistics

This page provides statistics for access management.

PoE GigaBit Ethernet Switch			
Switch 1	Access Management Statistics		
Auto-refresh	Refresh	Clear	
Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTP\$	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

192.168.2.1/access\_mgmt\_statistics.htm

## Interface

The interface type through which the remote host can access the switch.

## Received Packets

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:** Click this box to enable an automatic refresh of the page at regular intervals.

**Refresh:** Click to refresh the page immediately.

**Clear:** Clear all statistics.

### 6.1.3.2 Security / Network

#### Port Security Switch Status

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

**PoE GigaBit Ethernet Switch**

Switch 1

Configuration  
Monitor  
System  
Ports  
Security  
Access  
Management  
Statistics  
Network  
Port Security  
Switch  
Port  
NAS  
ACL Status  
DHCP  
ARP Inspection  
IP Source Guard  
AAA  
Switch  
LACP  
Loop Protection  
Spanning Tree  
MVR  
PMAC  
LLDP  
PoE  
MAC Table  
VLAN  
Stack  
VCL  
Flow  
Diagnostics  
Maintenance

Port Security Switch Status

User Module Legend

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

Port Status for Switch 1

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	-	-
11	----	Disabled	-	-
12	----	Disabled	-	-
13	----	Disabled	-	-
14	----	Disabled	-	-
15	----	Disabled	-	-
16	----	Disabled	-	-
17	----	Disabled	-	-
18	----	Disabled	-	-
19	----	Disabled	-	-
20	----	Disabled	-	-
21	----	Disabled	-	-
22	----	Disabled	-	-
23	----	Disabled	-	-
24	----	Disabled	-	-
25	----	Disabled	-	-
26	----	Disabled	-	-

## User Module Legend

The legend shows all user modules that may request Port Security services.

### 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 Status

The table has one row for each port on the switch and a number of columns, which are:

### 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 (Current, Limit)

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 (-).

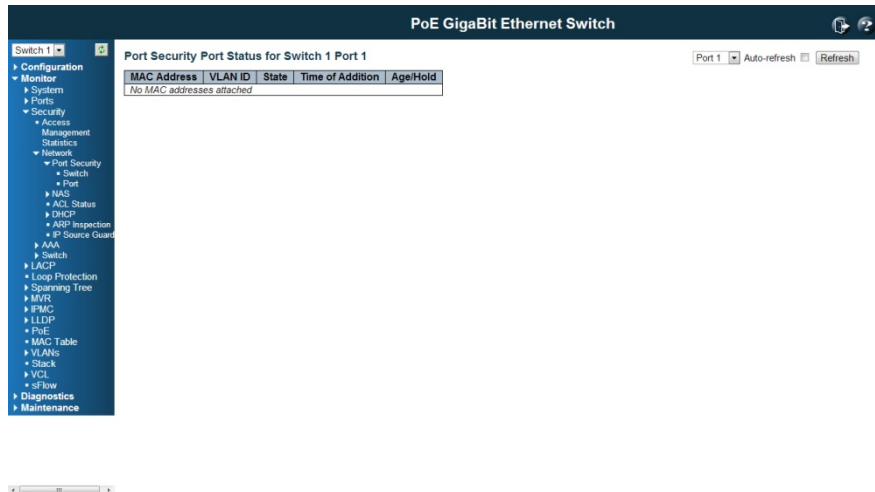
#### Buttons

**Refresh:** Click to refresh the page immediately.

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

### Port Security Port Status

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.



## 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

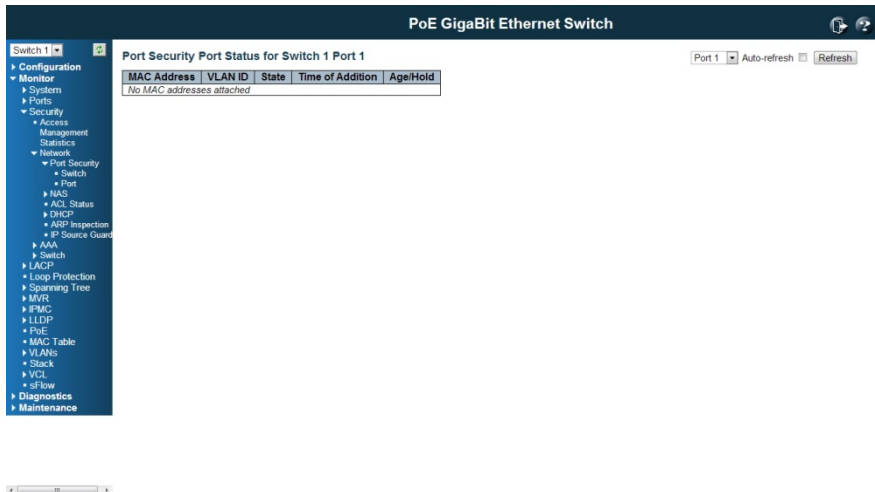
Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

## 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.



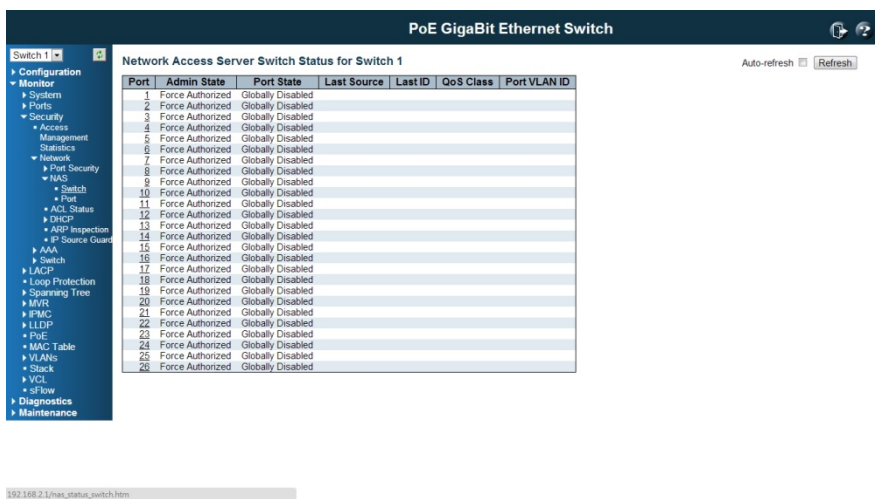
## Buttons

**Refresh:** Click to refresh the page immediately.

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

## Security / Network / NAS

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



## Port

The switch port number. Click to navigate to detailed NAS statistics for this port.



### 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.

### 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

**Refresh:** Click to refresh the page immediately.

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

## Port State

### 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.

## Port Counters

### EAPOL Counters

These supplicant frame counters are available for the following administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

EAPOL Counters			
Direction	Name	IEEE Name	Description
Rx	<b>Total</b>	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	<b>Response ID</b>	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	<b>Responses</b>	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than

			Response Identity frames) that have been received by the switch.
Rx	<b>Start</b>	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	<b>Logoff</b>	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	<b>Invalid Type</b>	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	<b>Invalid Length</b>	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	<b>Total</b>	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	<b>Request ID</b>	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	<b>Requests</b>	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

### Backend Server Counters

These backend (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X

- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Backend Server Counters			
Direction	Name	IEEE Name	Description
Rx	<b>Access Challenge</b>	dot1xAuthBackendAccessChallenges	<p><b>802.1X-based:</b> Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant.</p> <p>Indicates that the backend server has communication with the switch.</p> <p><b>MAC-based:</b> Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</p>
	<b>Other Requests</b>	dot1xAuthBackendOtherRequestsToSupplicant	<p><b>802.1X-based:</b> Counts the number of times that the switch sends an EAP Request packet</p>

			following the first to the supplicant. Indicates that the backend server chose an EAP-method. <b>MAC-based:</b> Not applicable.
Rx	<b>Auth. Successes</b>	dot1xAuthBackendAuthSuccesses	<b>802.1X- and MAC-based:</b> Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	<b>Auth. Failures</b>	dot1xAuthBackendAuthFails	<b>802.1X- and MAC-based:</b> Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	<b>Responses</b>	dot1xAuthBackendResponses	<b>802.1X-based:</b>

	<p>Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.</p> <p><b>MAC-based:</b></p> <p>Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</p>
--	---

### Last Supplicant/Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- Port-based 802.1X
- Single 802.1X

- Multi 802.1X
- MAC-based Auth.

Last Supplicant/Client Info		
Name	IEEE Name	Description
<b>MAC Address</b>	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
<b>VLAN ID</b>	-	The VLAN ID on which the last frame from the last supplicant/client was received.
<b>Version</b>	dot1xAuthLastEapolFrameVersion	<b>802.1X-based:</b> The protocol version number carried in the most recently received EAPOL frame. <b>MAC-based:</b> Not applicable.
<b>Identity</b>	-	<b>802.1X-based:</b> The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. <b>MAC-based:</b> Not applicable.

### Selected Counters

#### Selected Counters

The Selected Counters table is visible when the port is in one of the following administrative states:

- Multi 802.1X
- MAC-based Auth.

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

### Attached MAC Addresses

#### Identity

Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be

shown in the Selected Counters table. If no supplicants are attached, it shows *No supplicants attached*.

This column is not available for MAC-based Auth.

### MAC Address

For Multi 802.1X, this column holds the MAC address of the attached supplicant.

For MAC-based Auth., this column holds the MAC address of the attached client.

Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows *No clients attached*.

### VLAN ID

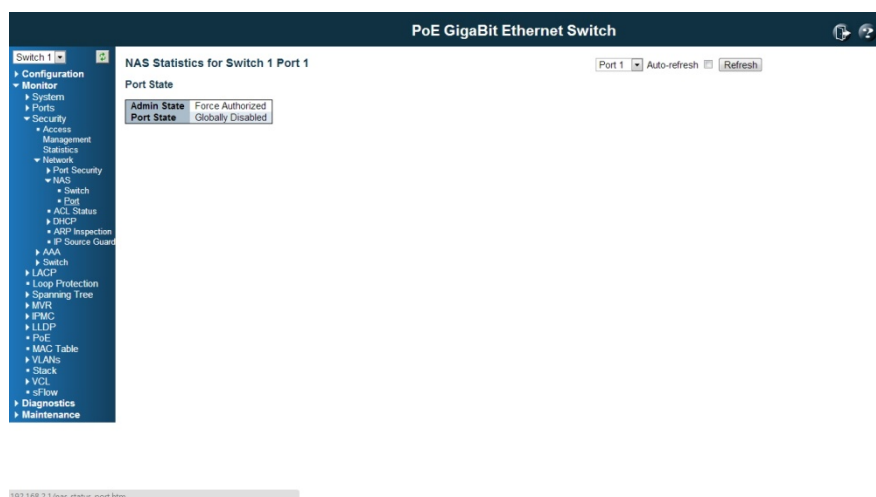
This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

### State

The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

### Last Authentication

Shows the date and time of the last authentication of the client (successful as well as unsuccessful).



### Buttons

The port select box determines which port is affected when clicking the buttons.



## Auto-refresh ☐

Check this box to enable an automatic refresh of the page at regular intervals.

Click to refresh the page immediately.

This button is available in the following modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Click to clear the counters for the selected port.

This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.

This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

## Network / ACL 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.



## 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.

## 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 Copy

Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are **Disabled** or a specific port number. When **Disabled** is displayed, the port copy 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

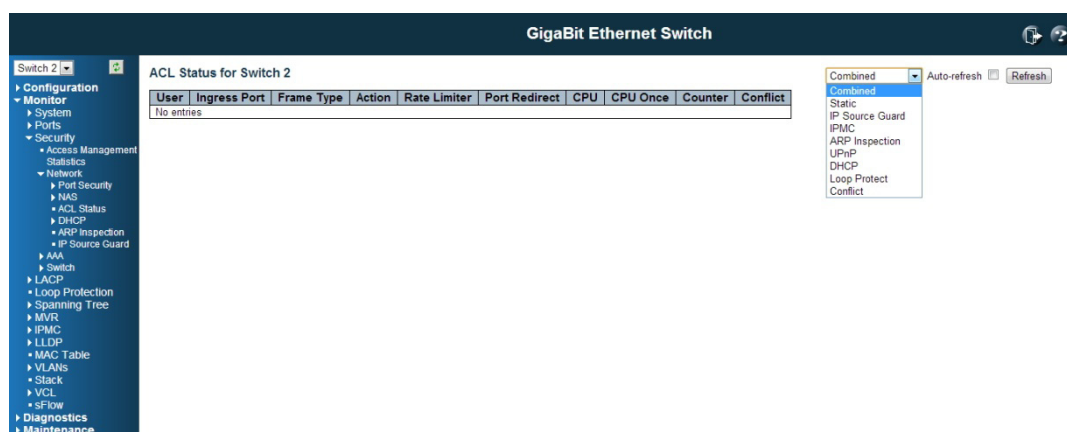
Forward first packet that matched the specific ACE to CPU.

## 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



: Select the ACL status from this drop down list.

**Refresh:** Click to refresh the page immediately.

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

## DHCP Snooping Statistics

This page provides statistics for DHCP snooping. The statistics show only packet counters when DHCP snooping mode is enabled and relay mode is disabled. And it doesn't count the DHCP packets for DHCP client.

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

192.168.2.1/dhcp\_snooping\_statistics.htm

## Receive and Transmit Packets

### Rx and Tx Discover

The number of discover (option 53 with value 1) packets received and transmitted.

### Rx and Tx Offer

The number of offer (option 53 with value 2) packets received and transmitted.

### Rx and Tx Request

The number of request (option 53 with value 3) packets received and transmitted.

### Rx and Tx Decline

The number of decline (option 53 with value 4) packets received and transmitted.

### Rx and Tx ACK

The number of ACK (option 53 with value 5) packets received and transmitted.

### Rx and Tx NAK

The number of NAK (option 53 with value 6) packets received and transmitted.

### Rx and Tx Release

The number of release (option 53 with value 7) packets received and transmitted.

### Rx and Tx Inform

The number of inform (option 53 with value 8) packets received and transmitted.

## Rx and Tx Lease Query

The number of lease query (option 53 with value 10) packets received and transmitted.

## Rx and Tx Lease Unassigned

The number of lease unassigned (option 53 with value 11) packets received and transmitted.

## Rx and Tx Lease Unknown

The number of lease unknown (option 53 with value 12) packets received and transmitted.

## Rx and Tx Lease Active

The number of lease active (option 53 with value 13) packets received and transmitted.

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

## Buttons

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

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for the selected port.

## DHCP Relay Statistics

This page provides statistics for DHCP relay.

PoE GigaBit Ethernet Switch

Switch 1

- Configuration
  - Monitor
  - System
  - Ports
  - Security
    - Access Management Statistics
    - Port Security
    - NAS
    - ACL Status
    - DHCP
      - Snooping Statistics
      - Relay Statistics
      - ARP Inspection
      - IP Source Guard
    - AAA
    - Switch
    - LACP
    - Loop Protection
    - Spanning Tree
    - MVR
    - IFMAC
    - LLDP
    - PoE
    - MAC Table
    - VLANs
    - Stack
    - VCL
    - sFlow
  - Diagnostics
  - Maintenance

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

192.168.2.1/dhcp\_relay\_statistics.htm

## Server Statistics

### 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.

## Client Statistics

### 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:** Click this box to enable an automatic refresh of the page at regular intervals.

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears statistics.

## Network / Dynamic ARP Inspection 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.

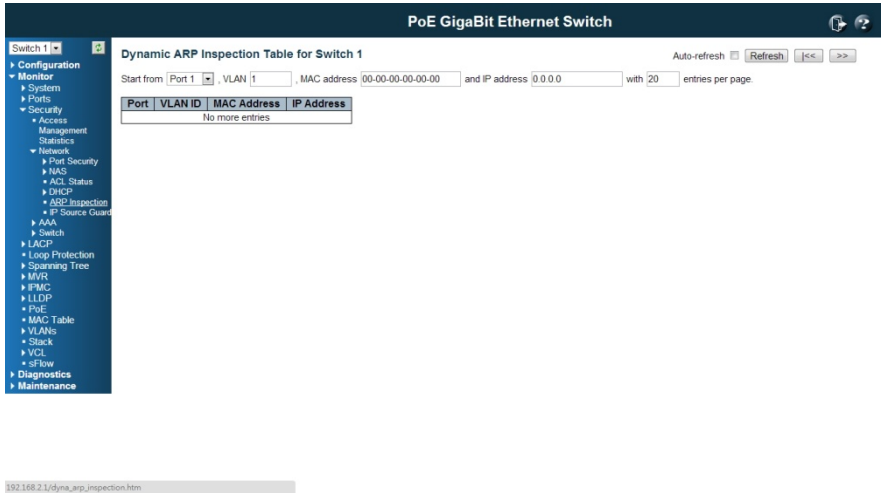
### Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection 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 Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed table as a basis for the next lookup.

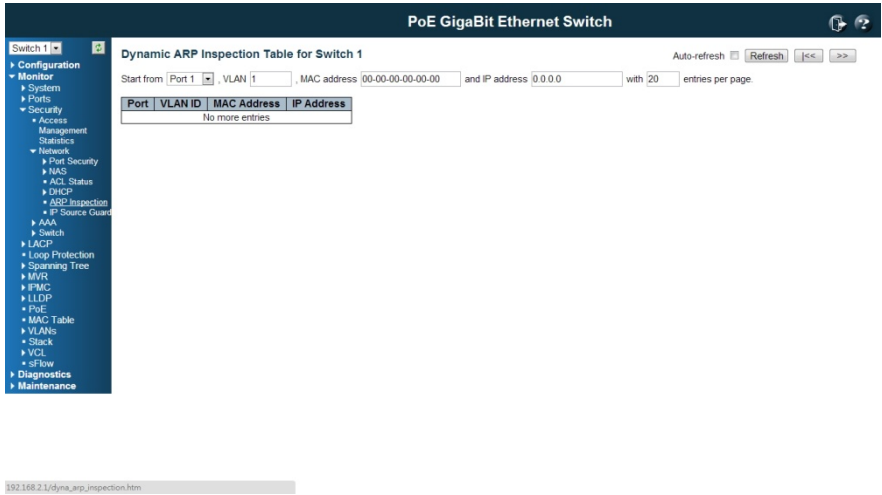
When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.



## ARP Inspection Table Columns

### 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:** Click this box to enable an automatic refresh of the page at regular intervals.

**Refresh:** Click to refresh the page immediately.

**Clear:** Flushes all dynamic entries.

**/<<:** Updates the table starting from the first entry in the Dynamic ARP Inspection Tables.

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

## Network / Dynamic IP Source Guard Table

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.

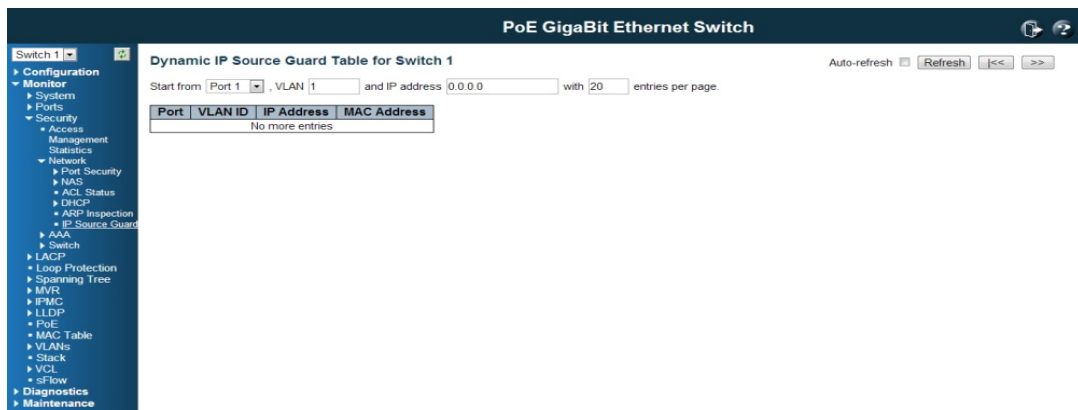
The screenshot shows the 'Dynamic IP Source Guard Table for Switch 1' interface. It includes a sidebar with navigation options (Configuration, Monitor, Ports, Security, etc.) and a main content area. The main content area has a search filter: 'Start from Port 1, VLAN 1 and IP address 0.0.0.0 with 20 entries per page'. Below this is a table with columns 'Port', 'VLAN ID', 'IP Address', and 'MAC Address'. The table currently displays 'No more entries'. There are also buttons for 'Auto-refresh', 'Refresh', and navigation arrows.

## Navigating the IP Source Guard Table

Each page shows up to 99 entries from the Dynamic IP Source Guard 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 Dynamic IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.



192.168.2.1/dyna\_ip\_source\_guard.htm

## IP Source Guard Table Columns

### 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:** Click this box to enable an automatic refresh of the page at regular intervals.

**Refresh:** Click to refresh the page immediately.

**Clear:** Flushes all dynamic entries.

**/<<:** Updates the table starting from the first entry in the Dynamic IP Source Guard Tables.

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

### 6.1.3.3 Security / AAA

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

Authentication configuration page.

The screenshot shows the configuration page for a PoE GigaBit Ethernet Switch. On the left is a navigation menu with categories like Configuration, Monitor, System, Ports, Security, Access, Management, Statistics, Network, AAA, RADIUS, Switch, LACP, Loop Protection, Spanning Tree, MVR, IPMG, LLDP, PoE, MAC Table, VLANs, Stack, VCL, and Diagnostics. The main content area is titled 'PoE GigaBit Ethernet Switch' and contains two tables: 'RADIUS Authentication Server Status Overview' and 'RADIUS Accounting Server Status Overview'. Both tables have columns for '#', 'IP Address', and 'Status'. The authentication table shows 5 servers with IP addresses 0.0.0.1812, all with a status of 'Disabled'. The accounting table shows 5 servers with IP addresses 0.0.0.1813, all with a status of 'Disabled'. There are 'Auto-refresh' and 'Refresh' buttons in the top right of the configuration area.

#	IP Address	Status
1	0.0.0.1812	Disabled
2	0.0.0.1812	Disabled
3	0.0.0.1812	Disabled
4	0.0.0.1812	Disabled
5	0.0.0.1812	Disabled

#	IP Address	Status
1	0.0.0.1813	Disabled
2	0.0.0.1813	Disabled
3	0.0.0.1813	Disabled
4	0.0.0.1813	Disabled
5	0.0.0.1813	Disabled

192.168.2.1/auth\_status\_radius\_overview.htm

### RADIUS Authentication Servers

#

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.

### State

The current state of the server. This field takes one of the following values:

**Disabled:** The server is disabled.

**Not Ready:** The server is enabled, but IP communication is not yet up and running.

**Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

**Dead (X seconds left):** Access attempts were made to this server, but it did not reply within the configured timeout. The server has 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.

### RADIUS Accounting Servers

#

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.

## State

The current state of the server. This field takes one of the following values:

**Disabled:** The server is disabled

**Not Ready:** The server is enabled, but IP communication is not yet up and running.

**Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept 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.

## Buttons

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

**Refresh:** Click to refresh the page immediately.

## RADIUS Authentication Statistics

This page provides detailed statistics for a particular RADIUS server.

The screenshot displays the configuration page for a PoE GigaBit Ethernet Switch, specifically the RADIUS Authentication and Accounting Statistics for Server #1. The interface includes a left-hand navigation menu with options like Configuration, Monitor, System, Ports, Security, Access, Management, Statistics, Network, AAA, RADIUS, Overview, RADIUS Details, Switch, LACP, Loop Protection, Spanning Tree, MVR, RMC, LLDP, PoE, MAC Table, VLANs, Stack, NCL, sFlow, Diagnostics, and Maintenance. The main content area is divided into two sections: RADIUS Authentication Statistics and RADIUS Accounting Statistics. Each section contains a table with 'Receive Packets' and 'Transmit Packets' columns, and an 'Other Info' section. The authentication statistics table shows metrics like Access Accepts, Access Rejects, Access Challenges, Malformed Access Responses, Bad Authenticators, Unknown Types, and Packets Dropped. The accounting statistics table shows Responses, Malformed Responses, Bad Authenticators, Unknown Types, and Packets Dropped. The 'Other Info' section for both tables displays the IP Address (0.0.0.0:1812), State (Disabled), and Round-Trip Time (0 ms).

RADIUS Authentication Statistics for Server #1	
Receive Packets	Transmit Packets
Access Accepts	0
Access Rejects	0
Access Challenges	0
Malformed Access Responses	0
Bad Authenticators	0
Unknown Types	0
Packets Dropped	0

RADIUS Accounting Statistics for Server #1	
Receive Packets	Transmit Packets
Responses	0
Malformed Responses	0
Bad Authenticators	0
Unknown Types	0
Packets Dropped	0

Other Info

Field	Value
IP Address	0.0.0.0:1812
State	Disabled
Round-Trip Time	0 ms

## RADIUS Authentication Statistics

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.

### Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	<b>Access Accepts</b>	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	<b>Access Rejects</b>	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	<b>Access Challenges</b>	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	<b>Malformed Access Responses</b>	radiusAuthClientExtMalformedAccessResponses	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.
Rx	<b>Bad Authenticators</b>	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	<b>Unknown Types</b>	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	<b>Packets Dropped</b>	Radius Auth Client Ext-Packets Dropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	<b>Access Requests</b>	Radius	The number of RADIUS Access-Request

		AuthClientExtAccess Requests	packets sent to the server. This does not include retransmissions.
Tx	<b>Access Retransmissions</b>	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	<b>Pending Requests</b>	radiusAuthClientExtPendingRequests	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.
Tx	<b>Timeouts</b>	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

## Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
<b>State</b>	-	Shows the state of the server. It takes one of the following values: <b>Disabled:</b> The selected server is disabled. <b>Not Ready:</b> The server is enabled, but IP communication is not yet up and running. <b>Ready:</b> The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. <b>Dead (X seconds left):</b> 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

<b>Round-Trip Time</b>		than one server is enabled.
	Radius	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that
	AuthClientExtRoundTri pTime	matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

## RADIUS Accounting Statistics

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.

The screenshot shows the configuration page for a PoE GigaBit Ethernet Switch. On the left is a navigation menu with options like Configuration, Monitor, System, Ports, Security, Access, Management, Statistics, Network, AAA, RADIUS, Switch, LACP, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, PoE, MAC Table, VLANs, Stack, VCL, and Diagnostics. The main content area displays 'RADIUS Authentication Statistics for Server #1' and 'RADIUS Accounting Statistics for Server #1'. Each section has a table with 'Receive Packets' and 'Transmit Packets' counts. The authentication table includes metrics like Access Accepts, Access Rejects, Access Challenges, Malformed Access Responses, Bad Authenticators, Unknown Types, and Packets Dropped. The accounting table includes Responses, Malformed Responses, Bad Authenticators, Unknown Types, and Packets Dropped. Both tables also show 'Other Info' including IP Address, State, and Round-Trip Time.

192.168.2.1/auth\_status\_radius\_details.htm

## Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	<b>Responses</b>	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	<b>Malformed Responses</b>	radiusAccClientExtMalformedResponses	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.
Rx	<b>Bad</b>	radiusAcctClientExtBadAu	The number of RADIUS packets

	<b>Authenticators</b>	thenticators	containing invalid authenticators received from the server.
Rx	<b>Unknown Types</b>	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	<b>Packets Dropped</b>	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	<b>Requests</b>	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	<b>Retransmissions</b>	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	<b>Pending Requests</b>	radiusAccClientExtPendingRequests	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.
Tx	<b>Timeouts</b>	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

### Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
<b>State</b>	-	Shows the state of the server. It takes one of the following values: <b>Not Ready:</b>



		<p><b>Disabled:</b> The selected server is disabled.</p> <p><b>Not Ready:</b> The server is enabled, but IP communication is not yet up and running.</p> <p><b>aReady:</b> The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.</p> <p><b>Dead (X seconds left):</b> 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.</p>
<b>Round-Trip Time</b>	radiusAccClientExtRoundTripTime	<p>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.</p>

## Buttons

The server select box determines which server is affected by clicking the buttons.

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

**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 operations..

## 6.1.3.4 Switch / SNMP / RMON

### RMON Statistics Overview

This page provides an overview of RMON statistics entries.

PoE GigaBit Ethernet Switch

Switch 1

RMON Statistics Status Overview for Switch 1

Auto-refresh ☐ Refresh

Start from Control Index 0 with 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jab.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

192.168.2.1/mon\_statistics\_status.htm

The displayed counters are:

## Data Source

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.

## 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**

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.

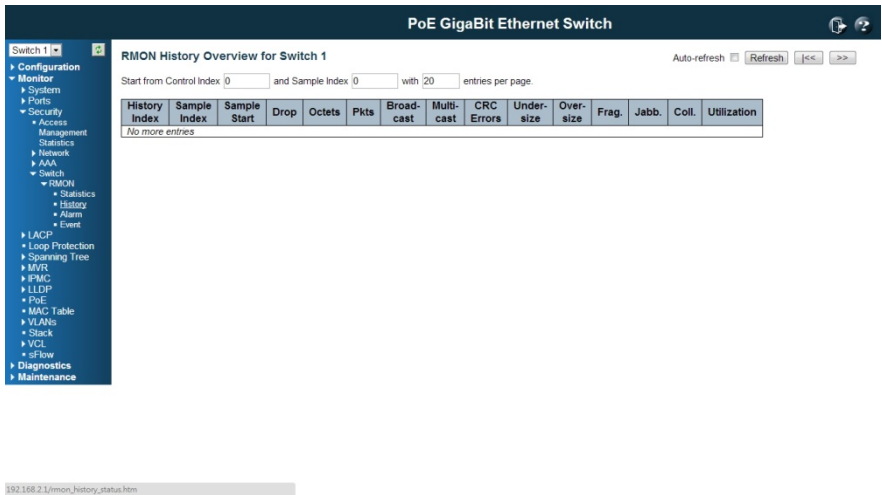
#### **Buttons**

**Refresh:** Click to refresh the page immediately.

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

# RMON History Overview

This page provides an overview of RMON history entries.



The displayed fields are:

## 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 total number of events in which packets were dropped by the probe due to lack of resources.

## Drops

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.

### **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**

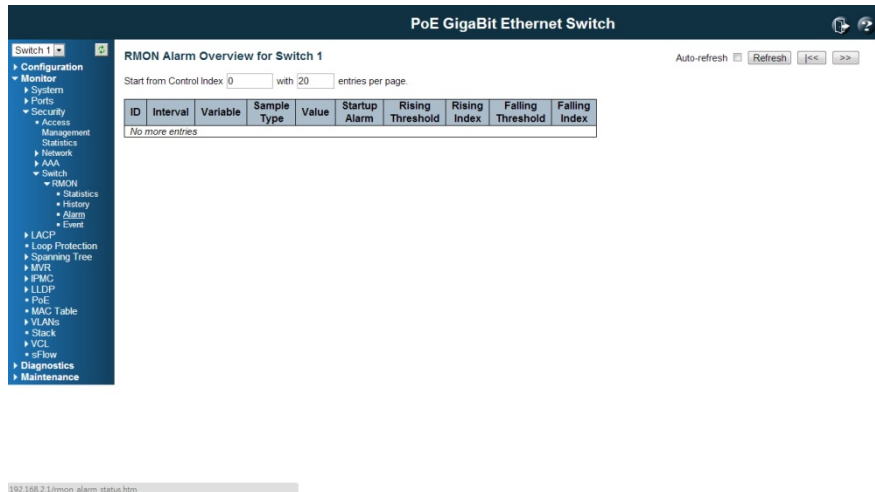
**Refresh:** Click to refresh the page immediately.

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

## **RMON Alarm Overview**

This page provides an overview of RMON alarm entries.

The displayed fields are:



## 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, possible sample types are:

### Rising Threshold

Rising threshold value.

### Rising Index

Rising event index.

### Falling Threshold

Falling threshold value.

### Falling Index

Falling event index.

## Buttons

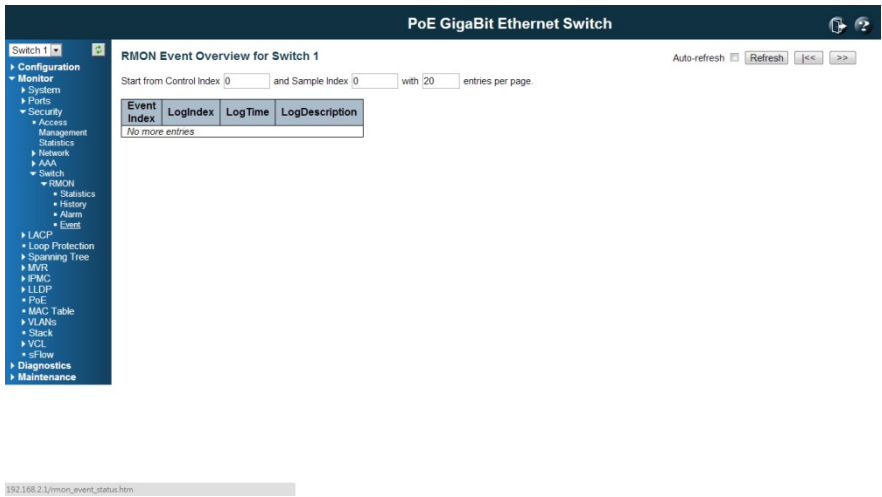
**Refresh:** Click to refresh the page immediately.

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

# RMON Event Overview

This page provides an overview of RMON event entries.

The displayed fields are:



## Event Index

Indicates the index of the event entry.

## Log Index

Indicates the index of the log entry.

## Log Time

Indicates Event log time

## Log Description

Indicates the Event description.

## Buttons

**Refresh:** Click to refresh the page immediately.

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

## 6.1.4 LACP System Status

### 6.1.4.1 System Status

This page provides a status overview for all LACP instances.

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

#### 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.

#### Last changed

The time since this aggregation changed.

#### Local Ports

Shows which ports are a part of this aggregation for this switch.

#### Buttons

**Refresh:** Click to refresh the page immediately.

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



### 6.1.4.2 LACP Port Status

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

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	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-
13	No	-	-	-	-	-
14	No	-	-	-	-	-
15	No	-	-	-	-	-
16	No	-	-	-	-	-
17	No	-	-	-	-	-
18	No	-	-	-	-	-
19	No	-	-	-	-	-
20	No	-	-	-	-	-
21	No	-	-	-	-	-
22	No	-	-	-	-	-
23	No	-	-	-	-	-
24	No	-	-	-	-	-
25	No	-	-	-	-	-
26	No	-	-	-	-	-

#### 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.

#### Buttons

**Refresh:** Click to refresh the page immediately.

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

### 6.1.4.3 LACP statistics

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

PoE GigaBit Ethernet Switch

Switch 1

LACP Statistics for Switch 1

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
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0

592 166.2.1/lacp\_statistics.htm

#### 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:** Click this box to enable an automatic refresh of the page at regular intervals.

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears the counters for all ports.

### 6.1.5 Loop Protection

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

Loop protection port status is:

#### 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

**Refresh:** Click to refresh the page immediately.

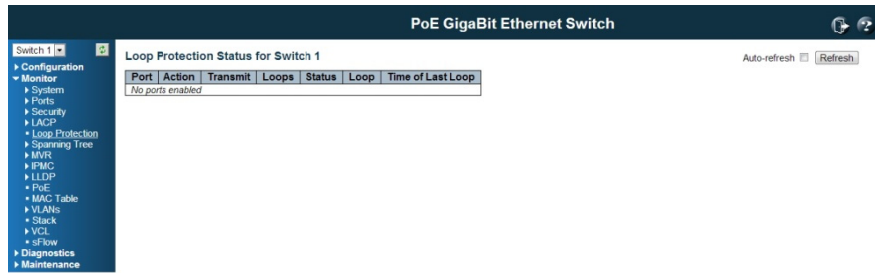
**Auto-refresh** ☐ : Check this box to enable an automatic refresh of the page at regular intervals.

### 6.1.6 STP Bridge Status

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

#### 6.1.6.1 Bridge Status

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



192.168.2.1/loop\_status.htm

## 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 Change Last

The time since last Topology Change occurred.

## Buttons

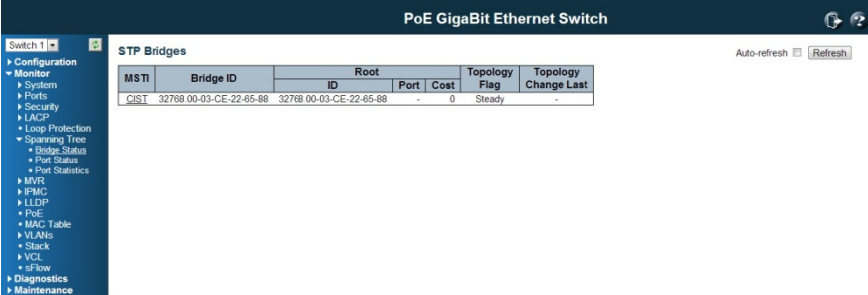
**Refresh:** Click to refresh the page immediately.

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

### 6.1.6.2 STP Port Status

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

STP port status is:



The screenshot shows the 'STP Bridges' configuration page for a 'PoE GigaBit Ethernet Switch'. On the left is a navigation menu with options like Configuration, Monitor, System, Ports, Security, LACP, Loop Protection, Spanning Tree, Bridge Status, Port Status, Port Statistics, MVR, IPAC, LLDP, PoE, MAC Table, VLANs, Stack, VCL, xFlow, Diagnostics, and Maintenance. The main area displays a table of STP Bridges. The table has columns for MSTI, Bridge ID, Root ID, Port, Cost, Topology Flag, and Topology Change Last. A single row is shown for MSTI CIST, Bridge ID 32768.00-03-CE-22-65-88, Root ID 32768.00-03-CE-22-65-88, Port -, Cost 0, Topology Flag Steady, and Topology Change Last -. Above the table is an 'Auto-refresh' checkbox and a 'Refresh' button. Below the table is a small text link: 192.168.2.1/mstp\_status\_bridges.htm.

MSTI	Bridge ID	Root ID	Port	Cost	Topology Flag	Topology Change Last
CIST	32768.00-03-CE-22-65-88	32768.00-03-CE-22-65-88	-	0	Steady	-

#### 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

**Refresh:** Click to refresh the page immediately.

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

### 6.1.6.3 STP Port Statistics

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

The STP port statistics counters are:

Port	CIST Role	CIST State	Uptime
1.1	Disabled	Discarding	-
1.2	DesignatedPort	Forwarding	0d 00:29:38
1.3	Disabled	Discarding	-
1.4	Disabled	Discarding	-
1.5	Disabled	Discarding	-
1.6	Disabled	Discarding	-
1.7	Disabled	Discarding	-
1.8	Disabled	Discarding	-
1.9	Disabled	Discarding	-
1.10	Disabled	Discarding	-
1.11	Disabled	Discarding	-
1.12	Disabled	Discarding	-
1.13	Disabled	Discarding	-
1.14	Disabled	Discarding	-
1.15	Disabled	Discarding	-
1.16	Disabled	Discarding	-
1.17	Disabled	Discarding	-
1.18	Disabled	Discarding	-
1.19	Disabled	Discarding	-
1.20	Disabled	Discarding	-
1.21	Disabled	Discarding	-
1.22	Disabled	Discarding	-
1.23	Disabled	Discarding	-
1.24	Disabled	Discarding	-
1.25	Disabled	Discarding	-
1.26	Disabled	Discarding	-

192.168.2.1/mstp\_status\_ports.htm

#### Port

The switch port number of the logical STP port.

#### MSTP

The number of MSTP Configuration BPDU's received/transmitted on the port.

#### RSTP

The number of RSTP Configuration 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

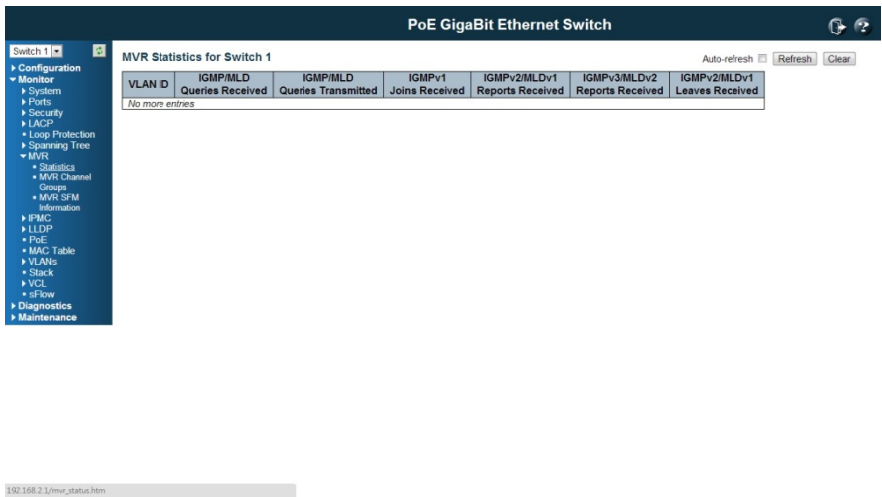
**Refresh**:: Click to refresh the page immediately.

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

6.1.7 MVR Status

6.1.7.1 Statistics

This page provides MVR Statistics information.



VLAN ID

The Multicast VLAN ID.

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.

### Buttons

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears all Statistics counters.

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

### 6.1.7.2 MVR Group Table

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

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- Monitor
  - System
  - Ports
  - Security
    - LLDP
    - Loop Protection
    - Spanning Tree
  - MVR
    - Statistics
    - MVR Channel
      - Groups
      - MVR SFM Information
  - IPMC
  - LLDP
  - PoE
  - MAC Table
  - VLANs
  - Stack
  - VCL
  - sFlow
- Diagnostics
- Maintenance

MVR Channels (Groups) Information for Switch 1

Auto-refresh ☐ Refresh << >>

Start from VLAN 1 and Group Address with 20 entries per page.

VLAN ID	Groups	Port Members
No more entries		

192.168.2.1/mvr\_groups\_info.htm

### Navigating the MVR Group Table

Each page shows up to 99 entries from the MVR Group 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 MVR Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MVR Group Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MVR Group Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

## MVR Group Table Columns

### VLAN ID

VLAN ID of the group.

### Groups

Group ID of the group displayed.

### Port Members

Ports under this group.

## Buttons

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

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

**|<<**: Updates the table starting from the first entry in the MVR Group Table.

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

## 6.1.8 Monitor / IPMC / IGMP Snooping

### 6.1.8.1 IGMP Snooping

## IGMP Snooping Status

This page provides IGMP Snooping status.

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-	-
16	-	-	-	-	-	-	-	-	-
17	-	-	-	-	-	-	-	-	-
18	-	-	-	-	-	-	-	-	-
19	-	-	-	-	-	-	-	-	-
20	-	-	-	-	-	-	-	-	-
21	-	-	-	-	-	-	-	-	-
22	-	-	-	-	-	-	-	-	-
23	-	-	-	-	-	-	-	-	-
24	-	-	-	-	-	-	-	-	-
25	-	-	-	-	-	-	-	-	-
26	-	-	-	-	-	-	-	-	-

### 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 denotes the specific port is configured and learnt to be a router port.

### Buttons

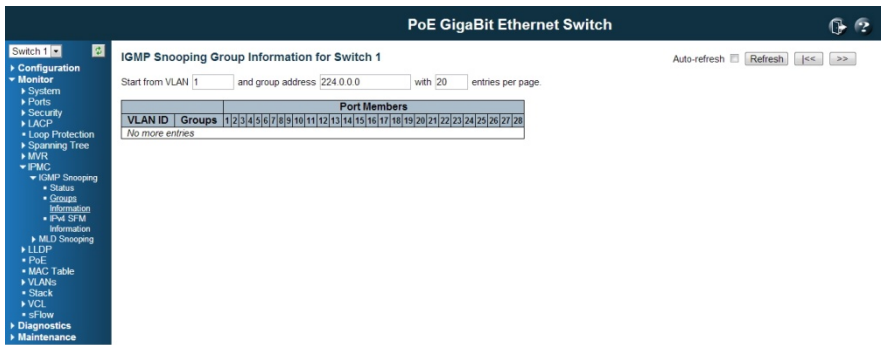
**Refresh:** Click to refresh the page immediately.

**Clear:** Clears all Statistics counters.

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

# IGMP Group 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.



192.168.2.1/gmrc\_igmp\_groups\_info.htm

## Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group 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 IGMP Group Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

## IGMP Group Table Columns

### VLAN ID

VLAN ID of the group.

### Groups

Group address of the group displayed.

### Port Members

Ports under this group.

## Buttons

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

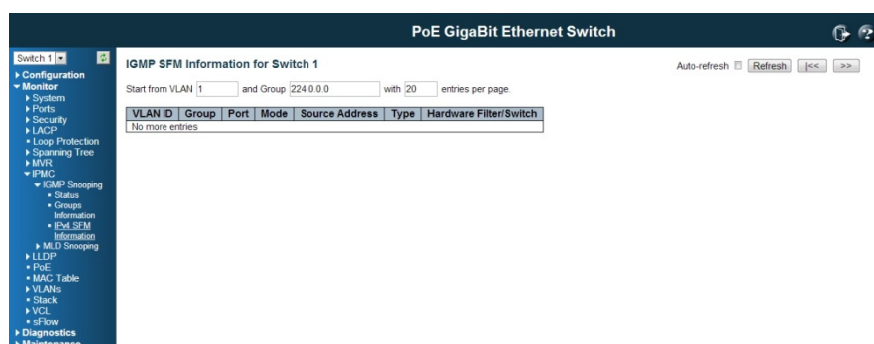
**Refresh**: Refreshes the displayed table starting from the input fields.

**<<**: 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.

## IGMP SFM Information Table

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses belong to the same group are treated as single entry.



192.168.2.1/igmp\_igmpsfm\_info.htm

## Navigating the IGMP SFM Information Table

Each page shows up to 99 entries from the IGMP SFM Information 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 IGMP SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start

address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

### IGMP SFM Information Table Columns

#### VLAN ID

VLAN ID of the group.

#### Group

Group address of the group displayed.

#### Port

Switch port number.

#### Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

#### Source Address

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

#### Type

Indicates the Type. It can be either Allow or Deny.

### Buttons

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

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

|<<: Updates the table starting from the first entry in the IGMP SFM Information Table.

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

### 6.1.8.2 MLD Snooping Status

This page provides MLD Snooping status.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

Monitor

System

Ports

Security

LACP

Loop Protection

Spanning Tree

MVR

PMF

IGMP Snooping

MLD Snooping

Status

Groups

Information

IPv6 SPM

Information

LLDP

PVE

MAC Table

VLANs

Stack

VCL

sFlow

Diagnostics

Maintenance

MLD Snooping Status for Switch 1

Auto-refresh ☐ Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
1	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-
16	-	-	-	-	-	-	-	-
17	-	-	-	-	-	-	-	-
18	-	-	-	-	-	-	-	-
19	-	-	-	-	-	-	-	-
20	-	-	-	-	-	-	-	-
21	-	-	-	-	-	-	-	-
22	-	-	-	-	-	-	-	-
23	-	-	-	-	-	-	-	-
24	-	-	-	-	-	-	-	-
25	-	-	-	-	-	-	-	-
26	-	-	-	-	-	-	-	-

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-
25	-
26	-

192.168.2.1/pmc\_mldonp\_status.htm

## VLAN ID

The VLAN ID of the entry.

## Querier Version

Working Querier Version currently.

## Host Version

Working Host Version currently.

## Querier Status

Show 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 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 denotes the specific port is configured and learnt to be a router port.

## Buttons

**Refresh:** Click to refresh the page immediately.

**Clear:** Clears all Statistics counters.

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

## MLD Group Table

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.

PoE GigaBit Ethernet Switch

Switch 1

Configuration

- Monitor
- System
- Ports
- Security
- LAGP
- Loop Protection
- Spanning Tree
- MVR
- IPMFC
- IGMP Snooping
- MLD Snooping
  - Status
  - Groups
  - Information
  - IPv6 SPM
  - Information
- LLDP
- PoE
- MAC Table
- VLANs
- Stack
- VCL
- sFlow
- Diagnostics
- Maintenance

MLD Snooping Group Information for Switch 1

Auto-refresh ☐ Refresh << >>

Start from VLAN 1 and group address #00: with 20 entries per page.

VLAN ID	Groups	Port Members																									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

No more entries

192.168.2.1/gmc\_mldoop\_groups\_info.htm

## Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group 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 MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest MLD Group Table match. In addition, the



two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

## Buttons

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

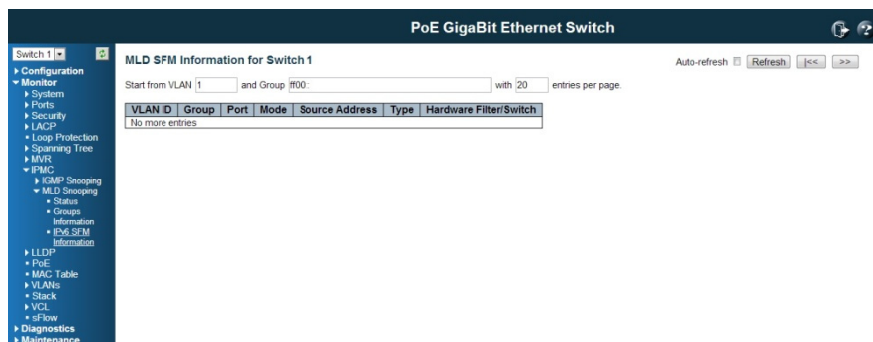
**Refresh:** Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the MLD Group Table.

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

## MLD SFM Information Table

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses belong to the same group are treated as single entry.



190.168.2.1/gmc\_mldsm\_v2info.htm

## Navigating the MLD SFM Information Table

Each page shows up to 64 entries from the MLD SFM Information 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 MLD SFM Information

Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next MLD SFM Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

When the end is reached the text "No more entries" is shown in the displayed table.

Use the button to start over.

### MLD SFM Information Table Columns

#### VLAN ID

VLAN ID of the group.

#### Group

Group address of the group displayed.

#### Port

Switch port number.

#### Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

#### Source Address

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

#### Type

Indicates the Type. It can be either Allow or Deny.

### Buttons

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

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

|<<: Updates the table starting from the first entry in the MLD SFP Information Table.

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

## 6.1.9 Monitor / LLDP

### 6.1.9.1 LLDP / Neighbor

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:

Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbour information found						

192.168.2.1/ldp\_neighbours.htm

#### 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.

#### Remote Port ID

The **Remote Port ID** is the identification of the neighbour port.

#### System Name

**System Name** is the name advertised by the neighbour unit.

#### Port Description

**Port Description** is the port description 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. WAN 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.

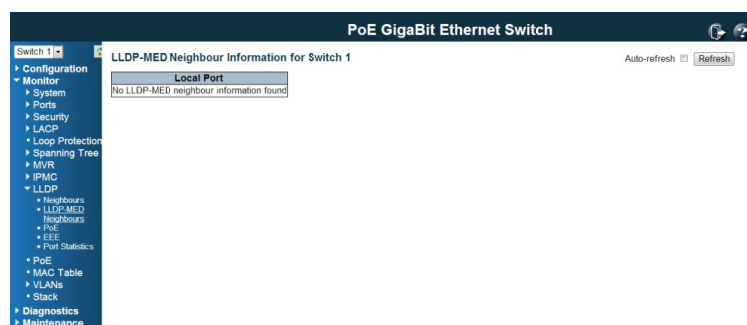
## Buttons

**Refresh:** Click to refresh the page immediately.

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

### 6.1.9.2 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:



192.168.2.1/ldp\_neighbours\_med.htm

## 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 Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch / Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater ( included for historical reasons )
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

### LLDP-MED Endpoint Device Definition

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

### **LLDP-MED Generic Endpoint (Class I)**

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

### **LLDP-MED Media Endpoint (Class II)**

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

### **LLDP-MED Communication Endpoint (Class III)**

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

### **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 Signaling - for use in network topologies that require a different policy for the voice signaling 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 Signaling - for use in network topologies that require a different policy for the guest voice signaling 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 Signaling - for use in network topologies that require a separate policy for the video signaling 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).



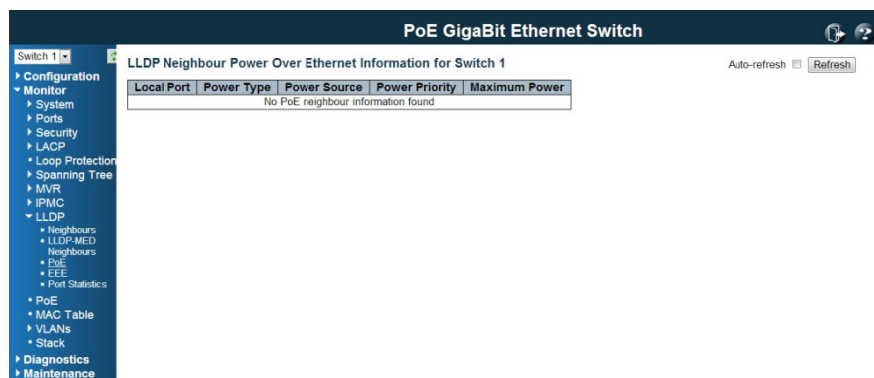
## Buttons

**Refresh:** Click to refresh the page immediately.

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

### 6.1.9.3 LLDP EEE

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wake up time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wake up time ", as a way to agree upon the minimum wake up time they need. This page provides an overview of EEE information exchanged by LLDP.



Local Port	Power Type	Power Source	Power Priority	Maximum Power
No PoE neighbour information found				

192.168.2.1/ldp\_poe\_neighbors.htm

### LLDP Neighbors EEE Information

The displayed table contains a row for each port. The columns hold the following information:

#### 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 desertion 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 activated**

Show if the switch and the link partner have agree upon which wakeup times to use.

Red - Switch and link partner have not agreed upon wakeup time.

Green - Switch and link partner have agreed upon wakeup time.

## Buttons

**Refresh:** Click to refresh the page immediately.

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

### 6.1.9.4 LLDP 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.

PoE GigaBit Ethernet Switch

Switch 1

LLDP Global Counters for Switch 1

Auto-refresh ☐ Refresh Clear

Global Counters				
Neighbour entries were last changed 1970-01-01T00:00:00+00:00 (100 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 for Switch 1

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	4	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
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0

## Global Counters

### Neighbour entries were last changed on

It also 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 Counters**

The displayed table contains a row for each port. The columns hold the following information:

### **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.

### Org. 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

**Refresh:** Click to refresh the page immediately.

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

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

## 6.1.10 Dynamic MAC Table

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.

### Navigating the MAC Table

Each page shows up to 999 entries from the MAC 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 MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table. The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Switch 1

Configuration

Monitor

System

Ports

Security

LACP

Loop Protection

Spanning Tree

MVR

IPMG

LLDP

PoE

MAC Table

VLANs

Stack

VCL

sFlow

Diagnostics

Maintenance

PoE GigaBit Ethernet Switch

Auto-refresh

Refresh

Clear

<<

>>

MAC Address Table for Switch 1

Start from VLAN

1

and MAC address

00-00-00-00-00-00

with

20

entries per page.

Switch	Type	VLAN	MAC Address	CPU	Port Members																											
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	Static	1	00-03-CE-22-65-88	✓																												
1	Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
1	Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
1	Static	1	33-33-FF-22-65-88	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
1	Dynamic	1	54-53-ED-2F-20-CE	✓																												
1	Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		

## MAC Table Columns

### Switch (stack only)

The stack unit where the entry is learned.

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

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

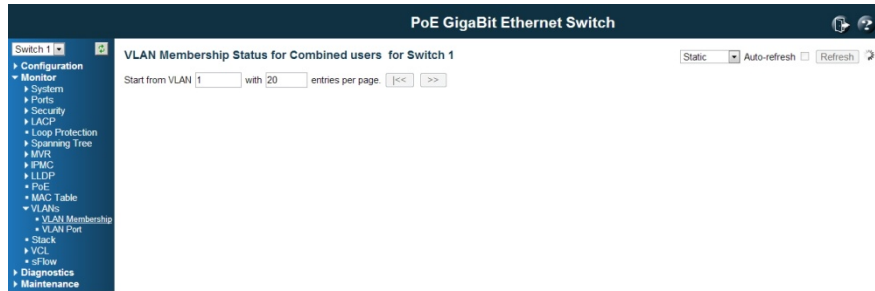
**Clear:** Flushes all dynamic entries.

**<<:** 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.

### 6.1.11 VLAN Membership Status

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



192.168.2.1/vlan\_membership\_stat.htm

#### VLAN USER

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:

**CLI/Web/SNMP:** These are referred to as static.

**NAS:** NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

**MVRP:** Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.


**Voice VLAN:** Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

**MVR:** MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.


**MSTP:** The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

## 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.

If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as .

## VLAN Membership

The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

### Navigating the VLAN Monitor page

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.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

### Navigating the VLAN Monitor page

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.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the closest next VLAN Table match. The will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.



## Buttons

: Select VLAN Users from this drop down list.

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

**Refresh:** Click to refresh the page immediately.

## VLAN Port Status

This page provides VLAN Port Status.

GigaBit Ethernet Switch

Switch 2

VLAN Port Status for Static user for Switch 2

Static ☒ Auto-refresh ☐ Refresh

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	Unkware	Disabled	All	Untag_this	1	No
2	1	Unkware	Disabled	All	Untag_this	1	No
3	1	Unkware	Disabled	All	Untag_this	1	No
4	1	Unkware	Disabled	All	Untag_this	1	No
5	1	Unkware	Disabled	All	Untag_this	1	No
6	1	Unkware	Disabled	All	Untag_this	1	No
7	1	Unkware	Disabled	All	Untag_this	1	No
8	1	Unkware	Disabled	All	Untag_this	1	No
9	1	Unkware	Disabled	All	Untag_this	1	No
10	1	Unkware	Disabled	All	Untag_this	1	No
11	1	Unkware	Disabled	All	Untag_this	1	No
12	1	Unkware	Disabled	All	Untag_this	1	No
13	1	Unkware	Disabled	All	Untag_this	1	No
14	1	Unkware	Disabled	All	Untag_this	1	No
15	1	Unkware	Disabled	All	Untag_this	1	No
16	1	Unkware	Disabled	All	Untag_this	1	No
17	1	Unkware	Disabled	All	Untag_this	1	No
18	1	Unkware	Disabled	All	Untag_this	1	No
19	1	Unkware	Disabled	All	Untag_this	1	No
20	1	Unkware	Disabled	All	Untag_this	1	No
21	1	Unkware	Disabled	All	Untag_this	1	No
22	1	Unkware	Disabled	All	Untag_this	1	No
23	1	Unkware	Disabled	All	Untag_this	1	No
24	1	Unkware	Disabled	All	Untag_this	1	No
25	1	Unkware	Disabled	All	Untag_this	1	No
26	1	Unkware	Disabled	All	Untag_this	1	No

## VLAN USER

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN User types:

**CLI/Web/SNMP:** These are referred to as static.

**NAS:** NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

**MVRP:** Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

**Voice VLAN:** Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

**MVR:** MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

**MSTP:** The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

#### 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 frames 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 behavior 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

: Select VLAN Users from this drop down list.

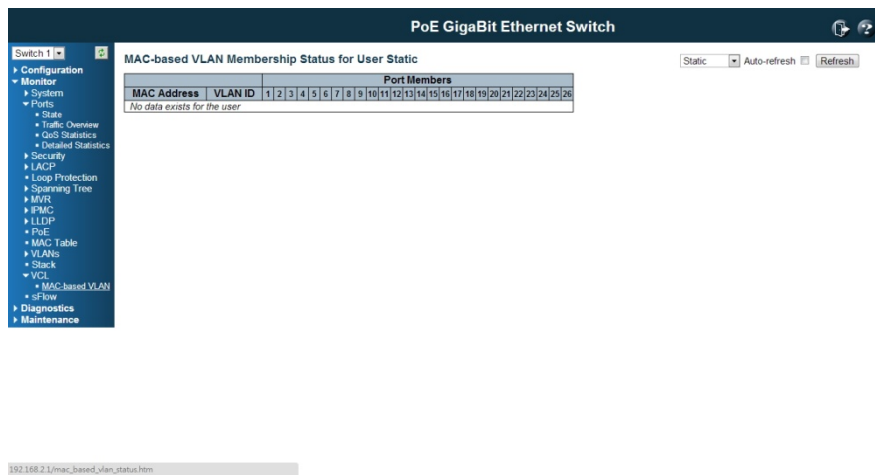
**Auto-refresh** ☐ : Check this box to enable an automatic refresh of the page at regular intervals.

**Refresh:** Click to refresh the page immediately.

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
11	1	UnAware	Disabled	All	Untag_this	1	No
12	1	UnAware	Disabled	All	Untag_this	1	No
13	1	UnAware	Disabled	All	Untag_this	1	No
14	1	UnAware	Disabled	All	Untag_this	1	No
15	1	UnAware	Disabled	All	Untag_this	1	No
16	1	UnAware	Disabled	All	Untag_this	1	No
17	1	UnAware	Disabled	All	Untag_this	1	No
18	1	UnAware	Disabled	All	Untag_this	1	No
19	1	UnAware	Disabled	All	Untag_this	1	No
20	1	UnAware	Disabled	All	Untag_this	1	No
21	1	UnAware	Disabled	All	Untag_this	1	No
22	1	UnAware	Disabled	All	Untag_this	1	No
23	1	UnAware	Disabled	All	Untag_this	1	No
24	1	UnAware	Disabled	All	Untag_this	1	No
25	1	UnAware	Disabled	All	Untag_this	1	No
26	1	UnAware	Disabled	All	Untag_this	1	No

### 6.1.13 VCL MAC-Based VLAN Status

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:



**CLI/Web/SNMP:** These are referred to as static.

**NAS:** NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

## MAC Address

Indicates the MAC address.

## VLAN ID

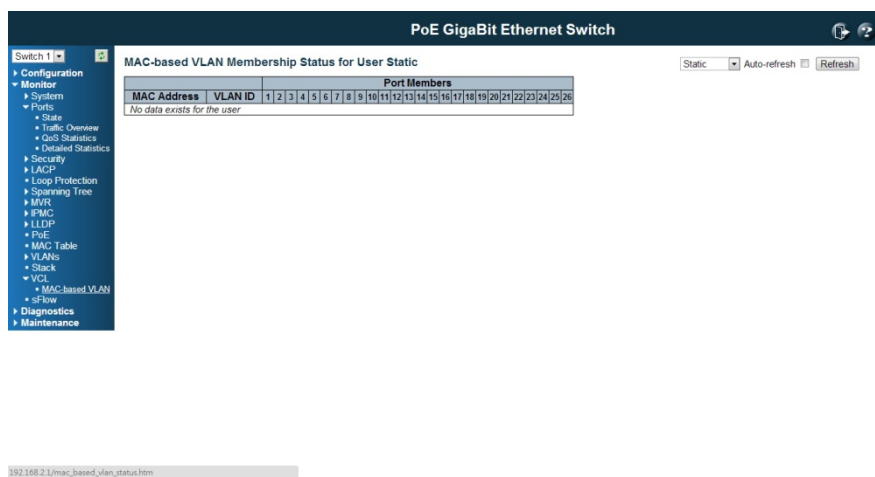
Indicates the VLAN ID.

## Port Members

Port members of the MAC-based VLAN entry.

## Buttons

**Refresh:** Refreshes the displayed table.



### 6.1.14 sFlow

This page shows the sFlow Statistics.

#### Flow Sampling

Packet flow sampling refers to arbitrarily choosing some packets out of a specified number, reading the first "Max Hdr Size" bytes and exporting the sampled datagram for analysis.

The attributes associated with the flow sampling are: sampler type, sampling rate, maximum header size.

#### Counter Sampling

Counter sampling performs periodic, time-based sampling or polling of counters associated with an interface enabled for sFlow.

Attribute associated with counter sampling is polling interval.

#### sFlow Ports

List of the port numbers on which sFlow is configured.

#### Sampler Type

Configured sampler type on the port and could be any of the types: None, RX, TX, ALL.

## 6.2 Diagnostic

This section provides some convenient tool for user to do switch diagnostic from remote site.

### 6.2.1 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

Type the IP Address, ping length (default = 56 bytes), ping count (default=5) and ping interval (default =1). Then press "**Start**" to start ping remote host. After you press **Start**, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

#### ICMP Ping Output Result

PING server 192.168.2.100, 56 bytes of data.

64 bytes from 192.168.2.100: icmp\_seq=0, time=0ms

64 bytes from 192.168.2.100: icmp\_seq=1, time=0ms

64 bytes from 192.168.2.100: icmp\_seq=2, time=0ms

64 bytes from 192.168.2.100: icmp\_seq=3, time=0ms

64 bytes from 192.168.2.100: icmp\_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

#### 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 0 second to 30 seconds.

### 6.2.2 Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Type the IPv6 Address, ping length (default = 56 bytes), ping count (default=5) and ping interval (default =1). Then press "**Start**" to start ping remote host. After you press **Start**, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip 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 Output

```
PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

You can configure the following properties of the issued ICMP packets:

#### 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

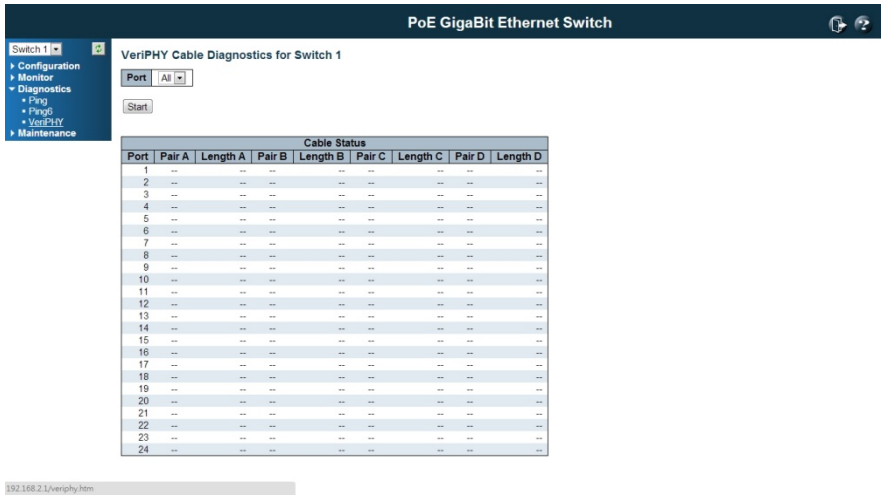
The interval of the ICMP packet. Values range from 0 second to 30 seconds.

### 6.2.3 VeriPHY Cable Diagnostic

This page is used for running the VeriPHY Cable Diagnostics.

Select the port and then press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.



## Port

The port where you are requesting VeriPHY Cable Diagnostics.

## Cable Status

**Port:** Port number.

**Pair:** The status of the cable 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.



## 6.3 Maintenance

The section allows user to maintain the switch, such as Reset Factory Default, Firmware upgrading, Configuration Save/Restore and Restart the device.

### 6.3.1 Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.

#### Restart Device

Are you sure you want to perform a Restart?

**Yes:** Click to restart device.

**No:** Click to return to the Port State page without restarting.

### 6.3.2 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.

#### Factory Defaults

Are you sure you want to reset the configuration to  
Factory Defaults?

**Yes:** Click to reset the configuration to Factory Defaults.

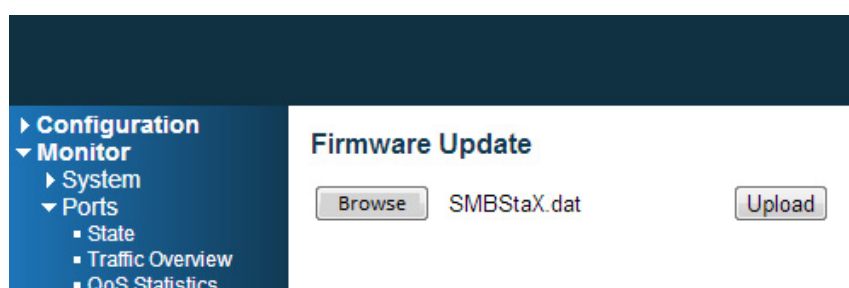
**No:** Click to return to the Port State page without resetting the configuration.

**Note:** Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default.

### 6.3.3 Software Upload

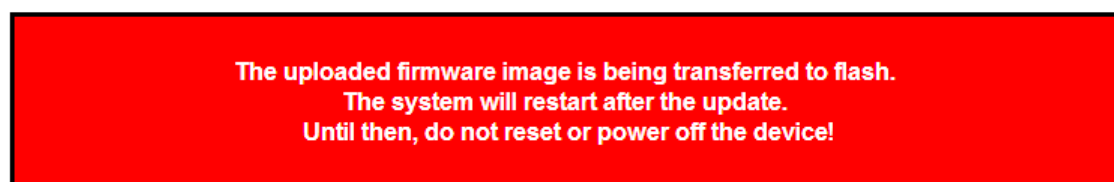
#### 6.3.3.1 Firmware Update

This page facilitates an update of the firmware controlling the switch.



"**Browse**" to the location of a software image, you can see the file name in the right of the Browse command. Click "**Upload**" to start the process.

#### Firmware update in progress



Waiting, please stand by...

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

### 6.3.3.2 Image Select

There are 2 image saved within the switch.

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.

#### Software Image Selection

Active Image	
Image	managed
Version	PoE (standalone) dev-build by root@virtual-centos 2012-07-01T15:54:24+08:00
Date	2012-07-01T15:54:24+08:00

Alternate Image	
Image	managed.bk
Version	SMBStaX (standalone) dev-build by uwai@Uwai-Fedora 2012-11-06T16:35:36+08:00 Config:config.mk
Date	2012-11-06T16:35:36+08:00

#### 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.

#### Image Information

<b>Image</b>
The flash index name of the firmware image. The name of primary (preferred) image is <code>image</code> , the alternate image is named <code>image.bk</code> .
<b>Version</b>
The version of the firmware image.
<b>Date</b>
The date where the firmware was produced.

## Buttons

**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.

### 6.3.4 Configuration

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:

Header tags: `<?xml version="1.0"?>` and `<configuration>`. These tags are mandatory and must be present at the beginning of the file.

Section tags: `<platform>`, `<global>` and `<switch>`. The platform section must be the first section tag and this section must include the correct platform ID and version. The global section is optional and includes configuration which is not related to specific switch ports. The switch section is optional and includes configuration which is related to specific switch ports.

Module tags: `<ip>`, `<mac>`, `<port>` etc. These tags identify a module controlling specific parts of the configuration.

Group tags: `<port table>`, `<vlan table>` etc. These tags identify a group of parameters, typically a table.

Parameter tags: `<mode>`, `<entry>` etc. These tags identify parameters for the specific section, module and group. The `<entry>` tag is used for table entries.

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

The example below shows a small configuration file only including configuration of the MAC address age time and the learning mode per port. When loading this file, only the included parameters will be changed. This means that the age time will be set to 200 and the learn mode will be set to automatic.

```
< ?xml version="1.0"?>
<configuration>
<platform>
<pid val="3"></pid>
<version val="1"></version>
</platform>
<global>
```

```
<mac>  
<age val="200"></age>>  
</mac>  
</global>  
<switch sid="1">  
<mac>  
<entry port="1-24" learn mode="auto"></entry>  
</mac>  
</switch>  
< /configuration>
```

**Save:** Click to save the configuration file.

**Upload:** Click to upload the configuration file.



## **Safety Warnings**

For your safety, be sure to read and follow all warning notices and instructions.

- Do not open the device. Opening or removing the device cover can expose you to dangerous high voltage points or other risks. Only qualified service personnel can service the device. Please contact your vendor for further information.
- Do not use your device during a thunderstorm. There may be a risk of electric shock brought about by lightning.
- Do not expose your device to dust or corrosive liquids.
- Do not use this product near water sources.
- Make sure to connect the cables to the correct ports.
- Do not obstruct the ventilation slots on the device.



## CE-Declaration of Conformity

For the following equipment:

Germering, 31st of October, 2014

### **24-Port 10/100/1000Base-T + 2-Port 10G SFP ALL-SG8826MX-10G**



The safety advice in the documentation accompanying the products shall be obeyed. The conformity to the above directive is indicated by the CE sign on the device.

The Allnet ALL-SG8826MX-10G conforms to the Council Directives of 2004/108/EC.

This equipment meets the following conformance standards:

*EN55022:2010: Class A*

*IEC61000-3-2:2005+A1:2008+A2:2009*

*IEC61000-3-3:2008*

*EN55024:2010*

*IEC61000-4-2:2008*

*IEC61000-4-3:2006+A1:2007+A2:2010*

*IEC61000-4-4:2004+A1:2010 IEC61000-4-5:2005*

*IEC61000-4-6:2008*

*IEC61000-4-8:2009*

*IEC61000-4-11:2004*

This equipment is intended to be operated in all countries.

This declaration is made by

ALLNET GmbH Computersysteme  
Maistraße 2  
82110 Germering  
Germany

Germering, 31.10.2014

  
\_\_\_\_\_  
Wolfgang Marcus Bauer  
CEO

### **DISCLAIMER\_OF\_WARRANTY**

This Program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2 of the License.

This Program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this Program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

The full text of the GNU General Public License version 2 is included with the software distribution in the file LICENSE.GPLv2

### **NO WARRANTY**

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

### **Written Offer for Source Code**

For binaries that you receive from ALLNET GmbH Computersysteme on physical media or within the download of the offered firmware that are licensed under any version of the GNU General Public License (GPL) or the GNU LGPL, you can receive a complete machine-readable copy of the source code by sending a written request to:

ALLNET GmbH Computersysteme  
Maistrasse 2  
82110 Germering

Your request should include: (i) the name of the covered binary, (ii) the version number of the ALLNET product containing the covered binary, (iii) your name, (iv) your company name (if applicable) and (v) your return mailing and email address (if available). We may charge you a nominal fee to cover the cost of the media and distribution. Your request must be sent within three (3) years of the date you received the GPL or LGPL covered code. For your



convenience, some or all of the source code may also be found at:

<http://www.allnet.de/gpl.html>

## **LICENSE.GPLv2**

### **GNU GENERAL PUBLIC LICENSE**

#### **Version 2, June 1991**

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

#### **Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too. When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

## GNU GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them

as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
  - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
  - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
  - c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and

conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### **NO WARRANTY**

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### **END OF TERMS AND CONDITIONS**

##### **How to Apply These Terms to Your New Programs**

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA  
Also add information on how to contact you by electronic and paper mail. If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

#### **LICENSE.LGPLv2.1**

#### **GNU LESSER GENERAL PUBLIC LICENSE**

#### **Version 2.1, February 1999**

Copyright (C) 1991, 1999 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA

02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document,

but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

### **Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below. When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different

from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom.

The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

## **GNU LESSER GENERAL PUBLIC LICENSE**

### **TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION**

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications



and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees

extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License. However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them

and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
  - a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
  - b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on

consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.  
  
Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### **NO WARRANTY**

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN

IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## **END OF TERMS AND CONDITIONS**

### **How to Apply These Terms to Your New Libraries**

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library 'Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990 Ty Coon, President of Vice

That's all there is to it!