

# User Manual



## **GSW-2008MS**

**Managed Gigabit Ethernet CPE Switch**



**CTC UNION TECHNOLOGIES CO., LTD.**

## **LEGAL**

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

## **TRADEMARKS**

Microsoft is a registered trademark of Microsoft Corp.

HyperTerminal™ is a registered trademark of Hilgraeve Inc.

ActiPHY™ and VeriReach™ are registered trademarks of Vitesse® Semiconductor

## **Federal Communications Commission (FCC) NOTICE**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of 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 and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. 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.

This unit was tested with shielded cables on the peripheral devices. Shielded cables must be used with the unit to insure compliance. This statement can be deleted if unit was not tested with shielded cables.

The manufacture is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference that may cause undesired operation.

Change or modifications that are not expressly approved by the manufacturer could void the user's authority to operate the equipment.

## **CISPR PUB.22 Class B COMPLIANCE:**

This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class B.

## **WARNING:**

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

## **CE NOTICE**

Marking by the symbol CE indicates compliance of this equipment to the EMC directive of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:2006+A1:2007, Class A, EN55024:2010.

**CTC Union Technologies Co., Ltd.**

Far Eastern Vienna Technology Center (Neihu Technology Park)  
8F, No. 60, Zhouzi St.  
Neihu, Taipei, 114  
Taiwan  
Phone: +886-2-2659-1021  
FAX: +886-2-2799-1355

**GSW-2008MS**

Managed Gigabit Ethernet CPE Switch

User Manual

Version 1.0 July 2014

This manual supports the following models:

GSW-2008MS Managed Gigabit Ethernet 8TP+2FX CPE Switch

This document is the current official release manual. Please check CTC Union's website for any updated manual or contact us by E-mail at [sales@ctcu.com](mailto:sales@ctcu.com). Please address any comments for improving this manual or to point out omissions or errors to [marketing@ctcu.com](mailto:marketing@ctcu.com). Thank you.

<b>CHAPTER 1. INTRODUCTION .....</b>	<b>8</b>
1.1 WELCOME.....	8
1.2 PRODUCT DESCRIPTION .....	8
1.3 PRODUCT FEATURES .....	8
1.4 PRODUCT SPECIFICATIONS .....	9
<b>CHAPTER 2. PANELS &amp; LED INDICATORS.....</b>	<b>10</b>
2.1 FRONT PANEL .....	10
2.2 REAR PANEL .....	10
2.2.1 Fiber Connections .....	11
2.2.2 Reset Push-Button.....	11
2.2.3 Power .....	11
2.3 LED INDICATORS .....	11
<b>CHAPTER 3. INSTALLATION .....</b>	<b>12</b>
3.1 INTRODUCTION .....	12
3.1.1 Wall-Mounting (GSW-2008MS).....	12
3.1.2 Cable Tray Installation.....	13
3.1.3 Wall-Mounting (GSW-2008MS with Cable Tray).....	15
<b>CHAPTER 4. INTRODUCTION TO CLI.....</b>	<b>17</b>
4.1 INTRODUCTION .....	17
4.2 TELNET OPERATION .....	17
4.2.1 CLI Online Help.....	18
4.2.2 TCP/IP Configuration via CLI.....	18
4.2.2.1 IP Address, Subnet Mask, Default Router .....	18
4.2.2.2 DHCP .....	19
4.2.2.3 DNS Server .....	19
4.2.2.4 Display TCP/IP Settings.....	19
4.2.3 Factory Default.....	19
4.2.4 Reboot Device .....	20
4.2.5 Admin Password.....	20
4.2.6 Logout .....	20
<b>CHAPTER 5. WEB CONFIGURATION &amp; OPERATION.....</b>	<b>21</b>
5.1 HOME PAGE .....	21
5.1.1 Login.....	21
5.1.2 Port Status.....	21
5.1.3 Refresh .....	22
5.1.4 Help System.....	22
5.1.5 Logout .....	22
5.2 SYSTEM.....	22
5.2.1 System Configuration .....	23
5.2.2 System Information.....	23
5.2.3 System IP .....	23
5.2.4 System IPv6 .....	24
5.2.5 System Auto Provision Configuration .....	25
5.2.6 System NTP Configuration .....	25
5.2.7 System Time .....	26
5.2.8 System Log Configuration .....	27
5.2.9 System Log Information .....	27
5.2.10 System Detailed Log .....	28
5.2.11 System CPU Load.....	28
5.3 POWER REDUCTION (GREEN ETHERNET) .....	28
5.3.1 Green Ethernet LED.....	29
5.3.2 Green Ethernet Configuration.....	29
5.4 THERMAL PROTECTION.....	30
5.4.1 Configuration .....	30
5.4.2 Status .....	31

5.5 PORTS .....	31
5.5.1 Ports Configuration .....	31
5.5.2 Ports Auto Laser Shutdown .....	33
5.5.3 Ports State .....	33
5.5.4 Ports SFP .....	33
5.5.5 Ports Traffic Overview .....	34
5.5.6 Ports QoS Statistics .....	35
5.5.7 Ports QCL Status .....	35
5.5.8 Ports Detailed Statistics .....	36
5.6 SECURITY .....	37
5.6.1 Switch .....	37
5.6.1.1 Users .....	37
5.6.1.2 Privilege Levels .....	38
5.6.1.3 Auth Method .....	39
5.6.1.4 SSH .....	40
5.6.1.5 HTTPS .....	40
5.6.1.6 Access Management .....	41
5.6.1.6.1 Configuration .....	41
5.6.1.6.2 Access Management Statistics .....	42
5.6.1.7 SNMP .....	43
5.6.1.7.1 System Configuration .....	43
5.6.1.7.2 SNMPv3 Community Configuration .....	45
5.6.1.7.3 SNMPv3 User Configuration .....	45
5.6.1.7.4 SNMPv3 Group Configuration .....	47
5.6.1.7.5 SNMPv3 View Configuration .....	47
5.6.1.7.6 SNMPv3 Access Configuration .....	48
5.6.1.8 RMON .....	49
5.6.1.8.1 RMON Statistics Configuration .....	49
5.6.1.8.2 RMON History Configuration .....	49
5.6.1.8.3 RMON Alarm Configuration .....	50
5.6.1.8.4 RMON Event Configuration .....	51
5.6.1.8.5 RMON Statistics Overview .....	51
5.6.1.8.6 RMON History Overview .....	52
5.6.1.8.7 RMON Alarm Overview .....	53
5.6.1.8.8 RMON Event Overview .....	53
5.6.2 Network .....	54
5.6.2.1 Port Security .....	54
5.6.2.1.1 Limit Control .....	54
5.6.2.1.2 Switch Status .....	56
5.6.2.1.3 Port Status .....	57
5.6.2.2 NAS .....	57
5.6.2.2.1 Configuration .....	58
5.6.2.2.2 Switch Status .....	60
5.6.2.2.3 Port Statistics .....	61
5.6.2.3 ACL .....	62
5.6.2.3.1 Ports .....	62
5.6.2.3.2 Rate Limiters .....	63
5.6.2.3.3 Access Control List .....	63
5.6.2.3.4 ACL Status .....	67
5.6.2.4 DHCP .....	68
5.6.2.4.1 DHCP Snooping Configuration .....	68
5.6.2.4.2 DHCP Relay Configuration .....	68
5.6.2.4.3 DHCP Snooping Statistics .....	69
5.6.2.4.4 DHCP Relay Statistics .....	70
5.6.2.5 IP Source Guard .....	71
5.6.2.5.1 Configuration .....	71
5.6.2.5.2 Static Table .....	71
5.6.2.5.3 Dynamic Table .....	72
5.6.2.6 ARP Inspection .....	72
5.6.2.6.1 Configuration .....	72
5.6.2.6.2 Static Table .....	73

5.6.2.6.3 Dynamic Table .....	73
5.6.2.7 AAA.....	74
5.6.2.7.1 Configuration .....	74
5.6.2.7.2 RADIUS Overview.....	75
5.6.2.7.3 RADIUS Details.....	76
5.7 AGGREGATION .....	78
5.7.1 Static.....	78
5.7.2 LACP .....	79
5.7.2.1 Port Configuration.....	79
5.7.2.2 System Status.....	80
5.7.2.3 Port Status.....	80
5.6.2.4 Port Statistics .....	81
5.8 LOOP PROTECTION .....	81
5.8.1 Configuration .....	81
5.8.2 Status .....	82
5.9 SPANNING TREE .....	83
5.9.1 Bridge Settings .....	83
5.9.2 MSTI Mapping.....	85
5.9.3 MSTI Priorities.....	85
5.9.4 CIST Ports .....	86
5.9.5 MSTI Ports .....	87
5.9.6 Bridge Status .....	87
5.9.7 Port Status.....	89
5.9.8 Port Statistics .....	89
5.10 MVR.....	90
5.10.1 Configuration .....	90
5.10.2 Statistics .....	92
5.10.3 MVR Channel Groups .....	92
5.10.4 MVR SFM Information.....	93
5.11 IPMC.....	93
5.11.1 IGMP Snooping.....	93
5.11.1.1 Basic Configuration .....	94
5.11.1.2 VLAN Configuration.....	95
5.11.1.3 Port Group Filtering.....	96
5.11.1.4 Status .....	96
5.11.1.5 Groups Information.....	97
5.11.1.6 IPv4 SFM Information.....	97
5.11.2 MLD Snooping .....	98
5.11.2.1 Basic Configuration .....	98
5.11.2.2 VLAN Configuration.....	99
5.11.2.3 Port Group Filtering.....	100
5.11.2.4 Status .....	100
5.11.2.5 Groups Information.....	101
5.11.2.6 IPv6 SFM Information.....	101
5.12 LLDP.....	101
5.12.1 Configuration .....	102
5.12.2 LLDP-MED.....	103
5.12.3 Neighbours.....	105
5.12.4 LLDP-MED Neighbours .....	106
5.12.5 Neighbours EEE Information .....	106
5.12.6 Port Statistics .....	107
5.13 MAC TABLE .....	108
5.13.1 Configuration .....	108
5.13.2 MAC Address Table .....	109
5.14 VLAN TRANSLATION.....	109
5.14.1 Port to Group Mapping .....	109
5.14.2 VID Translation Mapping.....	110
5.15 VLANs .....	110
5.15.1 Membership Configuration .....	111
5.15.2 Ports Configuration .....	112
5.15.3 Membership Status .....	113

5.15.4 Port Status.....	113
5.16 PRIVATE VLANS.....	114
5.16.1 PVLAN Membership .....	114
5.16.2 Port Isolation.....	115
5.17 VCL .....	115
5.17.1 MAC-based.....	115
5.17.1.1 Membership Configuration .....	115
5.17.1.2 Membership Status .....	116
5.17.2 Protocol-based VLAN .....	116
5.17.2.1 Protocol to Group.....	116
5.17.2.2 Group to VLAN .....	117
5.17.3 IP Subnet-based VLAN.....	118
5.18 VOICE VLAN .....	118
5.18.1 Configuration .....	119
5.18.2 OUI .....	120
5.19 QoS.....	121
5.19.1 Port Classification.....	121
5.19.2 Port Policing .....	122
5.19.3 Port Scheduler.....	122
5.19.4 Port Shaping .....	124
5.19.5 Port Tag Remarking.....	124
5.19.6 Port DSCP .....	125
5.19.7 DSCP-Based QoS.....	126
5.19.8 DSCP Translation .....	127
5.19.9 DSCP Classification .....	127
5.19.10 QoS Control List.....	128
5.19.11 Storm Control.....	131
5.20 MIRRORING.....	131
5.21 UPNP.....	132
5.22 DIAGNOSTICS.....	132
5.22.1 Ping.....	132
5.22.2 Ping6.....	133
5.22.3 VeriPHY.....	133
5.23 MAINTENANCE.....	134
5.23.1 Restart Device .....	134
5.23.2 Factory Defaults .....	134
5.23.3 Software .....	135
5.23.3.1 Upload.....	135
5.23.3.2 Image Select .....	135
5.23.4 Configuration .....	135
5.23.4.1 Save .....	135
5.23.4.2 Upload.....	135
<b>APPENDIX A: ACRONYMS.....</b>	<b>136</b>

# Chapter 1. Introduction

## 1.1 Welcome

Welcome and thank you for purchasing this "world class" product from CTC Union. We hope this product is everything you wanted and more. Our Product Managers and R&D team have placed a "quality first" motto in our development of this series of Gigabit Ethernet switches with the desire of providing a highly stable and reliable product that will give years of trouble free operation.

In this chapter we will introduce this series, for Gigabit Ethernet applications. Chapter 2 will describe the panels and LED indicators. Chapter 3 shows the administrator how to mount the device on the wall and install optional cable tray management. All the models in this series utilize almost identical management interfaces, whether Telnet, SSH, HTTP (Web GUI) or SNMP (Simple Network Management Protocol). Chapter 4 will cover the basic operation using Telnet CLI. Chapter 5 will detail all of the configuration settings by using an easy to point and click Web interface which can be accessed from any available web browser.

## 1.2 Product Description

**GSW-2008MS** is a Managed Gigabit Ethernet CPE switch designed to make conversion between 8-Port 10/100/1000Base-T RJ-45 and 2 port 100/1000Base-X fiber optics with SFP optical modules. Traditionally, transmission distance of Gigabit Ethernet over fiber interface can be extended from 550m to 100km using the flexibility of any third party pluggable SFP modules. GSW-2008MS has an optional cable tray which allows the installer to enclose the excessive fiber loop within the tray housing, providing protection for the sensitive fiber at subscriber site. GSW-2008MS is fully compliant with IEEE 802.3, 802.3u, 802.3ab and 802.3z standards. End-users can simply connect their devices, such as Ethernet home gateway, wireless access point or NIC on PC/laptop via 10/100/1000Base-T twisted pair to the RJ-45 ports of the CPE switch. No Ethernet crossover cables are required and link status can be easily monitored from the comprehensive LED display.

When GSW-2008MS is deployed as a stand-alone solution, it incorporates an easy to use Web user interface for operation, administration and maintenance both local and remotely. All of the enabled Layer 2 features and functions of GSW-2008MS can be configured and monitored via web interface and SNMP management. GSW-2008MS is the most suitable solution for deploying and provisioning the FTTX service of operators or service providers.

## 1.3 Product Features

- 8 x 10/100/1000Base-T(X) RJ-45 with 2 x 100/1000Base-X SFP Fiber
- 12VDC input via universal switching adapter
- Cable diagnostic, length measurement, cable OK or broken point distance
- Supports IEEE802.3az EEE (Energy Efficient Ethernet) Management to optimize power consumption
- STP, RSTP, MSTP, QoS, Traffic classification QoS, CoS, Bandwidth control for Ingress and Egress, broadcast storm control, DiffServ, IEEE802.1q VLAN, MAC based VLAN, IP subnet based VLAN, Protocol based VLAN, VLAN translation, MVR, Dynamic IEEE 802.3ad LACP Link Aggregation, Static Link Aggregation, IGMP/MLD snooping V1/V2/V3, IGMP Filtering / Throttling, IGMP query, IGMP proxy reporting, MLD snooping
- Security : Port based and MAC based IEEE802.1X, RADIUS, ACL, TACACS+, HTTP/HTTPS, SSL/SSH v2
- CLI, Web based management, SNMP v1/v2c/v3, Telnet server for management
- Software upgrade via TFTP and HTTP, dual partitioned flash for quick recovery from upgrade failure
- DHCP client/Relay/Snooping/Snooping option 82/Relay option 82
- RMON, MIB II, port mirroring, event syslog, DNS, NTP/SNTP, IEEE802.1ab LLDP
- Supports IPv6 Telnet server/ICMP v6, SNMP, HTTP, SSH/SSL, NTP/SNTP, TFTP, QoS, ACL
- CE, FCC Certified



## 1.4 Product Specifications

Standards	IEEE 802.3	10Base-T 10Mbit/s Ethernet
	IEEE 802.3u	100Base-TX, 100Base-FX, Fast Ethernet
	IEEE 802.3ab	1000Base-T Gbit/s Ethernet over twisted pair
	IEEE 802.3z	1000Base-X Gbit/s Ethernet over Fiber-Optic
	IEEE 802.1Q	Virtual LANs (VLAN)
	IEEE 802.1X	Port based Network Access Control, Authentication
	IEEE 802.3x	Flow control for Full Duplex
	IEEE 802.1ad	Stacked VLANs, Q-in-Q
	IEEE 802.1p	LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization
	IEEE 802.1ab	Link Layer Discovery Protocol (LLDP)
	IEEE 802.3az	EEE (Energy Efficient Ethernet)
Switch	VLAN Groups	up to 4096
	Switching Fabric	20Gbps
	Data Processing	Store and Forward
	Flow Control	IEEE 802.3x for full duplex mode, back pressure for half duplex mode
	MTU	9600 Bytes (Jumbo Frames)
	MAC Table	8K
Connectors	LAN	8 x RJ-45 10/100/1000BaseT(X) auto detect speed, auto negotiate duplex, auto MDI/MDI-X function, Full/Half duplex
	Fiber	2 X 100/1000Base-X dual speed mode SFP slot, supporting DDMI
Ethernet	Network Cable	UTP/STP Cat.5e cable or above
	EIA/TIA-568	100-ohm (100m)
	Protocol	CSMA/CD
	Reverse polarity	auto detect/correct
	Protection	Present
	Overload current protection	Present
	CPU Watch Dog	Present
Power	Power Supply	External AC adapter, 12VDC 1A capacity
LED	LED Indicators	PWR, Fiber1~2, LAN 1~8

## Chapter 2. Panels & LED Indicators

This section describes the front panel, rear panel and top panel of GSW-2008MS. The front panel of GSW-2008MS only has LAN ports; while, the rear panel provides SFP cages, reset push-button and AC power port. LED indicators are located on the top panel to provide real-time indications of link status. See below for detailed descriptions.

### 2.1 Front Panel

There are 8 shielded RJ-45 that provide LAN connections from GSW-2008MS Switch. These ports support Ethernet speeds of 10/100/1000M automatically. Each of these eight LAN ports has associated LEDs, located on the top panel, which indicate the active link state and the detected speed of the interface. A green indicates a link and a speed of 100M, while amber color indicates a link and speed of 1000M.

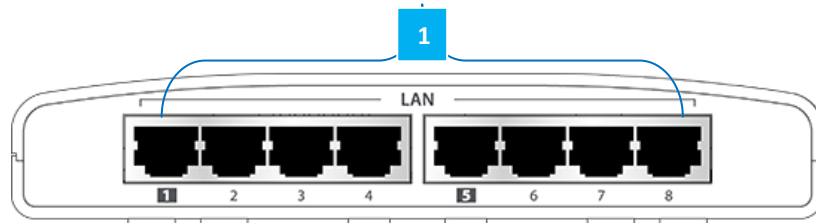


Figure 1: Front View

- 1 10/100/1000M RJ-45 LAN ports

### 2.2 Rear Panel

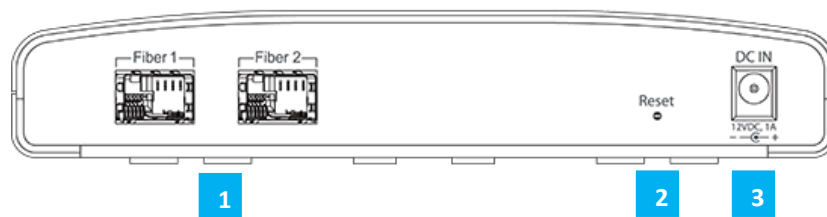


Figure 2: Rear View

- 1 100/1000 SFP cage
- 2 Reset push-button
- 3 DC jack

### 2.2.1 Fiber Connections

Refer to the graphic drawing above. GSW-2008MS utilizes an SFP module for fiber transmission. The fiber port has an associated status LED (viewed from the top) to indicate the presence or absence of fiber link and will also flash when there is Ethernet activity on the port. The SFP cage may insert any standard SFP module and be configured for 100M or 1000M operation. There is no 'lock out' mechanism, so any third party SFP, compliant with MSA, can be used in GSW-2008MS.

### 2.2.2 Reset Push-Button

There is a recessed push-button switch used to reset GSW-2008MS or to return it to factory defaults. Pressing the reset momentarily once will "warm boot" the switch. Pressing and holding the pushbutton switch for more than 3 seconds and then releasing will set the running configuration to the original factory default settings, including the original factory default IP address followed by a "warm boot". If the IP address of the switch is unknown, it may be necessary to do a factory default reset. The IP address will then be the known default.

### 2.2.3 Power

GSW-2008MS uses an external AC power adapter that supports wide voltage range input and is of a 'green' power efficiency design. Plug the power adapter's DC plug into the GSW-2008MS prior to plugging the adapter into the AC power source.

## 2.3 LED Indicators

LED indicators are located on the top of unit. Each port has a corresponding LED indicator that provides a visual and real-time indication of the current operating state. A description of these LED indicators is provided below.



**Figure 3: Top of unit**

LED	Color	Meaning
PWR	Blue	The switch is receiving power.
	Off	The switch does not receive power.
Fiber 1 & Fiber 2	Amber	The fiber port link is up and operating at 1000Mbps.
	Green	The fiber port link is up and operating at 100Mbps.
	Amber Blinking/Green Blinking	The fiber port is receiving and transmitting traffic.
	Off	The fiber port link is down.
LAN 1~LAN8	Amber	When the LAN port is up and operating at 1000Mbps.
	Green	When the LAN port is up and operating at 100Mbps.
	Amber + Green	When the LAN port is up and operating at 10Mbps.
	Amber Blinking/Green Blinking/Amber + Green Blinking	The LAN port is receiving and transmitting traffic.
	Off	The LAN port link is down.

## Chapter 3. Installation

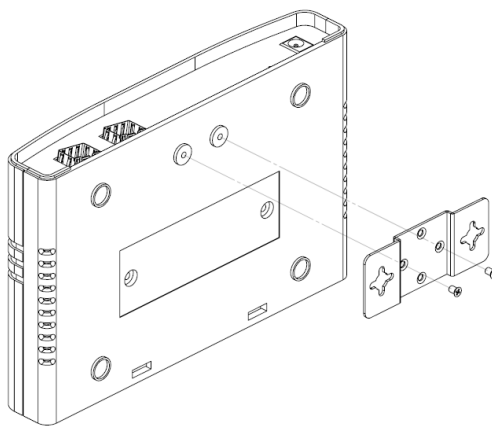
### 3.1 Introduction

GSW-2008MS is designed for placing on a desktop or optionally can be mounted on the wall. We also offer a fiber cable tray that can meet varying needs of cable management. GSW-2008MS comes without wall-mounting kit and fiber tray from the factory. If you need to order optional accessories, please contact our sales representatives directly.

#### 3.1.1 Wall-Mounting (GSW-2008MS)

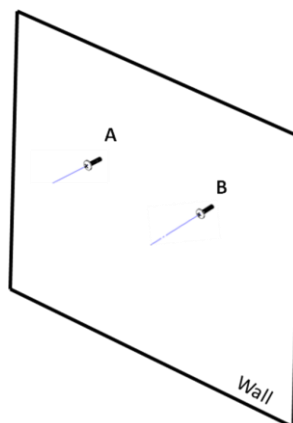
Wall-mounting kit is an optional accessory. It does not come with the standard package of the device. Before starting installing your device on the wall, please make sure you have a bracket and screws at hand. Follow the steps below to correctly install the device on a wall.

**Step 1.** Attach the bracket correctly and securely to the device using two wall-mounting screws as shown in Figure 4.



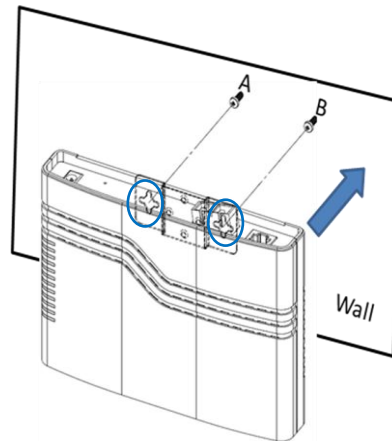
**Figure 4: Attach the wall-mounting bracket to the device**

**Step2.** Then, drill Hole A & B and install screws for hanging purposes as shown in Figure 5.



**Figure 5: Drill two holes and install screws for hanging purposes**

**Step 3:** Mount the device on the wall using two hanging screws with front panel facing downwards and slide it downward until it locks securely.

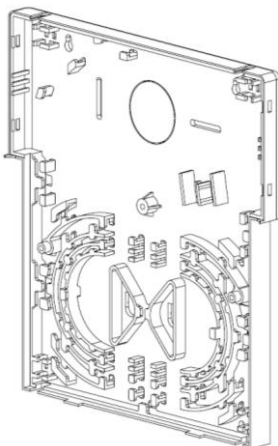


**Figure 6: Mounting the device on the wall**

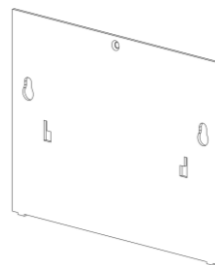
### 3.1.2 Cable Tray Installation

Cable tray kit is an optional accessory. It does not come with the standard package of the device. The cable tray is the specially-designed fiber organizer that is used to store the excessive fiber so as to prevent the fiber cable from unexpected damages. Before installing the cable tray, please make sure you have the device and cable tray kit at hand. Follow the steps below to correctly install the cable tray.

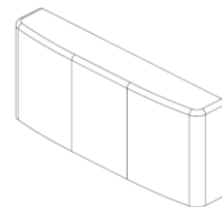
**Step 1.** Check the cable tray kit. Your cable tray kit should have the following parts: one cable tray base (Figure 7), one cable tray dust cover (Figure 8), one cable tray upper cover (Figure 9).



**Figure 7: Cable tray base**

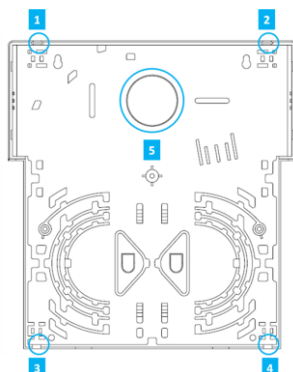


**Figure 8: Cable tray dust cover**

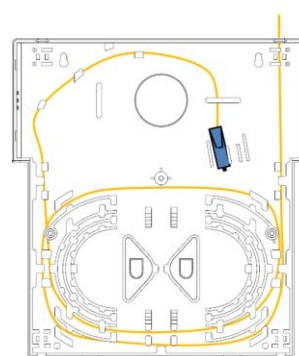


**Figure 9: Cable tray upper cover**

**Step 2.** Organize the fiber cable into the cable tray base. There are five fiber cable input holes that you can use to organize your cable (Figure 10). Use the cable tray fixations to fix your fiber cable securely on the cable tray while organizing. See Figure 11 for an example.



**Figure 10: Fiber cable input holes**



**Figure 11: Fiber cable installation**

**Step 3.** Put the dust cover on the cable tray base and slide the dust cover downward to securely fasten two items together (Figure 12 & 13).

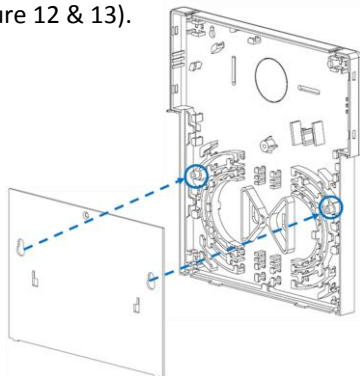


Figure 12: Install the cable tray dust cover

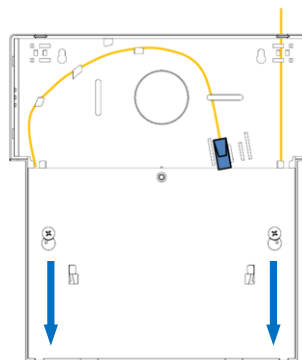


Figure 13: Fasten two items securely

**Step 4.** Use two mounting holes on GSW-2008MS (Figure 14) to install it on the cable tray base (Figure 15).

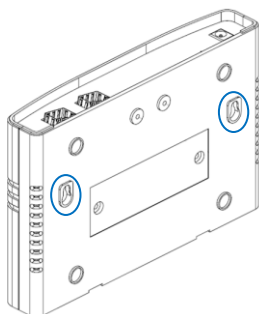


Figure 14: Cable tray mounting holes

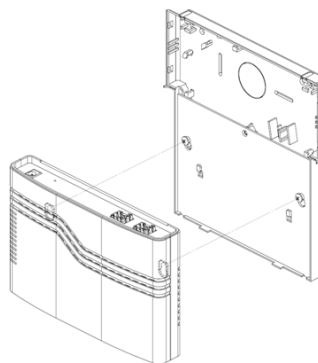


Figure 15: Install the device onto the cable tray

**Step 5.** Slide GSW-2008MS downward to attach two items securely together.

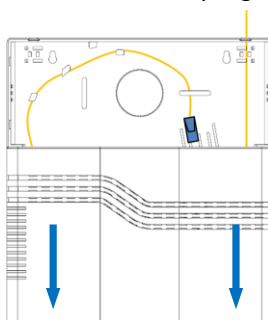


Figure 16: Slide the device down

**Step 6.** Connect the fiber cable connector to the SFP transceiver and power cable to the power port.

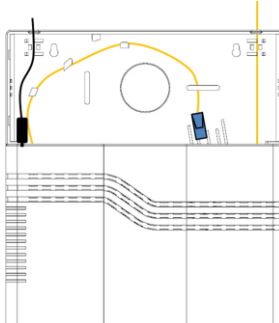
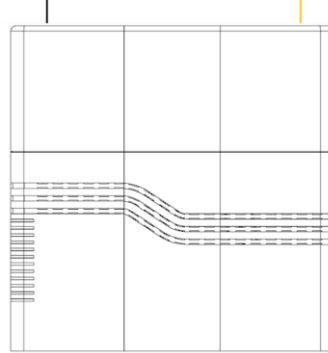


Figure 17: Connect to the SFP transceiver and power port

**Step 7.** Finally, install the fiber cable tray upper cover.



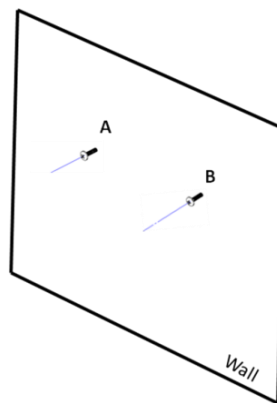
**Figure 18:** Install the fiber cable tray upper cover

### 3.1.3 Wall-Mounting (GSW-2008MS with Cable Tray)

GSW-2008MS with cable tray management can also be mounted on the wall. Before starting wall-mounting installation, make sure you have organized fiber cable into the cable tray base.

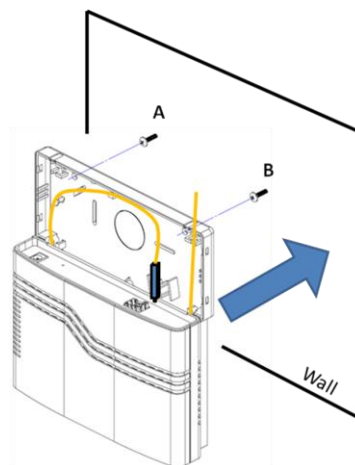
**Step 1.** Make sure you have organized fiber cable into the cable tray base.

**Step 2.** Drill Hole A & B and install screws for hanging purposes as shown in Figure 19.



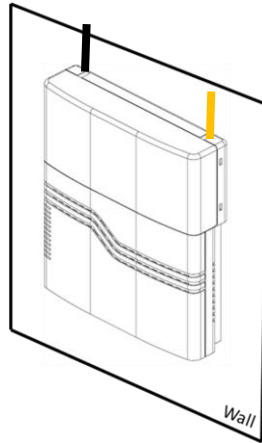
**Figure 19:** Drill two holes and install two screws for hanging purposes.

**Step 3:** Mount the device on the wall using two hanging screws with front panel facing downwards and slide it downward until it locks securely.



**Figure 20:** Mount the device on the wall

**Step 4.** Install the upper case cover.



**Figure 21:** Install the upper case cover



## Chapter 4. Introduction to CLI

### 4.1 Introduction

The GSW-2008MS Managed Gigabit Ethernet CPE switch provides a number of configuration/management methods. The first method of configuration/management uses a command line interface (CLI) via Telnet/SSH access and is familiar to most network engineers. This requires that networking be configured so that the device can be accessed via a LAN port. Accessing the GSW-2008MS from a network allows for both local and remote management.

For engineers that are not comfortable using CLI, this device should be managed using any standard Web Browser in a more user friendly 'point-and-click' method. Therefore, in most configuration scenarios, Telnet/SSH will only be used by experienced networking engineers.

After the device has been properly configured for the application and placed into service, a third method of configuration/management can be employed using Simple Network Management Protocol (SNMP). The operator will use SNMP management software to manage and monitor the GSW-2008MS switches on a network. This requires some configuration of the device to allow SNMP management. In addition, the network management platform will need to import and compile the proprietary MIB (management information base) file so that the management software knows "how" to manage the GSW-2008MS.

### 4.2 Telnet Operation

Default TCP/IP settings of GSW-2008MS:

IP Address: 192.168.0.1  
Subnet Mask: 255.255.255.0  
Username: admin  
Password: None (Leave this field blank)

From a cold start, the following screen will be displayed. At the "Username" prompt, enter 'admin' with no password.

```
Username: admin
Password:
Login in progress...
Welcome to CCLI (v1.2).
Type 'help' or '?' to get help.
>
```

### 4.2.1 CLI Online Help

While using the CLI, online help is always available by using 'help' command or typing '?' (question mark). Commands can be recalled by using the 'up/down arrow keys'.

Note: When making corrections while typing, please be aware that unless the terminal emulation program specifically issues a [CTRL-H] for [Backspace] that the backspace action must use the key combination of [CTRL-H] as the [Backspace] character is not recognized by the CLI.

```
>?
General Commands:
-----
Help/? : Get help on a group or a specific command
Up      : Move one command level up
Logout  : Exit CCLI

Command Groups:
-----
System      : System settings and reset options
IP          : IP configuration and Ping
Auto Provision: Auto Provision configuration
Port        : Port management
MAC         : MAC address table
VLAN        : Virtual LAN
PVLAN       : Private VLAN
Security    : Security management
STP         : Spanning Tree Protocol
Aggr        : Link Aggregation
LACP        : Link Aggregation Control Protocol
LLDP        : Link Layer Discovery Protocol
LLDPMED     : Link Layer Discovery Protocol Media
EEE         : Energy Efficient Ethernet
Thermal     : Thermal Protection
Led_power   : LED power reduction
PoE         : Power Over Ethernet
QoS         : Quality of Service
Mirror      : Port mirroring
Config      : Load/Save of configuration via TFTP
Firmware    : Download of firmware via TFTP
UPnP       : Universal Plug and Play
MVR         : Multicast VLAN Registration
Voice VLAN  : Specific VLAN for voice traffic
Loop Protect : Loop Protection
IPMC        : MLD/IGMP Snooping
sFlow      : sFlow Agent
VCL         : VLAN Control List

Type '<group>' to enter command group, e.g. 'port'.
Type '<group> ?' to get list of group commands, e.g. 'port ?'.
Type '<command> ?' to get help on a command, e.g. 'port mode ?'.
Commands may be abbreviated, e.g. 'por co' instead of 'port configuration'.
>
```

### 4.2.2 TCP/IP Configuration via CLI

#### 4.2.2.1 IP Address, Subnet Mask, Default Router

syntax: IP Setup [<ip\_addr>] [<ip\_mask>] [<ip\_router>] [<vid>]

```
>ip setup 192.168.0.251 255.255.255.0 192.168.0.10 1
>
```

Note: The default <vlan> for untagged packets is VID 1.  
Changing the IP address from Telnet will result in disconnection. Please avoid doing this and instead use web interface.

#### 4.2.2.2 DHCP

syntax: IP DHCP [enable|disable]

```
>ip dhcp disable
>
```

Note: The DHCP client is disabled by default. To set static IP on network with DHCP server, do not enable DHCP client.

#### 4.2.2.3 DNS Server

syntax: IP DNS <dns\_source>

```
>ip dns 192.168.0.1
>
```

Note: The <dns\_source> parameter points to the static DNS server for the network.

#### 4.2.2.4 Display TCP/IP Settings

syntax: IP Configuration

```
>ip configuration

IP Configuration:
=====

DHCP Client      : Disabled
DHCP Option 60   : GSW-2008MS
IP Address       : 192.168.0.1
IP Mask         : 255.255.255.0
IP Router       : 0.0.0.0
DNS Server      : 0.0.0.0
VLAN ID        : 1
DNS Proxy       : Disabled

IPv6 AUTOCONFIG mode : Enabled (Fallback in 300 seconds)
IPv6 Link-Local Address: fe80::6082:cdb9:19ab:c0e2
IPv6 Address      : ::192.168.0.16
IPv6 Prefix      : 96
IPv6 Router      : ::

Active Configuration for IPv6: (AUTOCONFIG... 300 seconds remaining)
IPv6 Address: fe80:2::6082:cdb9:19ab:c0e2/64 Scope:Link
Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500>
>
```

#### 4.2.3 Factory Default

syntax: System Restore Default <keep\_ip>

```
>system restore default
>
```

Note: To restore factory default but keep TCP/IP settings, use: "system restore default keep\_ip"

#### **4.2.4 Reboot Device**

syntax: System Reboot

```
>system reboot
>
```

#### **4.2.5 Admin Password**

syntax: Security Switch Users Add <username> <password> <privilege\_level>

```
>security switch add admin secret 15
>
```

Note: Sets the password "secret" for the admin user. (Admin user has the highest privilege level of 15.) To clear admin password, use a pair of double quotes to enter a null password.

```
>security switch add admin "" 15
>
```

#### **4.2.6 Logout**

syntax: Logout

```
>logout
Username:
```

Note: After the logout command is issued, the "Username:" login prompt will again be displayed.

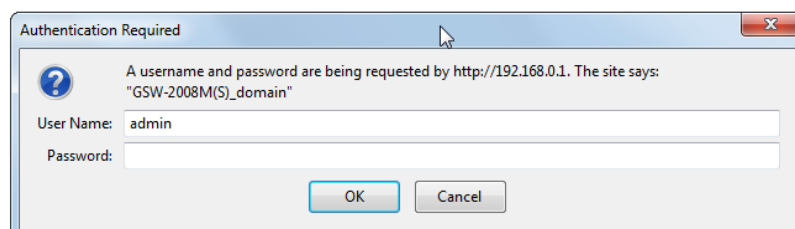
## Chapter 5. Web Configuration & Operation

### 5.1 Home Page

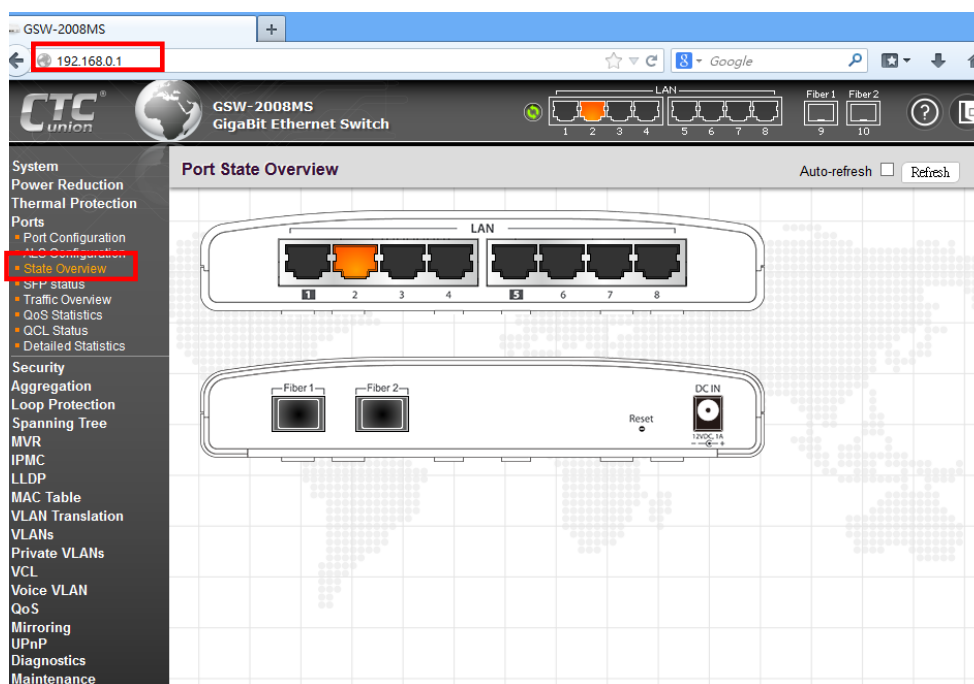
Using your favorite web browser, enter the IP address of the GSW-2008MS in the browser's location bar. The factory default address is 192.168.0.1.

#### 5.1.1 Login

A standard login prompt will appear depending on the type of browser used. The example below is with Firefox browser.



The GSW-2008MS factory default is username 'admin' with no password.



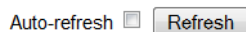
#### 5.1.2 Port Status

The initial page, when logged in, displays a graphical overview of the port status for the electrical and optical ports. The "Green" LAN port indicates a LAN connection with a speed of 100M. The "Amber" colored LAN port indicates a connection speed of 1000M.

The status display can be reached by using the left side menu, and return to Ports>State Overview.

### 5.1.3 Refresh

To update the screen, click the "Refresh" button. For automatic updating of the screen, the "Auto-refresh" tick box may be ticked. The screen will be auto refreshed every 3 seconds.



Unless connected directly on a local LAN, we recommend not using the auto-refresh function as it does generate a bit of traffic.

### 5.1.4 Help System

The device has an online "help" system to aid the engineer when setting the parameters of the device. Each functional setting page is accompanied by a specific "help" for that functional page. The user can display this help "pop up" at any time by clicking the "help" icon.

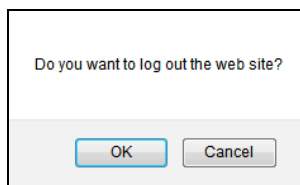


### 5.1.5 Logout

After completing configuration, we recommend logging out of the web GUI. This is easily accomplished by clicking the logout icon.



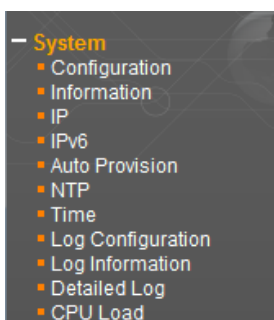
After clicking the logout icon, a confirmation screen will be displayed. Click "OK" to finish logging out or click "Cancel" to return to the web configuration GUI.



For the remainder of this section, each menu item will be explained one by one, in order as they descend down the menu screen, starting with the "System" menu.

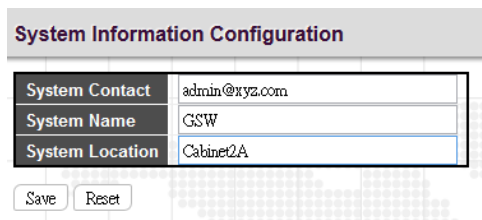
## 5.2 System

The configuration under the "System" menu includes device settings such as IP address, time server, etc.



### 5.2.1 System Configuration

The configuration information entered here will be reported in the standard SNMP MIB2 for 'sysContact' (OID 1.3.6.1.2.1.1.4), 'sysName' (OID 1.3.6.1.2.1.1.5) and 'sysLocation' (OID 1.3.6.1.2.1.1.6). Remember to click the 'Save' button after entering the configuration information.

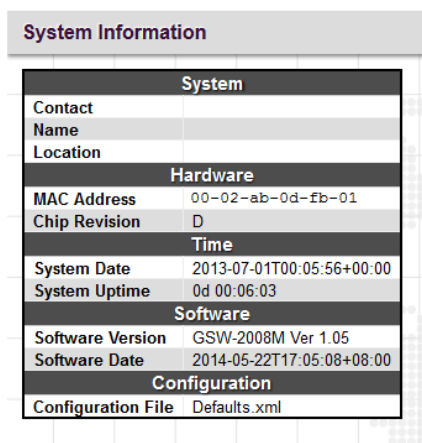


The screenshot shows a web form titled "System Information Configuration". It contains three input fields: "System Contact" with the value "admin@xyz.com", "System Name" with the value "GSW", and "System Location" with the value "Cabinet2A". Below the fields are "Save" and "Reset" buttons.

System Contact	admin@xyz.com
System Name	GSW
System Location	Cabinet2A

### 5.2.2 System Information

The system information screen will display the configuration information, the hardware MAC address and version, the system time, the system "uptime" and the software version and build date.

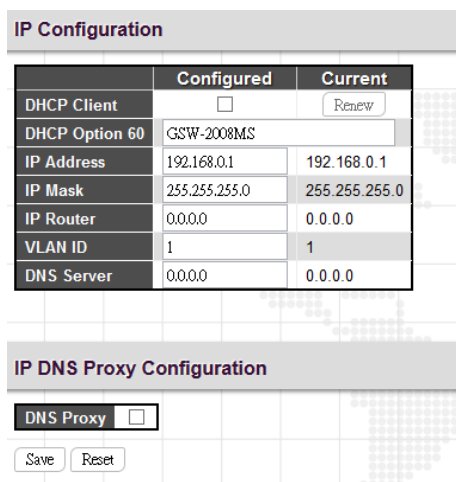


The screenshot shows a web page titled "System Information" displaying various system details in a table format, grouped by sections.

System	
Contact Name	
Location	
Hardware	
MAC Address	00-02-ab-0d-fb-01
Chip Revision	D
Time	
System Date	2013-07-01T00:05:56+00:00
System Uptime	0d 00:06:03
Software	
Software Version	GSW-2008M Ver 1.05
Software Date	2014-05-22T17:05:08+08:00
Configuration	
Configuration File	Defaults.xml

### 5.2.3 System IP

Setup the IP configuration, interface and routes.



The screenshot shows two web forms. The top form is "IP Configuration" with a table of fields for DHCP Client, DHCP Option 60, IP Address, IP Mask, IP Router, VLAN ID, and DNS Server. The bottom form is "IP DNS Proxy Configuration" with a checkbox for "DNS Proxy".

	Configured	Current
DHCP Client	<input type="checkbox"/>	<input type="button" value="Renew"/>
DHCP Option 60	GSW-2008MS	
IP Address	192.168.0.1	192.168.0.1
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

**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 server does not respond around 35 seconds 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.

**DHCP Option 60:** Configure the DHCP option 60 vendor class ID. The allowed string length is 0 to 60, and the allowed content is the ASCII characters from 0x20 to 0x7E.

**IP Address:** The IPv4 address of the interface is entered in dotted decimal notation. If DHCP is enabled, DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the IP address is configured, DHCP will stop and the configured IP settings will be used.

**IP Mask:** The IPv4 network mask is entered by a number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.

**IP Router:** This is the IP address of the gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

**VLAN:** This is the VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface.

**DNS Server:** This setting controls the DNS name resolution done by the switch.

### 5.2.4 System IPv6

Configure the switch-managed IPv6 information on this page. The Configured column is used to view or change the IPv6 configuration. The Current column is used to show the active IPv6 configuration.

IPv6 Configuration		
	Configured	Current
Auto Configuration	<input type="checkbox"/>	<input type="button" value="Renew"/>
Address	::192.168.0.16	::192.168.0.16 Link-Local Address: fe80::202:abff:fe0d:fb11
Prefix	96	96
Router	::	::

**Auto Configuration:** Enable IPv6 auto-configuration by checking this box. If system cannot obtain the stateless address in time, the configured IPv6 settings will be used. 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:** Provides 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 appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

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

**Router:** Provides 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 appear only once. It can also represent a legally valid IPv4 address. . For example, '::192.1.2.34'.



### 5.2.5 System Auto Provision Configuration

Configure auto provision on this page.

Auto Provision Configuration	
Auto Provision Mode	Disabled
HTTP/FTP Login	Disabled
HTTP/FTP Username	
HTTP/FTP Password	
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

**Auto Provision Mode:** Indicates the auto provision operation mode. Possible modes are:

**Enabled:** Enable auto provision mode operation. When auto provision mode operation is enabled, the device can download software and configuration automatically.

**Disabled:** Disable auto provision mode operation.

**HTTP/FTP Login:** Indicates the HTTP/FTP downloading mode operation. Possible modes are:

**Enabled:** When HTTP/FTP Login is enabled, the device downloads software and configuration with username and password if given at below.

**Disabled:** Downloads software and configuration without username and password.

**HTTP/FTP Username:** If both Auto Provision Mode and HTTP/FTP Login are enabled, this username is used as the ID when logging into HTTP or FTP server. The allowed string length is 0 to 20,

**HTTP/FTP Password:** If both Auto Provision Mode and HTTP/FTP Login are enabled, this password is used as the secret when logging into HTTP or FTP server. The allowed string length is 0 to 20.

### 5.2.6 System NTP Configuration

Configure NTP (Network Time Protocol) on this page.

NTP Configuration	
Mode	Enabled
Server 1	168.95.195.12
Server 2	
Server 3	
Server 4	
Server 5	
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

**Mode:** Indicates the NTP mode operation. Possible modes are:

**Enabled:** Enable NTP client mode operation.

**Disabled:** Disable NTP client mode operation.

**Server #:** Provides the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, ':::192.1.2.34'.

### 5.2.7 System Time

Setup the device time.

The screenshot shows a web configuration page with three main sections:

- Time Zone Configuration:** A dropdown menu for 'Time Zone' is set to '(GMT-05:00) Eastern Time (US and Canada)'. Below it, the 'Acronym' is set to 'EST'.
- Time Configuration:** A table with columns for Year, Month, Date, Hour, Minute, Second, and an 'Apply' button. The values are: Year: 2013, Month: 11, Date: 4, Hour: 19, Minute: 18, Second: 46.
- Daylight Saving Time Configuration:**
  - 'Daylight Saving Time Mode' is set to 'Recurring'.
  - Start Time settings:** Week: 2, Day: Sun, Month: Mar, Hours: 2, Minutes: 0.
  - End Time settings:** Week: 1, Day: Sun, Month: Nov, Hours: 2, Minutes: 0.
  - Offset settings:** Offset: 60 (1 - 1440) Minutes.

At the bottom, there are 'Save' and 'Reset' buttons.

The setting example above is for Eastern Standard Time in the United States. Daylight savings time starts on the second Sunday in March at 2:00AM. Daylight savings ends on the first Sunday in November at 2:00AM. The daylight savings time offset is 60 minutes (1 hour).

#### Time Zone Configuration

**Time Zone:** Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.

**Acronym:** Set the acronym of the time zone.

#### Daylight Saving Time Configuration

This page is used to setup Daylight Saving Time Configuration.

**Daylight Saving Time:** This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default is Disabled)

#### **Recurring & Non-Recurring Configurations:**

**Start time settings:** Select the starting week, day, month, year, hours, and minutes.

**End time settings:** Select the ending week, day, month, year, hours, and minutes.

**Offset settings:** Enter the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

### 5.2.8 System Log Configuration

Configure System Log on this page.

The image shows a 'System Log Configuration' form. It contains three input fields: 'Server Mode' with a dropdown menu set to 'Disabled', 'Server Address' with an empty text box, and 'Syslog Level' with a dropdown menu set to 'Info'. Below these fields are two buttons: 'Save' and 'Reset'.

**Server Mode:** This sets the server mode operation. When the mode of operation is enabled, the syslog message will send out to syslog server (at the server address). The syslog protocol is based on UDP communication and received on UDP port 514. 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. When the mode of operation is disabled, no syslog packets are sent out.

**Server Address:** This sets the IPv4 host address of syslog server. If the switch provides DNS feature, it also can be a host name.

**Syslog Level:** This sets what kind of messages will send to syslog server. Possible levels are:

**Info:** Send information, warnings and errors.

**Warning:** Send warnings and errors.

**Error:** Send errors only.

### 5.2.9 System Log Information

Displays the collected log information.

The image shows a 'System Log Information' display. At the top right, there are controls for 'Auto-refresh' (unchecked), 'Refresh', 'Clear', and navigation arrows. Below these are two dropdown menus: 'Level' set to 'All' and 'Clear Level' set to 'All'. A text line states 'The total number of entries is 6 for the given level.' Below this, there are input fields for 'Start from ID 1' and 'with 20 entries per page.' The main part of the display is a table with the following data:

ID	Level	Time	Message
1	Info	2013-11-04T03:58:24-05:00	Switch just made a cold boot.
2	Info	2013-11-04T03:58:40-05:00	Link up on port 1
3	Info	2013-11-04T03:58:44-05:00	Link down on port 1
4	Info	2013-11-04T04:01:00-05:00	Link up on port 1
5	Info	2013-11-04T04:19:51-05:00	Link up on port 6
6	Info	2013-11-04T04:20:43-05:00	Link up on port 2

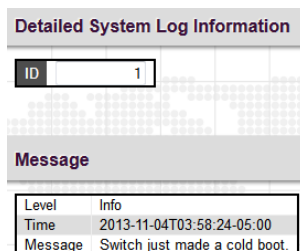
**Level:** Use this pull down to display all messages or messages of type info, warning or error.

**Clear Level:** Use this pull down to clear selected message types from the log.

Click a particular ID number to view its detailed log message. See 'System Detailed Log' section.

### 5.2.10 System Detailed Log

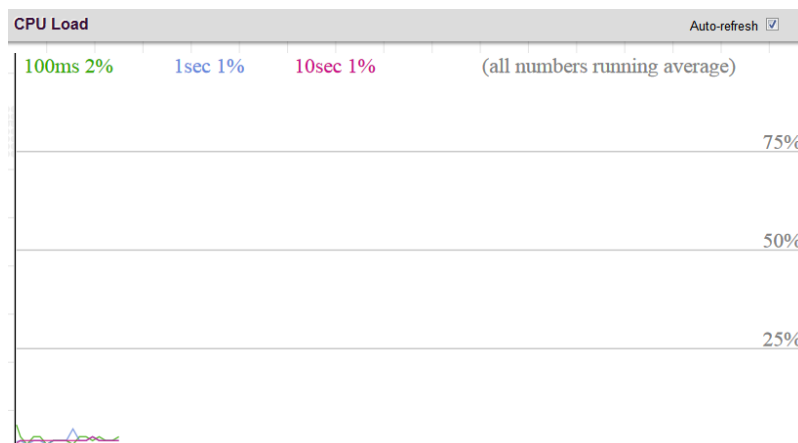
Displays individual log records.



View each log, by ID number.

### 5.2.11 System CPU Load

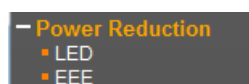
This page displays the CPU load, using an SVG graph.



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. Automatic refresh occurs every 3 seconds.

## 5.3 Power Reduction (Green Ethernet)

The configuration under the "Power Reduction" menu includes two power saving techniques.



### 5.3.1 Green Ethernet LED

Configure the LED light intensity to reduce power consumption.

**LED Power Reduction Configuration**

**LED Intensity Timers**

Delete	Time	Intensity
<input type="checkbox"/>	08:00	50 %
<input type="checkbox"/>	18:00	10 %

Add Time

**Maintenance**

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

Save Reset

The LED light intensity may be adjusted in a percentage of intensity during programmable time periods. In the above setting example, the LED intensity has been adjusted to 50% during daylight hours and reduced to only 10% intensity during night hours.

The maintenance checkbox will bring LED intensity to 100% for 10 seconds in the event of any error (such as link down).

### 5.3.2 Green Ethernet Configuration

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE was developed through the IEEE802.3az task force of the Institute of Electrical and Electronic Engineers (IEEE).

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 called 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 wakeup time information using the LLDP (Link Layer Discovery Protocol) protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.

For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic. For traffic that should not be held back, urgent queues may be assigned to reduce latency yet still result in overall power saving.

This page is used to configure EEE (Energy-Efficient Ethernet) Ethernet power savings.

**EEE Configuration**

Port	Enabled	EEE Urgent Queues							
		1	2	3	4	5	6	7	8
All	<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"/>
1	<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"/>
2	<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"/>
3	<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"/>
4	<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"/>
5	<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"/>
6	<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"/>
7	<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"/>
8	<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"/>
9	<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"/>
10	<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"/>

Save Reset

**Port:** The port number. "All" rules apply to all ports.

**Enabled:** Select the checkbox to enable EEE function on a port. By default, all ports (except Fiber port) are enabled with EEE function.

**EEE Urgent Queues:** 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. Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

## 5.4 Thermal Protection

This page allows the user to inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different priorities. Each priority can be given a temperature at which the corresponding ports shall be turned off.

- Thermal Protection
  - ▀ Configuration
  - ▀ Status

### 5.4.1 Configuration

**Thermal Protection Configuration**

Temperature settings for priority groups

Priority	Temperature
0	255 °C
1	255 °C
2	255 °C
3	255 °C

Port priorities

Port	Priority
All	< 0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0

Save Reset

**Temperature settings for priority groups:** Specify the temperature at which the ports with the corresponding priority will be turned off. Temperatures between 0°C and 255°C are supported.

**Port priorities:** The priority the port belongs to. There are 4 priority levels supported.

### 5.4.2 Status

Thermal Protection Status			
Thermal Protection Port Status			
Local Port	Temperature		Port status
1	39	°C	Port link operating normally
2	39	°C	Port link operating normally
3	38	°C	Port link operating normally
4	38	°C	Port link operating normally
5	38	°C	Port link operating normally
6	38	°C	Port link operating normally
7	38	°C	Port link operating normally
8	38	°C	Port link operating normally
9	38	°C	Port link operating normally
10	38	°C	Port link operating normally

**Local Port:** The port number.

**Temperature:** Display the current temperature on a certain port.

**Port status:** Display the current port status.

## 5.5 Ports

Configurations related to the fiber and electrical ports are performed under the Ports menu.

- Ports
  - Port Configuration
  - ALS Configuration
  - State Overview
  - SFP status
  - Traffic Overview
  - QoS Statistics
  - QCL Status
  - Detailed Statistics

### 5.5.1 Ports Configuration

This page displays current port configurations and allows some configuration here.

Port Configuration									
Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
All			<>			<input type="checkbox"/>	9600	<>	<>
1		Down	Auto nego			<input type="checkbox"/>	9600	Discard	Enabled
2		1Gfdx	Auto nego			<input type="checkbox"/>	9600	Discard	Enabled
3		Down	Auto nego			<input type="checkbox"/>	9600	Discard	Enabled
4		Down	Auto nego			<input type="checkbox"/>	9600	Discard	Enabled
5		Down	Auto nego			<input type="checkbox"/>	9600	Discard	Enabled
6		Down	Auto nego			<input type="checkbox"/>	9600	Discard	Enabled
7		Down	Auto nego			<input type="checkbox"/>	9600	Discard	Enabled
8		Down	Auto nego			<input type="checkbox"/>	9600	Discard	Enabled
9		Down	Auto nego			<input type="checkbox"/>	9600		
10		Down	Auto nego			<input type="checkbox"/>	9600		

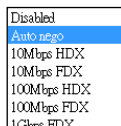
Save Reset

**Port:** This device is managed Gigabit switches with 8 electrical LAN ports numbered 1~8 and 2 fiber optical ports (for SFP module) numbered 9~10. Each logical port number is displayed in a row. The "All" settings will apply actions on all ports.

**Link:** The current link state for each port is displayed graphically. Green indicates the link is up and red indicates that it is down.

**Current Speed:** This column provides the current link speed (Auto nego, 10, 100, 1G) and duplex (fdx=Full Duplex, hdx=Half Duplex) of each port.

**Configured Speed:** This pull down selects any available link speed for the given switch port. Only speeds supported by the specific port are shown.



**Possible copper port settings are:**

Disabled - Disables the switch port operation.

Auto nego - Port auto negotiating speed with the link partner, selecting the highest speed that is compatible with the link partner and negotiating the duplex mode.

10Mbps HDX - Forces the port to 10Mbps half duplex mode.

10Mbps FDX - Forces the port to 10Mbps full duplex mode.

100Mbps HDX - Forces the port to 100Mbps half duplex mode.

100Mbps FDX - Forces the port to 100Mbps full duplex mode.

1Gbps FDX - Forces the port to 1Gbps full duplex



**Possible fiber port settings are:**

Disabled - Disables the switch port operation.

Auto nego - Port auto negotiating speed with the link partner, selecting the highest speed that is compatible with the link partner.

Detection - 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 SFP's speed might not be detectable.

100Mbps FDX - Forces the fiber port to 100Mbps full duplex mode.

1Gbps FDX - Forces the fiber port to 1Gbps full duplex mode.

**Flow Control:** 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 also related to the setting for Configured Link Speed.

**Maximum Frame Size:** Enter the maximum frame size allowed for the switch port, including FCS. This switch supports up to 9600 byte packets.

**Excessive Collision Mode:** This setting configures the port transmit collision behavior to either "Discard" (Discard frame after 16 collisions - default) or to "Restart" (Restart backoff algorithm after 16 collisions).



### 5.5.2 Ports Auto Laser Shutdown

This page allows the user to inspect and configure the current setting for transceiver module Tx power.

Auto Laser Shutdown Configuration			
Port	Mode	Period (0.1 Sec)	
		ON	OFF
1	Disabled	10	30
2	Disabled	10	30
3	Disabled	10	30
4	Disabled	10	30
5	Disabled	10	30
6	Disabled	10	30
7	Disabled	10	30
8	Disabled	10	30
9	Disabled	10	30
10	Disabled	10	30

Save Reset

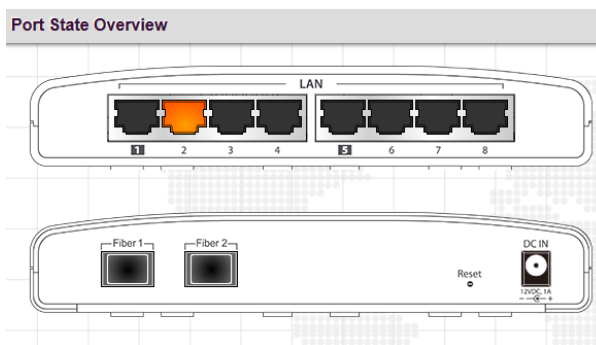
**(ALS) Mode:** Enable or disable the laser power of transceiver module shutdown automatically.

**Laser ON Period:** The period is Tx laser power turn ON. The allowed range is 2 to 30 in tenths of a second. The default period is 10 in tenths of a second (1 second).

**Laser OFF Period:** The period is Tx laser power turn OFF. The allowed range is 10 to 50 in tenths of a second. The default period is 30 in tenths of a second (3 second).

### 5.5.3 Ports State

Display an overview graphic of the switch.



This is the same graphic overview shown when first logging into the switch for management. "Green" colored ports indicate a 100M linked state, while "Amber" colored ports indicate a 1G linked state. "Grey" ports have no link. The link status display can be updated by clicking the "Refresh" button. When "Auto-refresh" is checked, the display will be updated every 3 seconds.

### 5.5.4 Ports SFP

This page provides status of SFP.

SFP Status	
Item	Information
Vendor Name	CTC UNION
Vendor PN	SFS-7020-WA
Vendor SN	2471007
Fiber Type	Single mode
Tx Power	-1.7 dBm
Rx Power	8.1 dBm
Tx Bias	13 mA
Supply Voltage	0.670 V
Temperature	26.1 °C

**Vendor Name:** The SFP vendor's (company) name.

**Vendor PN:** The part number provided by SFP vendor.

**Vendor SN:** The serial number provided by SFP vendor.

**Fiber Type:** The type of fiber channel transmission media (multi-mode or single mode).

**Tx Power:** The TX output power in dBm.

**Rx Power:** The RX received optical power in dBm.

**Tx Bias:** The TX bias current in mA.

**Supply Voltage:** The transceiver supply voltage in mV.

**Temperature:** The transceiver temperature in degree C.

### 5.5.5 Ports Traffic Overview

Displays a comprehensive overview of traffic on all ports.

Port Statistics Overview										Aut
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	0
2	1799	1384	390161	796272	0	0	0	0	0	91
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0

**Port:** The logical port (1~10) for the data 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.

The counter display can be updated by clicking the "Refresh" button. When "Auto-refresh" is checked, the display will be updated every 3 seconds. Clicking the "Clear" button will zero all counters and start counting again.

### 5.5.6 Ports QoS Statistics

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

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	0
2	1836	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1415
3	0	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	0
5	0	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	0
7	0	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	0
9	0	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	0

**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.

### 5.5.7 Ports QCL Status

This page shows the QCL status by different QCL users.

User	QCE#	Frame Type	Port	Class	DPL	DSCP	Conflict
Static	1	Ethernet	1,2	0	Default	Default	No

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:** 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 are 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.

### 5.5.8 Ports Detailed Statistics

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

Detailed Port Statistics Port 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.

#### Receive and Transmit Size Counters

**RX & TX 64 Bytes~1527:** Displays the number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

#### Receive and Transmit Queue Counters

**RX & TX Q0~Q7:** Displays 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.

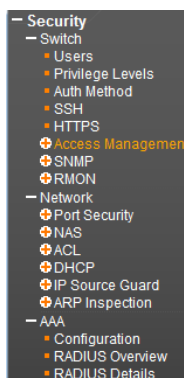
### Transmit Error Counters

**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.

## 5.6 Security

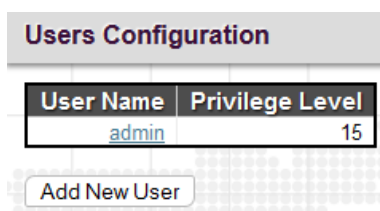
Under the security heading are three major icons, switch, network and AAA (Authentication and Accounting).



### 5.6.1 Switch

#### 5.6.1.1 Users

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



By default, there is only one user, 'admin', assigned the highest privilege level of 15.

**User Name:** The name identifying the user. Click the entries in User Name column to edit the existing users. Or click the "Add New User" button to insert a new user entry.

**Privilege Level:** The privilege level of the user.

**Add User**

**User Name:** Enter the new user name.

**Password:** Enter the password for this user account.

**Password (again):** Retype the password for this user account.

**Privilege Level:** Select the appropriate privilege level for this user account. 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 other values 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.

**5.6.1.2 Privilege Levels**

This page provides an overview of the privilege levels.

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Auto_Provision	5	10	5	10
Diagnostics	5	10	5	10
EEE	5	10	5	10
IP	5	10	5	10
IPMC_LIB	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
LLDP_MED	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MVR	5	10	5	10
Maintenance	15	15	15	15
Mirroring	5	10	5	10
PHY	5	10	5	10
POE	5	10	5	10
Port_Security	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
SNMP	5	10	5	10
Security	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
Timer	5	10	5	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10

**Group Name:** This name identifies the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:

**System:** Contact, Name, Location, Timezone, Daylight Saving Time, Log.

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

**IP:** Everything except 'ping'.

**Port:** Everything except 'VeriPHY'.

**Diagnostics:** 'ping' and 'VeriPHY'.

**Maintenance:** CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

**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

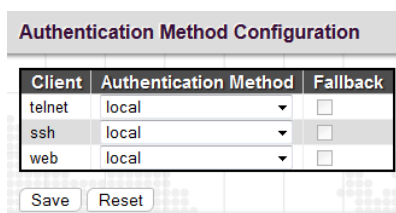
status/statistics read-only

status/statistics read-write (e.g. for clearing of statistics)

User Privilege should be the same or greater than the authorization Privilege level to have access to that group.

### 5.6.1.3 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.



**Client:** The management client for which the configuration below applies.

**Methods:** Method can be set to one of the following values:

**no:** Authentication is disabled and login is not possible.

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

**radius:** Use remote RADIUS server(s) for authentication.

**tacacs+:** Use remote TACACS+ server(s) for authentication.

---

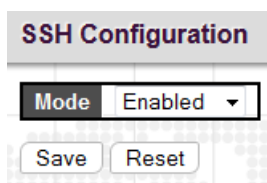
**Note:** Methods that involve remote servers will time out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

---

**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 function is only available when “Radius” or “Tacacs+” option is selected in authentication method field.

#### 5.6.1.4 SSH

Configure SSH on this page.



**Mode:** Indicates the SSH mode operation. Possible modes are:

**Enabled:** Enable SSH mode operation. By default, it is enabled.

**Disabled:** Disable SSH mode operation.

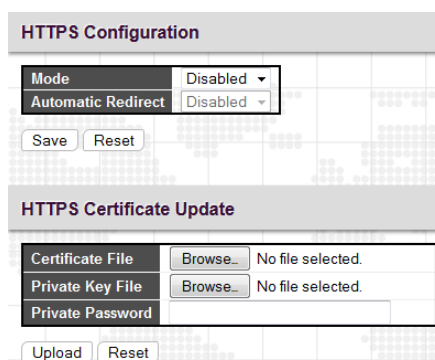
---

**Note:** SSH is preferred to Telnet, unless the management network is trusted. Telnet passes authentication credentials in plain text, making those credentials susceptible to packet capture and analysis. SSH provides a secure authentication method. The SSH in this device uses version 2 of SSH protocol.

---

#### 5.6.1.5 HTTPS

Configure HTTPS on this page.



#### HTTPS Configuration

**Mode:** Indicates the HTTPS operation mode. When the current connection is HTTPS and HTTPS mode operation is disabled, web browser will automatically redirect to an HTTP connection. Possible modes are:

**Enabled:** Enable HTTPS mode operation.

**Disabled:** Disable HTTPS mode operation.



**Automatic Redirect:** Indicates the HTTPS redirect mode operation. It applies only if HTTPS mode "Enabled" is selected. Automatically redirects HTTP of web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are:

**Enabled:** Enable HTTPS redirect mode operation.

**Disabled:** Disable HTTPS redirect mode operation.

**HTTPS Certificate Update**

**Certificate File:** Indicates a certificate file for uploading.

**Private Key File:** Indicates a private key file for uploading.

**Private Password:** Configure private key pass phrase. The allowed string length is 0 to 60.

**5.6.1.6 Access Management**

**5.6.1.6.1 Configuration**

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

**Access Management Protocol Configuration**

**Mode:** Indicates the access management mode operation. Possible modes are:

**Enabled:** Enable access management mode operation.

**Disabled:** Disable access management mode operation.

**Start IP address:** Indicates the start IP address for the access management entry.

**End IP address:** Indicates the end IP address for the access management entry.

**HTTP/HTTPS:** Checked indicates that the matched host can access the switch from HTTP/HTTPS interface.

**SNMP:** Checked indicates that the matched host can access the switch from SNMP.

**TELNET/SSH:** Indicates that the matched host can access the switch from TELNET/SSH interface.

Click the “Add New Entry” button to add a new entry.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

**Access Management Ports Configuration**

Configure access management ports table on this page. If the port is an Allowed port, it will allow access to the switch. Allowed ports are selected by check boxes.

**Mode:** Indicates the access management ports mode operation. Possible modes are:

**Enabled:** Enable access management ports mode operation.

**Disabled:** Disable access management ports mode operation.

**Port:** The switch port number of the logical port.

**Allowed:** Indicates that the host can access the switch from this port.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

**5.6.1.6.2 Access Management Statistics**

This page provides statistics for access management.

Access Management Statistics			
Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	312	312	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

**Interface:** The interface type through which any remote host can access the switch.

**Received Packets:** The number of received packets from the interface when access management mode is enabled.

**Allowed Packets:** The number of allowed packets from the interface when access management mode is enabled.

**Discarded Packets:** The number of discarded packets from the interface when access management mode is enabled.

### 5.6.1.7 SNMP

#### 5.6.1.7.1 System Configuration

Configure SNMP on this page.

SNMP System Configuration	
Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

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 Dying-gasp	Enabled
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

Save | Reset

#### SNMP System Configuration

**Mode:** Indicates the SNMP mode operation. Possible modes are:

**Enabled:** Enable SNMP mode operation.

**Disabled:** Disable SNMP mode operation.

**Version:** Indicates the SNMP supported version. Possible versions are:

**SNMP v1:** Set SNMP supported version 1.

**SNMP v2c:** Set SNMP supported version 2c.

**SNMP v3:** Set SNMP supported version 3.

**Read Community:** Indicates the community read access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.

**Write Community:** Indicates the community write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E. These two fields are applicable only for SNMP version v1 or v2c. If SNMP version is v3, the community string will be associated with SNMPv3 communities table. SNMPv3 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. Changes to the Engine ID will clear all original local users.

### SNMP Trap Configuration

Configure SNMP trap on this page.

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 Dying-gasp	Enabled
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

**Trap Mode:** Indicates the SNMP trap mode operation. Possible modes are:

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

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

**Trap Version:** Indicates the SNMP trap supported version. Possible versions are:

**SNMP v1:** Set SNMP trap supported version 1.

**SNMP v2c:** Set SNMP trap supported version 2c.

**SNMP v3:** 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 0x21 to 0x7E.

**Trap Destination Address:** Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.

**Trap Destination IPv6 Address:** Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

**Trap Authentication Failure:** Issues a notification message to the specified IP trap managers or not whenever SNMP authentication request fails.

**Enabled:** Enable trap authentication failure.

**Disabled:** Disable trap authentication failure.

**Trap Link-up and Link-down:** Issues a notification message whenever a port is link up and link down.

**Enabled:** Enable trap link-up and link-down.

**Disabled:** Disable trap link-up and link-down.

**Trap Dying gasp:** Enable or disable dying gasp trap sent to the server.

**Enabled:** Enable dying gasp trap mode operation.

**Disabled:** Disable dying gasp trap mode operation.

**Trap Inform Mode:** Indicates the SNMP trap inform mode operation. Possible modes are:

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

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

**Trap Inform Timeout (seconds):** Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

**Trap Inform Retry Times:** Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

**Trap Probe Security Engine ID:** Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:

**Enabled:** Enable SNMP trap probe security engine ID mode of operation.

**Disabled:** Disable SNMP trap probe security engine ID mode of operation.

**Trap Security Engine ID:** Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs use 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 use USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

#### 5.6.1.7.2 SNMPv3 Community Configuration

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

SNMPv3 Community Configuration			
Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0

**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 0x21 to 0x7E. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string. This string is case sensitive.

**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.

#### 5.6.1.7.3 SNMPv3 User Configuration

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

SNMPv3 User Configuration							
Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

**Engine ID:** An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a

simple agent, `usmUserEngineID` is always that agent's own `snmpEngineID` value. The value can also take the value of the `snmpEngineID` of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it is a 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 0x21 to 0x7E.

**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 it must first be ensured 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 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 0x21 to 0x7E.

**Privacy Protocol:** Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

**None:** No privacy protocol.

**DES:** An optional flag to indicate that this user uses DES authentication protocol.

**AES:** An optional flag to indicate that this user uses AES authentication protocol.

**Privacy Password:** A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

Click the "Add New Entry" button to insert a new entry to the list.

Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

Click the "Reset" button to restore changed settings to the default settings.

#### 5.6.1.7.4 SNMPv3 Group Configuration

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

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

Buttons: Add New Entry, Save, Reset

**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) for SNMPv3.

**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 0x21 to 0x7E.

**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 0x21 to 0x7E.

Click the “Add New Entry” button to add a new entry.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

#### 5.6.1.7.5 SNMPv3 View Configuration

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

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included	.1

Buttons: Add New Entry, Save, Reset

**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 0x21 to 0x7E.

**View Type:** Indicates the view type that this entry should belong to. Possible view types are:

**included:** An optional flag to indicate that this view subtree should be included.

**excluded:** An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

**OID Subtree:** The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or an asterisk(\*).

Click the “Add New Entry” button to add a new entry.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

#### 5.6.1.7.6 SNMPv3 Access Configuration

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

SNMPv3 Access Configuration					
Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▾	None ▾
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▾	default_view ▾

**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 0x21 to 0x7E.

**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) for SNMPv3.

**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 0x21 to 0x7E.

**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 0x21 to 0x7E.



## 5.6.1.8 RMON

### 5.6.1.8.1 RMON Statistics Configuration

Remote monitoring is a standard specification that enables various network monitors to exchange network monitoring data. RMON provides the user with more freedom in selecting networking monitoring probes that meet their particular networking needs.

Delete	ID	Data Source
<input type="checkbox"/>	1	.1.3.6.1.2.1.2.2.1.1.
<input type="checkbox"/>	2	.1.3.6.1.2.1.2.2.1.1.
<input type="checkbox"/>	3	.1.3.6.1.2.1.2.2.1.1.

Add New Entry Save Reset

**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.

Click the “Add New Entry” button to add a new entry.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.6.1.8.2 RMON History Configuration

RMON History Configuration is to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A RMON historical record can also be used to monitor intermittent problems.

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete	0	.1.3.6.1.2.1.2.2.1.1.	1800	50	

Add New Entry Save Reset

**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 polling interval. By default, 1800 seconds is specified. The allowed range is 1~3600 seconds.

**Buckets:** The number of buckets requested for this entry. By default, 50 is specified. The allowed range is 1~3600.

**Buckets Granted:** The number of buckets granted.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.6.1.8.3 RMON Alarm Configuration

RMON Alarm configuration defines specific criteria that will generate response events. It can be set to test data over any specified time interval and can monitor absolute or changing values. Alarms can also be set to respond to rising or falling thresholds.

RMON Alarm Configuration											
Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index	
<input type="checkbox"/>		30	1.3.6.1.2.1.2.2.1	Delta	0	RisingOrFalling	0	0	0	0	
<input type="button" value="Add New Entry"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>											

**ID:** Indicates the index of the entry. The range is from 1 to 65535.

**Interval:** The polling interval for sampling and comparing the rising and falling threshold. The range is from 1 to 2<sup>31</sup> seconds.

**Variable:** The object number of the MIB variable to be sampled. Only variables of the type ifEntry.n.n may be sampled. Possible variables are InOctets, InUcastPkts, InNUcastPkts, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPkts, OutNUcastPkts, OutDiscards, OutErrors, and OutQLen.

**Sample Type:** Test for absolute or relative change in the specified variable.

**Absolute:** The variable is compared to the thresholds at the end of the sampling period.

**Delta:** The last sample is subtracted from the current value and the difference is compared to the thresholds.

**Value:** The statistic value during the last sampling period.

**Startup Alarm:** Select a method that is used to sample the selected variable and calculate the value to be compared against the thresholds.

**Rising or Falling:** Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.

**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.

**Rising Threshold:** If the current value is greater than the rising threshold and the last sample value is less than this threshold, then an alarm will be triggered. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. The threshold range is -2147483647 to 2147483647.

**Rising Index:** Indicates the rising index of an event. The range is 1~65535.

**Falling Threshold:** If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the falling threshold. (Range: -2147483647 to 2147483647)

**Falling Index:** Indicates the falling index of an event. The range is 1~65535.

Click the "Add New Entry" button to insert a new entry to the list.

Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

Click the "Reset" button to restore changed settings to the default settings.

### 5.6.1.8.4 RMON Event Configuration

RMON Event Configuration page is used to set an action taken when an alarm is triggered.

Delete	ID	Desc	Type	Community	Event Last Time
Delete			none	public	0

Buttons: Add New Entry, Save, Reset

**ID:** Specifies an ID index. The range is 1~65535.

**Desc:** Enters a descriptive comment for this entry.

**Type:** Select an event type that will take when an alarm is triggered.

**None:** No event is generated.

**Log:** When the event is triggered, a RMON log entry will be generated.

**snmptrap:** Sends a trap message to all configured trap managers.

**logandtrap:** Logs an event and sends a trap message.

**Community:** A password-like community string sent with the trap. Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page prior to configuring it here. The allowed characters are 0~127.

**Event Last Time:** The value of sysUpTime when an event was last generated for this entry.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.6.1.8.5 RMON Statistics Overview

This RMON statistics overview page shows interface statistics. All values displayed have been accumulated since the last system reboot and are shown as counts per second. The system will automatically refresh every 60 seconds by default.

ID	Data Source (ifindex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

**ID:** Displays an ID index.

**Data Source:** Port ID to Monitor.

**Drop:** The total number of dropped packets due to lack of resources.

**Octets:** The total number of octets of data received.

**Pkts:** The total number of packets (including bad packets, broadcast 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.

**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.

**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.

**64 Bytes:** The total number of packets (including bad packets) received that were 64 octets in length.

**X~Y (65~127, 128~255, 256~511, 512~1023, 1024~1588):** The total number packets received between X and Y octets in length.

#### 5.6.1.8.6 RMON History Overview

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multicast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

**History Index:** Displays Index of History control entry.

**Sample Index:** Displays Index of the data entry associated with the control entry.

**Sample Start:** The time at which this sample started, expressed in seconds since the switch booted up.

**Drop:** The total number of dropped packets due to lack of resources.

**Octets:** The total number of octets of data received.

**Pkts:** The total number of packets (including bad packets, broadcast 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.

**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.

**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.

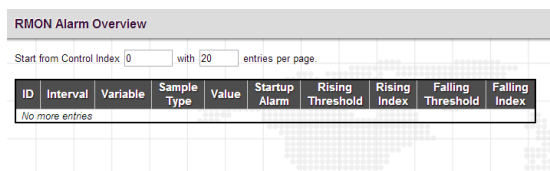
**Frag.:** The number of frames which size is less than 64 octets received with invalid CRC.

**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.

#### 5.6.1.8.7 RMON Alarm Overview



ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

**ID:** Display an alarm control index.

**Interval:** Interval in seconds for sampling and comparing the rising and falling threshold.

**Variable:** MIB object that is used to be sampled.

**Sample Type:** The method of sampling the selected variable and calculating the value to be compared against the thresholds.

**Value:** The value of the statistic during the last sampling period.

**Startup Alarm:** The alarm that may be triggered when this entry is first set to valid.

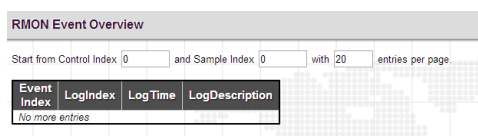
**Rising Threshold:** If the current value is greater than the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated.

**Rising Index:** The index of the event to use if an alarm is triggered by monitored variables crossing above the rising threshold.

**Falling Threshold:** If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated.

**Falling Index:** The index of the event to use if an alarm is triggered by monitored variables crossing below the falling threshold.

#### 5.6.1.8.8 RMON Event Overview



Event Index	LogIndex	LogTime	LogDescription
No more entries			

**Event Index:** Display the event entry index.

**Log Index:** Display the log entry index.

**Log Time:** Display Event log time.

**Log Description:** Display Event description.

## 5.6.2 Network

### 5.6.2.1 Port Security

Port Security Limit Control can restrict the number of users that can access the switch based on users' MAC address and VLAN ID on a per port basis. Once the number of users that wants to access the switch exceeds the specified number, a selected action will be taken immediately.

#### 5.6.2.1.1 Limit Control

Limit Control can restrict the number of users that can access the switch based on users' MAC address and VLAN ID on a per port basis. Once the number of users that wants to access the switch exceeds the specified number, a selected action will be taken immediately.

**Port Security Limit Control Configuration**

**System Configuration**

Mode: Disabled

Aging Enabled:

Aging Period: 3600 seconds

**Port Configuration**

Port	Mode	Limit	Action	State	Re-open
All	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
Fiber	Disabled	4	None	Disabled	Reopen

Save Reset

**Port Security Limit Control Configuration**

**System Configuration**

Mode: Disabled

Aging Enabled:

Aging Period: 3600 seconds

**Port Configuration**

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

Save Reset

#### System Configuration

**Mode:** Enable or disable port security limit control globally. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

**Aging Enabled:** If enabled, secured MAC addresses are subject to aging as discussed under Aging Period. 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.

**Aging Period:** If Aging Enabled is checked, then the aging period can be set up with the desired value. By default, the aging period is set to 3600 seconds. The allowed range is 10 - 10,000,000 second.

### **Port Configuration**

**Port:** Display the port number. "Port \*" rules apply to all ports.

**Mode:** Enable or disable port security limit control on a per port basis. To make limit control function work, port security limit control needs to be enabled globally and on a port.

**Limit:** The maximum number of MAC addresses that can be secured on this port. The number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

**Action:** If the limit is exceeded, the selected action will take effect.

**None:** Do not allow more than the specified limit of MAC addresses to access on a port. No action is further taken.

**Trap:** If Limit + 1 MAC addresses are 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 is 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 addresses 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:

- \* Boot the switch
- \* Disable and re-enable Limit Control on the port or the switch
- \* 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:** Display the current state of the port from the port security limit control's point of view. The displayed state might be one of the following:

**Disabled:** Limit control is either globally disabled or disabled on a port.

**Ready:** The limit is not reached yet.

**Limit Reached:** The limit is reached on a port. This state can only be shown if Action is set to None or Trap.

**Shutdown:** 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 shut down 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.

### 5.6.2.1.2 Switch Status

Port Security Switch Status					
<b>User Module Legend</b>					
User Module Name		Abbr			
Limit Control		L			
802.1X		8			
DHCP Snooping		D			
Voice VLAN		V			
<b>Port Status</b>					
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	-	-	

#### User Module Legend

**User Module Name:** The full name of a module that may request Port Security services.

**Abbr:** This column is the abbreviation for the user module used in the “Users” column in the “Port Status”.

#### Port Status

**Port:** Port number. Click a particular port number to see its port status.

**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 has enabled port security.

**State:** This shows the current status of a port. It can be one of the following states:

**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 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 (-).



### 5.6.2.1.3 Port Status

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

This page shows MAC addresses learned on a particular port.

**MAC Address:** When “Port Security Limit Control” is enabled globally and on a port, MAC addresses learned on a port shows in here.

**VLAN ID:** Display VLAN ID that is seen on this port.

**State:** Display whether the corresponding MAC address is forwarding or blocked. In the blocked state, it will not be allowed to transmit or receive traffic.

**Time of Addition:** Display the date and time when this MAC address was 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 is still forwarding 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.

### 5.6.2.2 NAS

Network Access Server configuration is useful to the networking environment that wants to authenticate clients (suplicants) before they can access resources on the protected network. To effectively control access to unknown clients, 802.1X defined by IEEE provides a port-based authentication procedure that can prevent unauthorized access to a network by requiring users to first submit credentials for authentication purposes.

A switch interconnecting clients and radius server usually acts as an authenticator and uses EAPOL (Extensible Authentication Protocol over LANs) to exchange authentication protocol messages with clients and a remote RADIUS authentication server to verify user identity and user’s access right. This section is for setting up authenticator’s configurations either on the system or on a per port basis. To configure backend server, please go to RADIUS configuration page.

### 5.6.2.2.1 Configuration

**Network Access Server Configuration**

**System Configuration**

Mode	Disabled
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

**Port Configuration for Switch 1**

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
All	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
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

#### System Configuration

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

**Reauthentication Enabled:** Select the checkbox to set clients to be re-authenticated after an interval set in "Reauthentication Period" field. Re-authentication can be used to detect if a new device is attached to a switch port.

**Reauthentication Period:** Specify the time interval for a connected device to be re-authenticated. By default, the re-authenticated period is set to 3600 seconds. The allowed range is 1~3600 seconds.

**EAPOL Timeout:** Specify the time that the switch waits for a supplicant response during an authentication session before transmitting a Request Identify EAPOL packet. By default, it is set to 30 seconds. The allowed range is 1~255 seconds.

**Aging Period:** Specify the period that is used to age out a client's allowed access to the switch via 802.1X and MAC-based authentication. The default period is 300 seconds. The allowed range is 10~1000000 seconds.

**Hold Time:** The time after an EAP Failure indication or RADIUS timeout that a client is not allowed access. This setting applies to ports running Single 802.1X, Multi 802.1X, or MAC-based authentication. By default, hold time is set to 10 seconds. The allowed range is 10~1000000 seconds.

**Radius-Assigned QoS Enabled:** Select the checkbox to globally enable RADIUS assigned QoS.

**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.

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 determines 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. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to

the Guest VLAN is disabled on all ports.

**Guest VLAN ID:** This VLAN ID is functional only when Guest VLAN is enabled. This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. The range is 1~4095.

**Max. Reauth. Count:** The maximum number of times the switch transmits an EAPOL Request Identity frame without receiving a response before adding a port to the Guest VLAN. The value can only be changed when the Guest VLAN option is globally enabled. The range is 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

**Port:** Port number. "Port \*" rules apply to all ports.

**Admin State:** Select the authentication mode on a port. This setting works only when NAS is globally enabled. 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:** This mode requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.

**Single 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:** 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.

**MAC-based Auth.:** Unlike port-based 802.1X, MAC-based authentication do not transmit or receive EAPOL frames. In MAC-based authentication, 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.

**RADIUS-Assigned QoS Enabled:** Select the checkbox to enable RADIUS-Assigned QoS on a port.

**Radius-Assigned VLAN Enabled:** Select the checkbox to enable RADIUS-Assigned VLAN on a port.

**Guest VLAN Enabled:** Select the checkbox to enable Guest VLAN on a port.

**Port State:** Display the current state of the port from 802.1X authentication point of view. The possible states are as follows:

**Globally Disabled:** 802.1X and MAC-based authentication are globally disabled.

**Link Down:** 802.1X and MAC-based authentication are enabled but there is no link on a port.

**Authorized:** The port is forced in authorized mode and the supplicant is successfully authorized.

**Unauthorized:** The port is forced in unauthorized mode and the supplicant is not successfully authorized by the RADIUS server.

**X Auth/Y Unauth:** The port is in a multi-supplicant mode. X clients are authorized and Y are unauthorized.

**Restart:** Restart client authentication using one of the methods described below. Note that the restart buttons are only enabled when the switch's authentication mode is globally enabled (under System Configuration) and the port's Admin State is an EAPOL-based or MACBased mode. Clicking these buttons will not cause settings changed on the page to take effect.

**Reauthenticate:** Schedules reauthentication to 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:** This forces the reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

#### 5.6.2.2.2 Switch Status

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

**Port:** Port number. Click a port to view the detailed NAS statistics.

**Admin State:** Display the port's current administrative state.

**Port Status:** Display the port state.

**Last Source:** The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication.

**Last ID:** The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication.

**QoS Class:** Display the QoS class that NAS assigns to the port. This field is left blank if QoS is not set by NAS.

**Port VLAN ID:** The VLAN ID of the port assigned by NAS. This field is left blank if VLAN ID is not set by NAS.

### 5.6.2.2.3 Port Statistics

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	1
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

#### **Port State**

**Admin State:** Display the port's current administrative state.

**Port Status:** Display the port state.

#### **Port Counters**

**Total:** The number of valid EAPOL frames of any type that have been received & transmitted by the switch.

**Response ID:** The number of valid EAPOL Response Identity frames that have been received & transmitted by the switch.

**Responses:** The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.

**Requests:** The number of valid EAPOL request frames (other than Request Identity frames) that have been transmitted by the switch.

**Start:** The number of EAPOL Start frames that have been received by the switch.

**Logoff:** The number of valid EAPOL Logoff frames that have been received by the switch.

**Invalid Type:** The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.

**Invalid Length:** The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.

### 5.6.2.3 ACL

ACL is a sequential list established to allow or deny users to access information or perform tasks on the network. In this switch, users can establish rules applied to port numbers to permit or deny actions or restrict rate limit.

#### 5.6.2.3.1 Ports

ACL Ports Configuration									
Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
All	0	<	<	Disabled Port 1 Port 2	<	<	<	<	All
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	3179
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

**Port:** The port number.

**Policy ID:** Assign an ACL policy ID to a particular port. A port can only use one policy ID; however, a policy ID can apply to many ports. The default ID is 0. The allowed range is 0~255.

**Action:** Permit or deny a frame based on whether it matches a rule defined in the assigned policy.

**Rate Limiter ID:** Select a rate limiter ID to apply to a port. Rate Limiter rule can be set up in “Rate Limiters” configuration page.

**Port Redirect:** Select a port to which matching frames are redirected.

**Mirror:** Enable or disable mirroring feature. When enabled, a copy of matched frames will be mirrored to the destination port specified in “Mirror” configuration page. ACL-based port mirroring set by this parameter and port mirroring set on the general Mirror Configuration page are implemented independently. To use ACL-based mirroring, enable the Mirror parameter on the ACL Ports Configuration page. Then open the Mirror Configuration page, set the “Port to mirror on” field to the required destination port, and leave the “Mode” field Disabled.

**Logging:** Enable logging of matched frames to the system log. To view log entries, go to System menu and then click the “System Log Information” option.

**Shutdown:** This field is to decide whether to shut down a port when matched frames are seen or not.

**State:** Select a port state.

**Enabled:** To re-open a port.

**Disabled:** To close a port.

**Counters:** The number of frames that have matched the rules defined in the selected policy.

### 5.6.2.3.2 Rate Limiters

ACL Rate Limiter Configuration

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

Save Reset

**Rate Limiter ID:** Display every rate limiter ID.

**Rate:** Specify the threshold above which packets are dropped. The allowed values are 0~3276700 pps or 1, 100, 200, 300...1000000 kbps.

**Unit:** Select the unit of measure used in rate.







### 5.6.2.3.3 Access Control List

Access Control List Configuration

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

Click on the  to insert a new ACE entry.

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.

## ACE Configuration

**Ingress Port:** Select the ingress port of the access control entry. Select “All” to apply an ACL rule to all ports or select a particular port.

**Policy Filter:** Select the policy filter type. “Any” means no policy filter is assigned to this rule (or don’t care). Select “Specific” to filter specific policy with this ACE.

**Frame Type:** Select a frame type to match. Available frame types include Any, Ethernet, ARP, IPv4. By default, any frame type is used.

**Action:** Select the action type, either to permit or deny.

**Rate Limiter:** Enable or disable the rate limiter when matched frames are found.

**Mirror:** Enable or disable mirror function.

**Logging:** Enable or disable logging when a frame is matched.

**Shutdown:** Enable or disable shutdown a port when a frame is matched.

**Counter:** Display the number of frames that have matched any of the rules defined for this ACL.

### VLAN Parameters

**802.1Q Tagged:** Select whether or not the frames should be tagged.

**VLAN ID Filter:** Select the VLAN ID filter for this ACE.

**Any:** No VLAN ID filter is specified. (Don’t care)

**Specific:** Specify a VLAN ID. A frame with the specified VLAN ID matches this ACE rule.

**Tag Priority:** Select the User Priority value found in the VLAN tag to match this rule.



### MAC Parameter

**SMAC Filter:** The type of source MAC address. Select “Any” to allow all types of source MAC addresses or select “Specific” to define a source MAC address. (This field is for ARP and Ethernet frame type only.)

**DMAC Filter:** The type of destination MAC address.

**Any:** To allow all types of destination MAC addresses

**MC:** Multicast MAC address

**BC:** Broadcast MAC address

**UC:** Unicast MAC address

**Specific:** Use this to self-define a destination MAC address. (This option is for Ethernet frame type only.)

### Ethernet Type Parameter

**Ether Type Filter:** This option can only be used to filter Ethernet II formatted packets. Select “Specific” to define an Ether Type value.

### ARP Parameter

**ARP/RARP:** Specify the type of ARP packet.

**Any:** No ARP/RARP opcode flag is specified

**ARP:** The frame must have ARP/RARP opcode set to ARP,

**RARP:** The frame must have ARP/RARP opcode set to RARP

**Other:** The frame has unknown ARP/RARP opcode flag

**Request/Reply:** Specify whether the packet is an ARP request, reply, or either type.

**Any:** No ARP/RARP opcode flag is specified

**Request:** The frame must have ARP Request or RARP Request opcode flag set.

**Reply:** The frame must have ARP Reply or RARP Reply opcode flag set.

**Sender IP Filter:** Specify the sender’s IP address.

**Any:** No sender IP filter is specified.

**Host:** Specify the sender IP address.

**Network:** Specify the sender IP address and sender IP mask.

**Target IP Filter:** Specify the destination IP address.

**Any:** No target IP filter is specified.

**Host:** Specify the target IP address.

**Network:** Specify the target IP address and target IP mask.

**ARP Sender SMAC Match:** Select “0” to indicate that the SHA (Sender Hardware Address) field in the ARP/RARP frame is not equal to source MAC address. Select “1” to indicate that SHA field in the ARP/RARP frame is equal to source MAC address. Select “Any” to indicate a match and not a match.

**RARP Target MAC Match:** Select “0” to indicate that the THA (Target Hardware Address) field in the ARP/RARP frame is not equal to source MAC address. Select “1” to indicate that THA field in the ARP/RARP frame is equal to source MAC address. Select “Any” to indicate a match and not a match.

**IP/Ethernet Length:** Select “0” to indicate that HLN (Hardware Address Length) field in the ARP/RARP frame is not equal to Ethernet (0x6) and the Protocol Address Length field is not equal to IPv4 (0x4). Select “1” to indicate that HLN (Hardware Address Length) field in the ARP/RARP frame is equal to Ethernet (0x6) and the Protocol Address Length field is equal to IPv4 (0x4). Select “Any” to indicate a match and not a match.

**IP:** Select “0” to indicate that Protocol Address Space field in ARP/RARP frame is not equal to IP (0x800). Select “1” to indicate that Protocol Address Space is equal to IP (0x800). Select “Any” to indicate a match and not a match.

**Ethernet:** Select “0” to indicate that Hardware Address Space field in ARP/RARP frame is not equal to Ethernet (1). Select “1” to indicate that Hardware Address Space field is equal to Ethernet (1). Select “Any” to indicate a match and not a match.

### **IP Parameters**

**IP Protocol Filter:** Select “Any”, “ICMP”, “UDP”, “TCP”, or “Other” protocol from the pull-down menu for IP Protocol filtering.

**IP TTL:** Select “Zero” to indicate that the TTL field in IPv4 header is 0. If the value in TTL field is not 0, use “Non-Zero” to indicate that. You can also select “any” to denote the value which is either 0 or not 0.

**IP Fragment:** Select “Any” to allow any values. “Yes” denotes that IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must match this entry. “No” denotes that IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not match this entry.

**IP Option:** Specify the options flag setting for this rule. Select “Any” to allow any values. “Yes” denotes that IPv4 frames where the options flag is set must match this entry. “No” denotes that IPv4 frames where the options flag is set must not match this entry.

**SIP Filter:** Select “Any”, “Host”, or “Network” for source IP filtering. If “Host” is selected, you need to indicate a specific host IP address. If “Network” is selected, you need to indicate both network address and subnet mask.

**SIP Address:** Specify a source IP address.

**SIP Mask:** Specify a source subnet mask.

**DIP Filter:** Select “Any”, “Host”, or “Network” for destination IP filtering. If “Host” is selected, you need to indicate a specific host IP address. If “Network” is selected, you need to indicate both network address and subnet mask.

**DIP Address:** Specify a destination IP address.

**DIP Mask:** Specify a destination subnet mask.

### 5.6.2.3.4 ACL Status

ACL Status										
User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
Static	All	Any	Permit	Disabled	Disabled	Disabled	No	No	10469	No
Static	1	Any	Permit	Disabled	Disabled	Disabled	No	No	0	No
Static	5	Any	Permit	Disabled	Disabled	Disabled	No	No	0	No
Static	2	Any	Permit	Disabled	Disabled	Disabled	No	No	0	No

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:** Display the ACL user.

**Ingress Port:** Display the ingress port of the ACE. This field could be all ports, a specific port or a range of ports.

**Frame Type:** Display 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.

**Action:** Display the forwarding action of the ACE.

**Permit:** Frames matching the ACE may be forwarded and learned.

**Deny:** Frames matching the ACE may be forwarded and learned.

**Filtered:** Frames matching the ACE are filtered.

**Rate Limiter:** Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

**Port Redirect:** Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

**Mirror:** Specify the mirror operation of this port. The allowed values are:

**Enabled:** Frames received on the port are mirrored.

**Disabled:** Frames received on the port are not mirrored. The default value is "Disabled".

**CPU:** Forward packet that matched the specific ACE to CPU.

**CPU Once:** Forward first packet that matched the specific ACE to CPU.

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

**Conflict:** Indicate the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

### 5.6.2.4 DHCP

DHCP Snooping allows the switch to protect a network from attacking by other devices or rogue DHCP servers. When DHCP Snooping is enabled on the switch, it can filter IP traffic on insecure (untrusted) ports that the source addresses cannot be identified by DHCP Snooping. The addresses assigned to connected clients on insecure ports can be carefully controlled by either using the dynamic binding registered with DHCP Snooping or using the static binding configured with IP Source Guard.

#### 5.6.2.4.1 DHCP Snooping Configuration

**DHCP Snooping Configuration**

Snooping Mode: Disabled

**Port Mode Configuration**

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

Save Reset

#### DHCP Snooping Configuration

**Snooping Mode:** Enable or disable DHCP Snooping function globally. 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.

#### Port Mode Configuration

**Port:** Port number. "Port All" rules apply to all ports.

**Mode:** Select the DHCP Snooping port mode. Ports can be set to either "Trusted" or "Untrusted".

#### 5.6.2.4.2 DHCP Relay Configuration

**DHCP Relay Configuration**

Relay Mode: Disabled

Relay Server: 0.0.0.0

Relay Information Mode: Enabled

Relay Information Policy: Replace

Save Reset

**Relay Mode:** Enable or disable the DHCP relay function.

**Relay Server:** Enter DHCP server IP address that is used by the switch’s DHCP relay agent.

**Relay Information Mode:** Enable or disable DHCP Relay option 82 function. Please note that “Relay Mode” must be enabled before this function is able to take effect.

**Relay Information Policy:** Select Relay Information policy for DHCP client that includes option 82 information.

**Replace:** Replace the DHCP client packet information with the switch’s relay information. This is the default setting.

**Keep:** Keep the client’s DHCP information.

**Drop:** Drop the packet when it receives a DHCP message that already contains relay information.

#### 5.6.2.4.3 DHCP Snooping Statistics

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

**Rx 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.

**Rx and Tx Discarded from Untrusted:** The number of discarded packet that are coming from untrusted port.

#### 5.6.2.4.4 DHCP Relay Statistics

DHCP Relay Statistics							
Auto-refresh <input type="checkbox"/> Refresh Clear							
<b>Server Statistics</b>							
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
<b>Client Statistics</b>							
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	0

#### DHCP Relay 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 Client:** 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.

### 5.6.2.5 IP Source Guard

#### 5.6.2.5.1 Configuration

The screenshot shows two configuration sections. The top section, 'IP Source Guard Configuration', has a 'Mode' dropdown set to 'Disabled' and a 'Translate dynamic to static' button. The bottom section, 'Port Mode Configuration', contains a table with columns for Port, Mode, and Max Dynamic Clients. The table lists ports 1 through 10, all with 'Disabled' mode and 'Unlimited' dynamic clients. Below the table are 'Save' and 'Reset' buttons.

Port	Mode	Max Dynamic Clients
All	Disabled	Unlimited
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

#### IP Source Guard Configuration

**Mode:** Enable or disable IP source guard globally.

**Translate dynamic to static:** Click this button to translate dynamic entries to static ones.

#### Port Mode Configuration

**Port:** The port number. “Port \*” rules apply to all ports.

**Mode:** Enable or disable IP source guard on a port. Please note that to make IP source guard work, both global mode and port mode must be enabled.

**Max Dynamic Clients:** Select the maximum number of dynamic clients that can be learned on a port. The available options are 0, 1, 2, unlimited. If the port mode is enabled and the maximum number of dynamic clients is equal 0, the switch will only forward IP packets that are matched in static entries for a given port.

#### 5.6.2.5.2 Static Table

The screenshot shows the 'Static IP Source Guard Table' interface. It features a table with columns for 'Delete', 'Port', 'VLAN ID', 'IP Address', and 'MAC address'. The 'Port' column has a dropdown menu currently showing '1'. Below the table is an 'Add New Entry' button and 'Save' and 'Reset' buttons.

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

**Port:** Select a port to which a static entry is bound.

**VLAN ID:** Enter VLAN ID that has been configured.

**IP Address:** Enter a valid IP address.

**MAC Address:** Enter a valid MAC address.

Click the “Add New Entry” button to insert a new entry to the list.

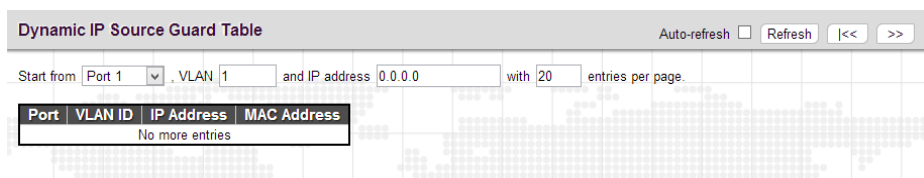
Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

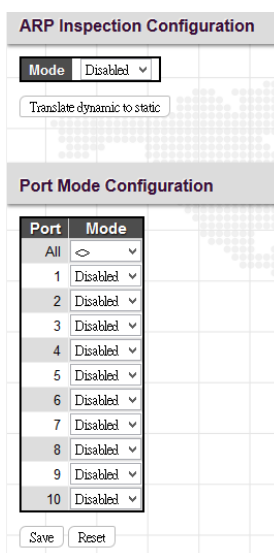
### 5.6.2.5.3 Dynamic Table

The Dynamic IP Source Guard table shows entries sorted by port, VLAN ID, IP address and MAC address. By default, each page displays 20 entries. However, it can display 999 entries by entering the number in “entries per page” input field.



## 5.6.2.6 ARP Inspection

### 5.6.2.6.1 Configuration



#### ARP Inspection Configuration

**Mode:** Enable or disable ARP inspection function globally.

#### Port Mode Configuration

**Port:** The port number. “Port All” rules apply to all ports.

**Mode:** Enable or disable ARP Inspection on a port. Please note that to make ARP inspection work, both global mode and port mode must be enabled.



### 5.6.2.6.2 Static Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Add New Entry

Save Reset

**Port:** Select a port to which a static entry is bound.

**VLAN ID:** Specify a configured VLAN ID.

**MAC Address:** Specify an allowed source MAC address in ARP request packets.

**IP Address:** Specify an allowed source IP address in ARP request packets.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.6.2.6.3 Dynamic Table

Dynamic ARP Inspection Table Auto-refresh  Refresh |<< >>

Start from Port 1, VLAN 1, MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

**Port:** The port number of this entry.

**VLAN ID:** VLAN ID in which the ARP traffic is permitted.

**MAC Address:** User MAC address of this entry.

**IP Address:** User IP address of this entry.

## 5.6.2.7 AAA

### 5.6.2.7.1 Configuration

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

#### Common Server Configuration

**Timeout:** The time the switch waits for a reply from an authentication server before it retransmits the request.

**Deadtime:** Deadtime is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. The allowed deadtime range is between 0 to 1440minutes.

#### RADIUS Authentication Server Configuration

**Enabled:** Select the checkbox to enable this authentication server configuration.

**Hostname:** The hostname or IP address for the RADIUS authentication server.

**Port:** The UDP port to be used on the RADIUS server for authentication.

**Key:** Specify the secret key up to 63 characters. This is shared between the RADIUS sever and the switch

#### RADIUS Accounting Server Configuration

**Enabled:** Select the checkbox to enable this accounting server configuration.

**Hostname:** The hostname or IP address for the RADIUS accounting server.

**Port:** The UDP port to be used on the RADIUS server for accounting.

**Key:** Specify the secret key up to 63 characters. This is shared between the RADIUS sever and the switch

#### TACACS+ Authentication Server Configuration

**Enabled:** Select the checkbox to enable this TACACS+ authentication server configuration.

**Hostname:** The hostname or IP address for the TACACS+ authentication server.

**Port:** The UDP port to be used on the TACACS+ server for authentication.

**Key:** Specify the secret key up to 63 characters. This is shared between the TACACS+ sever and the switch

### 5.6.2.7.2 RADIUS Overview

RADIUS Authentication Server Status Overview		
#	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

RADIUS Accounting Server Status Overview		
#	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

#### **RADIUS Authentication/Accounting Server Status Overview**

**IP Address:** The configured IP address and UPD port number.

**Status:** The current state of RADIUS authentication server. Displayed states include the following:

**Disabled:** This server is disabled.

**Not Ready:** The server is ready but IP communication is not yet up and running.

**Ready:** The server is ready and IP communication is not yet up and running. The RADIUS server is ready to accept access attempts.

Click the number in the pound sign (#) column to view each configured server's details.

### 5.6.2.7.3 RADIUS Details

RADIUS Authentication Statistics for Server #1			
Server #1		Auto-refresh <input type="checkbox"/>	Refresh
Clear			
Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address	0.0.0.0:1812		
State	Disabled		
Round-Trip Time	0 ms		

RADIUS Accounting Statistics for Server #1			
Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address	0.0.0.0:1813		
State	Disabled		
Round-Trip Time	0 ms		

#### RADIUS Authentication Statistics for Server

**Access Accepts:** The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

**Access Rejects:** The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

**Access Challenges:** The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

**Malformed Access Responses:** The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

**Bad Authenticators:** The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

**Unknown Types:** The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

**Packets Dropped:** The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

**Access Requests:** The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

**Access Retransmissions:** The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

**Pending Requests:** The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

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

**IP Address:** IP address and UDP port for the authentication server in question.

**State:** Shows the state of the server. It takes one of the following values:

**Disabled:** The selected server is disabled.

**Not Ready:** The server is enabled, but IP communication is not yet up and running.

**Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

**Dead (X seconds left):** Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

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

### RADIUS Accounting Statistics for Server

**Responses:** The number of RADIUS packets (valid or invalid) received from the server.

**Malformed Responses:** The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

**Bad Authenticators:** The number of RADIUS packets containing invalid authenticators received from the server.

**Unknown Types:** The number of RADIUS packets of unknown types that were received from the server on the accounting port.

**Packets Dropped:** The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

**Requests:** The number of RADIUS packets sent to the server. This does not include retransmissions.

**Retransmissions:** The number of RADIUS packets retransmitted to the RADIUS accounting server.

**Pending Requests:** The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

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

**IP Address:** IP address and UDP port for the accounting server in question.

**State:** Shows the state of the server. It takes one of the following values:

**Disabled:** The selected server is disabled.

**Not Ready:** The server is enabled, but IP communication is not yet up and running.

**Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

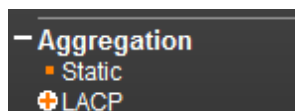
**Dead (X seconds left):** Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

**Round-Trip Time:** The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

## 5.7 Aggregation

Compared with adding cost to install extra cables to increase the redundancy and link speed, link aggregation is a relatively inexpensive way to set up a high-speed backbone network that transfers much more data than any one single port or device can deliver. Link aggregation uses multiple ports in parallel to increase the link speed. And there are two types of aggregation that are available, namely “Static” and “LACP”.

Under the Aggregation heading are two major icons, static and LACP.



### 5.7.1 Static

**Aggregation Mode Configuration**

**Hash Code Contributors**  
 Source MAC Address   
 Destination MAC Address   
 IP Address   
 TCP/UDP Port Number

**Aggregation Group Configuration**

Group ID	Port Members									
	1	2	3	4	5	6	7	8	9	10
Normal	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○

#### Aggregation Mode Configuration

**Source MAC Address:** All traffic from the same Source MAC address is output on the same link in a trunk.

**Destination MAC Address:** All traffic with the same Destination MAC address is output on the same link in a trunk.

**IP Address:** All traffic with the same source and destination IP address is output on the same link in a trunk.

**TCP/UDP Port Number:** All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk.

#### Aggregation Group Configuration

**Group ID:** Trunk ID number. “Normal” means that no aggregation is used. Five aggregation groups are available for use. Each group contains at least 2 to 10 links (ports). Please note that each port can only be used once in Group ID 1~5.

**Port Members:** Select ports to belong to a certain trunk.

## 5.7.2 LACP

The Switch supports dynamic Link Aggregation Control Protocol (LACP) which is specified in IEEE 802.3ad. Static trunks have to be manually configured at both ends of the link. In other words, LACP configured ports can automatically negotiate a trunked link with LACP configured ports on another devices. You can configure any number of ports on the Switch as LACP, as long as they are not already configured as part of a static trunk. If ports on other devices are also configured as LACP, the Switch and the other devices will negotiate a trunk link between them.

### 5.7.2.1 Port Configuration

Port	LACP Enabled	Key	Role	Timeout	Prio
All	<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

Save Reset

**Port:** The port number. “Port All” settings apply to all ports.

**LACP Enabled:** Enable LACP on a switch port.

**Key:** The “Auto” setting sets the key as appropriate by the physical link speed. Select “Specific” if you want a user-defined key value. The allowed key value range is 1~65535. Ports in an aggregated link group must have the same LACP port Key. In order to allow a port to join an aggregated group, the port Key must be set to the same value.

**Role:** The user can select either “Active” or “Passive” role depending on the device’s capability of negotiating and sending LACP control packets.

Ports that are designated as “Active” are able to process and send LACP control frames. Hence, this allows LACP compliant devices to negotiate the aggregated like so that the group may be changed dynamically as required. In order to add or remove ports from the group, at least one of the participating devices must set to “Active” LACP ports.

On the other hand, LACP ports that are set to “Passive” cannot send LACP control frames. In order to allow LACP-enabled devices to form a LACP group, one end of the connection must designate as “Passive” LACP ports.

**Timeout:** The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

**Prio:** The priority of the port. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

### 5.7.2.2 System Status

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

**Aggr ID:** Display the aggregation ID associated with the Link Aggregation Group (LAG).

**Partner System ID:** LAG’s partner system ID (MAC address).

**Partner Key:** The partner key assigned to this LAG.

**Partner Prio:** The priority value of the partner.

**Last Changed:** The time since this LAG changed.

**Local Ports:** The local ports that are a port of this LAG.

### 5.7.2.3 Port Status

LACP Status						
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	-	-	-	-	-

**Port:** The port number.

**LACP:** Show LACP status on a port.

**Yes:** LACP is enabled and the port link is up.

**No:** LACP is not enabled or the port link is down.

**Backup:** The port is in a backup role. When other ports leave LAG group, this port will join LAG.

**Key:** The aggregation key value on a port.

**Aggr ID:** Display the aggregation ID active on a port.

**Partner System ID:** LAG partner’s system ID.

**Partner Port:** The partner port connected to this local port.

**Partner Prio:** The priority value of the partner.



### 5.6.2.4 Port Statistics

LACP Statistics				
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

**Port:** The port number.

**LACP Received:** The number of LACP packets received on a port.

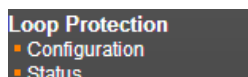
**LACP Transmitted:** The number of LACP packets transmitted by a port

**Discarded:** The number of unknown and illegal packets that have been discarded on a port.

## 5.8 Loop Protection

Loops sometimes occur in a network due to improper connecting, hardware problem or faulty protocol settings. When loops are seen in a switched network, they consume switch resources and thus downgrade switch performance. Loop Protection feature is provided in this switch and can be enabled globally or on a per port basis. Using loop protection enables the switch to automatically detect loops on a network. Once loops are detected, ports received the loop protection packet from the switch can be shut down or looped events can be logged.

In Loop Protection menu, you can select Configuration or Status.



### 5.8.1 Configuration

#### Loop Protection Configuration

**General Settings**

**Global Configuration**

Enable Loop Protection	Disable ▾
Transmission Time	5 seconds
Shutdown Time	180 seconds

**Port Configuration**

Port	Enable	Action	Tx Mode
All	<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 ▾
5	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
6	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
7	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
8	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
9	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
10	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾

**General Settings**

**Enable Loop Protection:** Enable or disable loop protection function.

**Transmission Time:** The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.

**Shutdown Time:** The period for which a port will be kept disabled. Valid values are 0 to 604800 seconds. 0 means that a port is kept disabled until next device restart.

**Port Configuration**

**Port:** List the number of each port. "All" settings apply to all ports.

**Enable:** Enable or disable the selected ports' loop protection function.

**Action:** When a loop is detected on a port, the loop protection will immediately take appropriate actions. Actions will be taken include "Shutdown Port", "Shutdown Port and Log" or "Log Only".

**Shutdown Port:** A loop-detected port is shutdown for a period of time configured in "Shutdown Time".

**Shutdown Port and Log:** A loop-detected port is shutdown for a period of time configured in "Shutdown Time" and the event is logged.

**Log Only:** The event is logged and the port remains enable.

**Tx Mode:** Enable or disable a port to actively generate loop protection PDUs or to passively look for looped PDUs.

**5.8.2 Status**

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

**Port:** The port number.

**Action:** Display the configured action that the switch will react when loops occur.

**Transmit:** Display the configured transmit (Tx) mode.

**Loops:** The number of loops detected on a port.

**Status:** The current loop status detected on a port.

**Loop:** Loops detected on a port or not.

**Time of Last Loop:** The time of the last loop event detected.

## 5.9 Spanning Tree

For some networking services, always-on connections are required to ensure that end users' online related activities are not interrupted due to unexpected disconnections. In these circumstances, multiple active paths between network nodes are established to prevent disconnections from happening. However, multiple paths interconnected with each other have a high tendency to cause bridge loops that make networks unstable and in worst cases make networks unusable. For example, the MAC address table used by the switch or bridge can fail, since the same MAC addresses (and hence the same network hosts) are seen on multiple ports. Second, a broadcast storm occurs. This is caused by broadcast packets being forwarded in an endless loop between switches. A broadcast storm can consume all available CPU resources and bandwidth.

To solve problems causing by bridge loops, spanning tree allows a network design to include redundant links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manually enabling/disabling these backup links.

The Spanning Tree Protocol (STP), defined in the IEEE Standard 802.1s, can create a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches) and disable the links which are not part of that tree, leaving a single active path between any two network nodes.

To provide faster spanning tree convergence after a topology change, an evolution of the Spanning Tree Protocol "Rapid Spanning Tree Protocol (RSTP)", is introduced by IEEE 802.1w. RSTP is a refinement of STP; therefore, it shares most of its basic operation characteristics. This essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it can make a rapid transition. This is one of the major elements which allows RSTP to achieve faster convergence times than STP.

The other extension of RSTP is IEEE 802.1s Multiple Spanning Tree protocol (MSTP) that allows different VLANs to travel along separate instances of spanning tree. Unlike STP and RSTP, MSTP eliminates the needs for having different STP for each VLAN. Therefore, in a large networking environment that employs many VLANs, MSTP can be more useful than legacy STP.

### 5.9.1 Bridge Settings

**STP Bridge Configuration**

**Basic Settings**

Protocol Version	MSTP ▼
Bridge Priority	32768 ▼
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

**Advanced Settings**

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	<input style="width: 100%;" type="text"/>

#### Basic Settings

**Protocol Version:** Select the appropriate spanning tree protocol. Protocol versions provided include "STP", "RSTP", and "MSTP".

**Bridge Priority:** Each switch has a relative priority and cost that is used to decide what the shortest path is to forward a packet. The lowest cost path (lowest numeric value) has a higher priority and is always used unless it is down. If you have

multiple bridges and interfaces then you need to adjust the priorities to achieve optimized performance. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

**Forward Delay:** For STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network. Valid values are 4-30 seconds.

**Max Age:** If another switch in the spanning tree does not send out a hello packet for a period of time, it is considered to be disconnected. Valid values are 6 to 40 seconds, and Max Age values must be smaller than or equal to  $(\text{Forward Delay} - 1) * 2$ .

**Maximum Hop Count:** The maximum number of hops allowed for MST region before a BPDU is discarded. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the BPDU is discarded. The default hop count is 20. The allowed range is 6-40.

**Transmit Hold Count:** The number of BPDU sent by a bridge port per second. When exceeded, transmission of the next BPDU will be delayed. By default, it is set to 6. The allowed transmit hold count is 1 to 10. Please note that increasing this value might have a significant impact on CPU utilization and decreasing this value might slow down convergence. It is recommended to remain Transmit Hold Count to the default setting.

### **Advanced Settings**

**Edge Port BPDU Filtering:** The purpose of Port BPDU Filtering is to prevent the switch from sending BPDU frames on ports that are connected to end devices.

**Edge Port BPDU Guard:** Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or mis-settings. When edge ports receive configuration BPDUs, they will be automatically set to non-edge ports and start a new spanning tree calculation process.

BPDU Guard is therefore used to prevent the device from suffering malicious attacks. With this function enabled, when edge ports receive configuration BPDUs, STP disables those affected edge ports. After a period of recovery time, those disabled ports are re-activated.

**Port Error Recovery:** When enabled, a port that is in the error-disabled state can automatically be enabled after a certain time.

**Port Error Recovery Timeout:** The time that has to pass before a port in the error-disabled state can be enabled. The allowed range is 30~86400 seconds.

### 5.9.2 MSTI Mapping

**MSTI Configuration**

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

**Configuration Identification**

Configuration Name	00-02-ab-03-fb-01
Configuration Revision	0

**MSTI Mapping**

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

#### Configuration Identification

**Configuration Name:** The name for this MSTI. By default, the switch's MAC address is used. The maximum length is 32 characters. In order to share spanning trees for MSTI, bridges must have the same configuration name and revision value.

**Configuration Revision:** The revision number for this MSTI. The allowed range is 0~65535.

#### MSTI Mapping

**MSTI:** MSTI instance number.

**VLAN Mapped:** Specify VLANs mapped to a certain MSTI. Both a single VLAN and a range of VLANs are allowed. Separate VLANs with a comma and use hyphen to denote a range of VLANs. (Example: 2,5,20-40) Leave the field empty for unused MSTI.

### 5.9.3 MSTI Priorities

**MSTI Configuration**

**MSTI Priority Configuration**

MSTI	Priority
All	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Save Reset

**MSTI:** Display MSTI instance number. “MSTI All” priority rule applies to all ports.

**Priority:** Select an appropriate priority for each MSTI instance. Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Note that lower numeric values indicate higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

### 5.9.4 CIST Ports

STP CIST Port Configuration										
CIST Aggregated Port Configuration										
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point	
-	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True	
CIST Normal Port Configuration										
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point	
All	<input type="checkbox"/>	<	<	<	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<	
1	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
2	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
3	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
4	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
5	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
6	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
9	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
10	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	

Save Reset

#### CIST Aggregated & Normal Port Configuration

**Port:** The port number.

**STP Enabled:** Enable STP function

**Path Cost:** Path cost is used to determine the best path between devices. If “Auto” mode is selected, the system automatically detects the speed and duplex mode to decide the path cost. Select “Specific”, if you want to use user-defined value. Valid values are 1 to 200000000. Please note that path cost takes precedence over port priority.

**Priority:** Select port priority.

**Admin Edge:** If an interface is attached to end nodes, you can set it to “Edge”.

**Auto Edge:** Select the checkbox to enable this feature. When enabled, a port is automatically determined to be at the edge of the network when it receives no BPDUs.

**Restricted Role:** If enabled, this 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.

**Restricted TCN:** If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

**BPDU Guard:** This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

**Point-to-Point:** Select the link type attached to an interface.

**Auto:** The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

**Forced True:** It is a point-to-point connection.

**Forced False:** It is a shared medium connection.

### 5.9.5 MSTI Ports

**MST1 MSTI Port Configuration**

**MSTI Aggregated Ports Configuration**

Port	Path Cost	Priority
-	Auto	128

**MSTI Normal Ports Configuration**

Port	Path Cost	Priority
All	<>	<>
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128
7	Auto	128
8	Auto	128
9	Auto	128
10	Auto	128

**Port:** The port number.

**Path Cost:** Path cost is used to determine the best path between devices. If “Auto” mode is selected, the system automatically detects the speed and duplex mode to decide the path cost. Select “Specific”, if you want to use user-defined value. Valid values are 1 to 200000000. Please note that path cost take precedence over port priority.

**Priority:** Select port priority.

### 5.9.6 Bridge Status

STP Bridges <span style="float: right;">Auto-refresh <input type="checkbox"/> Refresh</span>						
MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-02-AB-D6-68-B0	32768.00-02-AB-D6-68-B0	-	0	Steady	-

#### STP Bridge

**MSTI:** The bridge instance. Click this instance to view STP detailed bridge status.

**Bridge ID:** The unique bridge ID for this instance consisting a priority value and MAC address of the bridge switch.

**Root ID:** Display the root device’s priority value and MAC address.

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

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

**Topology Flag:** The current state of the Topology Change Notification flag for this bridge instance.

**Topology Change Last:** The time since this spanning tree was last configured.

**STP Detailed Bridge Status**

Click the MSTI instance to view STP detailed bridge status.

**STP Detailed Bridge Status**

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-02-AB-D6-68-B0
Root ID	32768.00-02-AB-D6-68-B0
Root Cost	0
Root Port	-
Regional Root	32768.00-02-AB-D6-68-B0
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

**CIST Ports & Aggregations State**

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
1	128.001	DesignatedPort	Forwarding	20000	Yes	Yes	0d 00:01:18
3	128.003	BackupPort	Discarding	20000	No	Yes	0d 00:01:18
5	128.005	DesignatedPort	Forwarding	200000	Yes	Yes	0d 00:01:39

**Bridge Instance:** The bridge instance.

**Bridge ID:** The unique bridge ID for this instance consisting a priority value and MAC address of the bridge switch.

**Root ID:** Display the root device’s priority value and MAC address.

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

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

**Regional Root:** The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (This parameter only applies to the CIST instance.)

**Internal Root Cost:** The Regional Root Path Cost. For the Regional Root Bridge the cost is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (This parameter only applies to the CIST instance.)

**Topology Flag:** The current state of the Topology Change Notification flag for this bridge instance.

**Topology Change Last:** The time since this spanning tree was last configured.

**CIST Ports & Aggregations State**

**Port:** Display the port number.

**Port ID:** The port identifier used by the RSTP protocol. This port ID contains the priority and the port number.

**Role:** The role assigned by Spanning Tree Algorithm. Roles can be “Designated Port”, “Backup Port”, “Root Port”.

**State:** Display the current state of a port.



**Blocking:** Ports only receive BPDU messages but do not forward them.

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

**Forwarding:** Ports forward packets and continue to learn addresses.

**Edge:** Display whether this port is an edge port or not.

**Point-to-Point:** Display whether this point is in point-to-point connection or not. This can be both automatically and manually configured.

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

### 5.9.7 Port Status

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

**Port:** The port number.

**CIST Role:** The role assigned by Spanning Tree Algorithm. Roles can be “Designated Port”, “Backup Port”, “Root Port” or “Non-STP”.

**CIST State:** Display the current state of a port. The CIST state must be one of the following:

**Discarding:** Ports only receive BPDU messages but do not forward them.

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

**Forwarding:** Ports forward packets and continue to learn addresses.

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

### 5.9.8 Port Statistics

STP Statistics										
Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	103	0	0	0	3	0	0	0	0
3	0	3	0	0	0	103	0	0	0	0
5	2228	114	0	0	0	0	0	0	0	0

**Port:** Display the port number.

**Transmitted & Received MSTP/RSTP/STP:** The number of MSTP/RSTP/STP configuration BPDU messages transmitted and received on a port.

**Transmitted & Received TCN:** The number of TCN messages transmitted and received on a port.

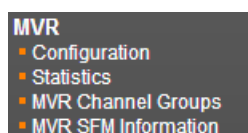
**Discarded Unknown/Illegal:** The number of unknown and illegal packets discarded on a port.

## 5.10 MVR

Multicast VLAN Registration protocol (MVR) allows a media server to transmit multicast stream in a single multicast VLAN when clients receiving multicast VLAN stream can reside in different VLANs. Clients in different VLANs intend to join or leave the multicast group simply by sending the IGMP Join or Leave message to a receiver port. The receiver port that belongs to one of the multicast groups can receive multicast stream from the media server.

MVR further isolates users who are not intended to receive multicast traffic and hence provide data security by VLAN segregation that allows only multicast traffic into other VLANs to which the subscribers belong. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).

The “MVR” menu contains the following sub menus.



### 5.10.1 Configuration

The screenshot shows the 'MVR Configurations' web page. At the top, there is a section for 'MVR Mode' with a dropdown menu set to 'Disabled'. Below this is the 'VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])' section, which contains a table with columns: Delete, MVR VID, MVR Name, Mode, Tagging, Priority, LLQI, and Interface Channel Setting. There is an 'Add New MVR VLAN' button below the table. The 'Immediate Leave Setting' section contains a table with columns: Port and Immediate Leave. The 'Port' column lists ports 1 through 10, and the 'Immediate Leave' column has a dropdown menu set to 'Disabled' for each port. At the bottom of the page, there are 'Save' and 'Reset' buttons.

#### MVR Configurations

**MVR Mode:** Enable or disable MVR feature globally on this device. Any multicast data from source ports will be sent to associated receiver ports registered in the table. By default, MVR feature is turned off.

#### VLAN Interface Setting

**MVR ID:** Specify multicast VLAN ID. Please note that MVR source ports are not recommended to be used as management VLAN ports. MVR source ports should be configured as members of the MVR VLAN, but MVR receiver ports should not be manually configured as members of this VLAN.

**MVR Name:** Optionally specify a user-defined name for this multicast VLAN. The maximum length of the MVR name string is 32. Both alphabets and numbers are allowed for use.

**Mode:** Two MVR operation modes are provided.


**Dynamic:** MVR allows dynamic MVR membership reports on source ports. (This is the default mode.)

**Compatible:** MVR membership reports are forbidden on source ports.

**Tagging:** Specify whether IGMP/MLD control frames will be sent tagged with MVR VID or untagged.

**Priority:** Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0~7.

**LLQI:** LLQI stands for Last Listener Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. By default, LLQI is set to 5 tenths of a second (0.5 second). The allowed range is 0~31744 tenths of a second.

**Interface Channel Profile:** Click the “Save” button before editing its Interface Channel Profile. Once “Save” is clicked, you are allowed to edit MVR channels of the selected IPMC profile settings by clicking the  button.

**Port Role:** Click the Port Role symbol to change the role status.

**Inactive (I):** By default, all ports are set to inactive. Inactive ports do not participate in MVR operations.

**Source (S):** Set a port (uplink ports) to source port. Source ports will receive and send multicast data. Subscribers can not directly be connected to source ports. Please also note that source ports cannot be management ports at the same time.

**Receiver (R):** Set a port to receiver port. Client or subscriber ports are configured to receiver ports so that they can issue IGMP/MLD messages to receive multicast data.

**Immediate Leave Setting**

**Port:** The port number.

**Immediate Leave:** Enable for disable immediate leave function. When enabled, the device immediately removes a port from a multicast stream as soon as it receives leave message for that group. This option only applies to an interface configured as MVR receivers.

Click the “Add New MVR VLAN” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

**MVR Channel Configuration**

Navigate Channel Setting with MVR VID  by  entries per page.

Delete	VLAN ID	VLAN Name	Start Address	End Address	Channel Name
<input type="button" value="Delete"/>	10	gold	<input type="text"/>	<input type="text"/>	<input type="text"/>

**VLAN ID:** Display the selected entry’s multicast VLAN ID. This field is not editable.

**VLAN Name:** Display the selected entry’s multicast VLAN Name. This field is not editable.

**Start Address:** Enter the starting IPv4 or IPv6 multicast streaming address that will be used as a streaming channel.

**End Address:** Enter the ending IPv4 or IPv6 multicast streaming address that will be used as a streaming channel.

**Channel Name:** Enter a descriptive name for this multicast VLAN. The maximum length of the channel name string is 32. Both alphabets and numbers are allowed but it should at least have one alphabet.

Click the “Add New MVR Channel” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.10.2 Statistics

MVR Statistics						
VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
10	0/0	0/0	0	0/0	0/0	0/0

This page displays MVR statistics information on queries, joins, reports and leaves messages.

**VLAN ID:** Display VLAN ID that is used for processing multicast traffic.

**IGMP/MLD Queries Received:** The number of received queries for IGMP and MLD.

**IGMP/MLD Queries Transmitted:** The number of transmitted queries for IGMP/MLD.

**IGMPv1 Joins Received:** The number of IGMPv1 received joins

**IGMPv2/MLDv1 Reports Received:** The number of IGMPv2 and MLDv1 received reports.

**IGMPv3/MLDv2 Reports Received:** The number of IGMPv3 and MLDv2 received reports.

**IGMPv2/MLDv1 Leaves Received:** The number of IGMPv2 and MLDv1 received leaves.

### 5.10.3 MVR Channel Groups

MVR Channels (Groups) Information												
Start from VLAN		1	and Group Address							with	20	entries per page.
		Port Members										
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	
No more entries												

Start from VLAN \_\_\_\_ and Group Address \_\_\_\_\_ with 20 entries per page.

This table displays MVR channels (groups) information and is sorted by VLAN ID.

**VLAN ID:** VLAN ID of the group.

**Groups:** Group ID

**Port Members:** Ports that belong to this group.

#### 5.10.4 MVR SFM Information

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

**VLAN ID:** VLAN ID of the group.

**Group:** The group address.

**Port:** Switch port number.

**Mode:** Indicate the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

**Source Address:** The source IP Address. Currently, the system limits the total number of source IP addresses for filtering to be 128. When there is no source filtering address, "None" is shown in the Source Address field.

**Type:** Indicate the Type. It can be either Allow or Deny.

**Hardware Filter/Switch:** Indicate whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

## 5.11 IPMC

The "IPMC" menu includes IGMP Snooping and MLD Snooping sub menu. Select the appropriate menu to set up detailed configurations.

### 5.11.1 IGMP Snooping

The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used more efficiently when supporting activities, such as, online streaming video and gaming.

IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 packets that IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch, it analyses all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch receives an IGMP report for a given multicast group from a host, the switch adds the host's port number to the multicast list for that group. When the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP snooping can reduce multicast traffic from streaming and other bandwidth intensive IP applications more effectively. A switch using IGMP snooping will only forward multicast traffic to the hosts in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also decreases the workload at the end hosts since their network cards (or operating system) will not receive and filter all the multicast traffic generated in the network.

### 5.11.1.1 Basic Configuration

The screenshot shows the IGMP Snooping Configuration web interface. It is divided into two main sections: Global Configuration and Port Related Configuration.

**Global Configuration:**

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 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:**

Port	Router Port	Fast Leave	Throttling
All	<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

At the bottom of the interface, there are 'Save' and 'Reset' buttons.

#### IGMP Snooping Configuration: Global Configuration

**Snooping Enabled:** Select the checkbox to globally enable IGMP Snooping feature. When enabled, this device will monitor network traffic and determine which hosts will receive multicast traffic. The switch can passively monitor or snoop on IGMP Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

**Unregistered IPMCv4 Flooding Enabled:** Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

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

**Proxy Enabled:** When enabled, the switch performs like “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006).

#### Port Related Configuration

**Port:** The port number. “All” rules apply to all ports.

**Router Port:** Select the checkbox on a given port to assign it as a router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

**Fast Leave:** Enable fast leave function if the checkbox is ticked. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

**Throttling:** This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. Other allowed options are 1~10

### 5.11.1.2 VLAN Configuration

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)
Delete		<input type="checkbox"/>	<input checked="" type="checkbox"/>	IGMP-Auto	2	125	100	10	1

Add New IGMP VLAN

Save Reset

This page is used to configure IGMP Snooping for an interface.

**VLAN ID:** Specify VLAN ID for IGMP snooping.

**Snooping Enabled:** Select the checkbox to enable snooping feature on an interface basis. When enabled, the switch will monitor network traffic on the specified interface to determine which hosts want to receive multicast services. If IGMP snooping is enabled globally and an interface's IGMP snooping is enabled on an interface, IGMP snooping on an interface will take precedence. When disabled, snooping can still be configured on an interface. However, settings will only take effect until IGMP snooping is enabled globally.

**Querier Election:** Enable to join querier election in the VLAN. When disabled, it will act as an IGMP non-querier.

**Querier Address:** Specify the IPv4 source address used in IP header for IGMP querier election. When the field is not specified, the switch uses the first available IPv4 management address of the IP interface associated with this VLAN.

**Compatibility:** This configures how hosts and routers take actions within a network depending on IGMP version selected. Available options are "IGMP-Auto", "Forced IGMPv1", "Forced IGMPv2", "Forced IGMPv3". By default, IGMP-Auto is used.

**RV:** The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

**QI (sec):** The Query Interval is the interval between IGMP General Query messages sent by the Querier. The default Querier Interval is 125 seconds.

**QRI:** The Query Response Interval is the maximum amount of time that the IGMP router waits to receive a response to a General Query message. The QRI applies when the switch is acting as the querier and is used to inform other devices of the maximum time this system waits for a response to general queries. By default, RQI is set to 10 seconds. The allowed range is 10~31744 tenths of a second.

**LLQI:** The Last Listener Query Interval sets the interval that waits for a response to a group-specific or group-and-source specific query message.

**URI:** The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. By default, URI is set to 1 second. The allowed range for URI is 0~31744 seconds.

Click the "Add New IGMP VLAN" button to add a new entry.

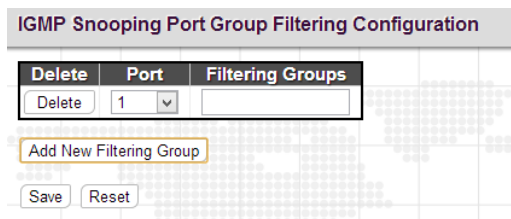
Click the "Delete" button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the "Save" button to save settings or changes.

Click the "Reset" button to restore changed settings to the default settings.

### 5.11.1.3 Port Group Filtering

The Port Filtering Configuration page is to filter specific multicast traffic on a per port basis. Before you select a filtering profile for filtering purposes, you must set up profiles in IPMC Profile page.



**Port:** The port number.

**Filtering Profile:** Enter multicast group address for filtering on a port. When a certain multicast group is specified on a port, IGMP join reports received on a port will be dropped.

Click the “Add New Filtering Group” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.11.1.4 Status

IGMP Snooping Status									
Statistics									
VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
Router Port									
Port	Status								
1	-								
2	-								
3	-								
4	-								
5	-								
6	-								
7	-								
8	-								
9	-								
10	-								

#### Statistics

**VLAN ID:** The VLAN ID of this entry.

**Querier Version:** The current working Querier version.

**Host Version:** The current host version.

**Querier Status:** Show the Querier status that is either "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

**Queries Transmitted:** The number of queries transmitted.

**Queries Received:** The number of queries received.

**V1 Reports Received:** The number of Received V1 Reports.



**V2 Reports Received:** The number of Received V2 Reports.

**V2 Leaves Received:** The number of Received V2 Leaves.

**Router Port**

**Port:** The port number.

**Status:** Indicate whether a specific port is a router port or not.

**5.11.1.5 Groups Information**

IGMP Snooping Group Information											
Start from VLAN <input type="text" value="1"/> and group address <input type="text" value="224.0.0.0"/> with <input type="text" value="20"/> entries per page.											
		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
No more entries											

**VLAN ID:** Display the VLAN ID of the group.

**Groups:** Display the group address.

**Port Members:** Ports that belong to this group.

**5.11.1.6 IPv4 SFM Information**

IGMP SFM Information						
Start from VLAN <input type="text" value="1"/> and Group <input type="text" value="224.0.0.0"/> with <input type="text" value="20"/> entries per page.						
VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

**VLAN ID:** Display the VLAN ID of the group.

**Groups:** Display the IP address of a multicast group.

**Port:** The switch port number.

**Mode:** The filtering mode maintained per VLAN ID, port number and group address.

**Source Address:** The source IP address available for filtering.

**Type:** Display either Allow or Deny type.

**Hardware Filter/Switch:** Indicates whether the data plane destined to the specific group address from the source IPv4 address can be handled by the chip or not.

### 5.11.2 MLD Snooping

Multicast Listener Discovery (MLD) snooping, similar to IGMP snooping for IPv4, operates on IPv6 for multicast traffic. In other words, MLD snooping configures ports to limit or control IPv6 multicast traffic so that multicast traffic is forwarded to ports (or users) who want to receive it. In this way, MLD snooping can reduce the flooding of IPv6 multicast packets in the specified VLANs. Please note that IGMP Snooping and MLD Snooping are independent of each other. They can both be enabled and function at the same time.

#### 5.11.2.1 Basic Configuration

Port	Router Port	Fast Leave	Throttling
All	<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

#### Global Configuration

**Snooping Enabled:** Select the checkbox to globally enable MLD Snooping feature. When enabled, this device will monitor network traffic and determine which hosts would like to receive multicast traffic. The switch can passively monitor or snoop on MLD Listener Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

**Unregistered IPMCv6 Flooding Enabled:** Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

**MLD SSM Range:** SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

**Leave Proxy Enabled:** To prevent multicast router from becoming overloaded with leave messages, MLD snooping suppresses leave messages unless received from the last member port in the group. When the switch acts as the querier, the leave proxy feature will not function.

**Proxy Enabled:** When MLD proxy is enabled, the switch exchanges MLD messages with the router on its upstream interface, and performs the host portion of the MLD task on the upstream interface as follows:

- When queried, it sends multicast listener reports to the group.
- When a host joins a multicast group to which no other host belongs, it sends unsolicited multicast listener reports to that group.
- When the last host in a particular multicast group leaves, it sends an unsolicited multicast listener done report to the all-routers address (FF02::2) for MLDv1.

#### Port Related Configuration

**Port:** List each port number. "All" rules apply to all ports.

**Router Port:** Select the checkbox on a given port to assign it as a router port. If MLD snooping cannot locate the MLD querier, you can manually designate a port which is connected to a known MLD querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

**Fast Leave:** Enable fast leave function if the checkbox is ticked. When a leave packet is received, the switch immediately removes it from a multicast service without sending a MLD group-specific (GS) query to that interface.

**Throttling:** This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new MLD join reports will be dropped. By default, unlimited is selected. Other allowed options are 1~10.

### 5.11.2.2 VLAN Configuration

This page is used to configure MLD Snooping for an interface.

**VLAN ID:** Specify VLAN ID for MLD snooping.

**Snooping Enabled:** Select the checkbox to enable snooping feature on an interface basis. When enabled, the switch will monitor network traffic on the specified interface to determine which hosts want to receive multicast services.

**MLD Querier:** Enable to join querier election in the VLAN. When enabled, the switch can serve as the MLDv2 querier in the bidding process with other competing multicast routers or switches. Once it becomes querier, it will be responsible for asking hosts periodically if they want to receive multicast traffic. When disabled, it will act as an IGMP non-querier.

**Compatibility:** This configures how hosts and routers take actions within a network depending on MLD version selected. Available options are “MLD-Auto”, “Forced MLDv1” and “Forced MLDv2”. By default, MLD-Auto is used.

**RV:** The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2. The allowed range is 1~255.

**QI (sec):** The Query Interval is the interval between IGMP General Query messages sent by the Querier. The default Querier Interval is 125 seconds. The allowed interval range is 1~255 seconds.

**QRI:** The Query Response Interval is the maximum amount of time that the IGMP router waits to receive a response to a General Query message. The QRI applies when the switch is acting as the querier and is used to inform other devices of the maximum time this system waits for a response to general queries. By default, RQI is set to 10 seconds. The allowed range is 10 – 31744 tenths of a second.

**LLQI:** The Last Listener Query Interval sets the interval that waits for a response to a group-specific or group-and-source specific query message.

**URI:** The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. By default, URI is set to 1 second. The allowed range for URI is 0~31744 seconds.

Click the “Add New MLD VLAN” button to add a new entry.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.11.2.3 Port Group Filtering

**Port:** Select a port number to be used for this rule.

**Filtering Profile:** Enter multicast group address for filtering on a port. When a certain multicast group is specified on a port, MLD join reports received on a port will be dropped.

### 5.11.2.4 Status

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-

#### Statistics

**VLAN ID:** The VLAN ID of this entry.

**Querier Version:** The current working Querier version.

**Host Version:** The current host version.

**Querier Status:** Show the Querier status that is either "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

**Queries Transmitted:** The number of queries transmitted.

**Queries Received:** The number of queries received.

**V1 Reports Received:** The number of Received V1 Reports.

**V2 Reports Received:** The number of Received V2 Reports.

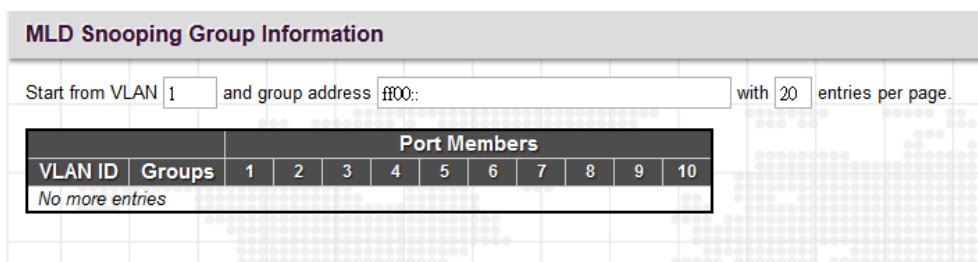
**V1 Leaves Received:** The number of Received V1 Leaves.

**Router Port**

**Port:** The port number.

**Status:** Indicate whether a specific port is a router port or not.

**5.11.2.5 Groups Information**

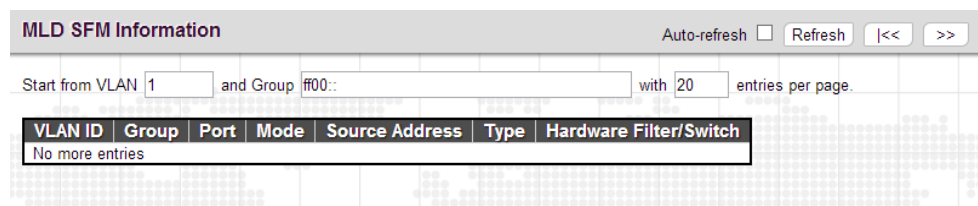


**VLAN ID:** Display the VLAN ID of the group.

**Groups:** Display the group address.

**Port Members:** Ports that belong to this group.

**5.11.2.6 IPv6 SFM Information**



**VLAN ID:** Display the VLAN ID of the group.

**Group:** Display the IP address of a multicast group.

**Port:** The switch port number.

**Mode:** The filtering mode maintained per VLAN ID, port number and group address.

**Source Address:** The source IP address available for filtering.

**Type:** Display either Allow or Deny type.

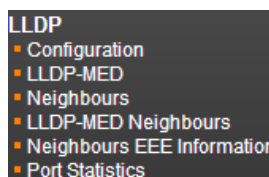
**Hardware Filter/Switch:** Indicates whether the data plane destined to the specific group address from the source IPv4 address can be handled by the chip or not.

**5.12 LLDP**

LLDP (Link Layer Discovery Protocol) runs over data link layer which is used for network devices to send information about themselves to other directly connected devices on the network. By using LLDP, two devices running different network layer protocols can learn information about each other. A set of attributes referred to TLVs are used to discover

neighbour devices. Details such as port description, system name, system description, system capabilities, management address can be sent and received on this device.

The “LLDP” menu contains the following sub menus. Select the appropriate menu to set up detailed configurations.



### 5.12.1 Configuration

**LLDP Configuration**

**LLDP Parameters**

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

**LLDP Port Configuration**

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
All	<>	<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"/>

Save Reset

#### LLDP Parameters

**Tx Interval:** Specify the interval between LLDP frames are sent to its neighbours for updated discovery information. The valid values are 5~32768 seconds. The default is 30 seconds.

**Tx Hold:** This setting defines how long LLDP frames are considered valid and is used to compute the TTL. Valid range is 2~10 times. The default is 4.

**Tx Delay:** Specify a delay between the LLDP frames that contain changed configurations. Tx Delay cannot be larger than 1/4 of the Tx interval value. The valid values are 1 - 8192 seconds.

**Tx Reinit:** Specify a delay between the shutdown frame and a new LLDP initialization. The valid values are 1~10 seconds.

#### LLDP Port Configuration

**Port:** The port number. “All” settings apply to all ports.

**Mode:** Select the appropriate LLDP mode.

**Disabled:** LLDP information will not be sent and LLDP information received from neighbours will be dropped.

**Enabled:** LLDP information will be sent and LLDP information received from neighbours will be analyzed.

**Rx Only:** The switch will analyze LLDP information received from neighbours.

**Tx Only:** The switch will send out LLDP information but will drop LLDP information received from neighbours.

**CDP Aware:** CDP aware operation is used to decode incoming CDP (Cisco Discovery Protocol) frames. If enabled, CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded, all others are discarded. CDP TLVs are mapped into LLDP neighbors table as shown below:

**Optional TLVs:** LLDP uses several attributes to discover neighbour devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent from this device. Uncheck the boxes if they are not appropriate to be known by other neighbour devices.

### 5.12.2 LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.

**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 LLDP 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. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a 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 between Network Connectivity Devices, or to 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 to either East of the prime meridian or West of the prime meridian.

**Altitude:** Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters).

**Meters:** Representing meters of Altitude defined by the vertical datum specified.

**Floors:** Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

**Map Datum:** The Map Datum is used for the coordinates given in these options:

**WGS84:** (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

**NAD83/NAVD88:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

**NAD83/MLLW:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

### **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 (Neighbourhood):** Neighbourhood, block.

**Street:** Street - Example: Poppelvej.

**Leading street direction:** Example: N.

**Trailing street suffix:** Example: SW.

**Street suffix:** Example: Ave, Platz.

**House no.:** Example: 21.

**House no. suffix:** Example: A, 1/2.

**Landmark:** Landmark or vanity address - Example: Columbia University.

**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:** Example: 4.

**Room no.:** Room number - Example: 450F.

**Place type:** Example: Office.



**Postal community name:** Example: Leonia.

**P.O. Box:** Example: 12345.

**Additional code:** Example: 1320300003.

**Emergency Call Service**

**Emergency Call Service:** Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

**Policies**

**Policy ID:** Specify the ID for this policy.

**Application Type:** The application types include “Voice”, “Voice Signalling”, “Guest Voice”, “Guest Voice Signalling”, “Softphone Voice”, “Video Conferencing”, “Streaming”, “Video Signalling”.

**Tag:** Tag indicating whether the specified application type is using a “tagged” or an “untagged” VLAN.

**VLAN ID:** Specify the VLAN ID for the port.

**L2 Priority:** Specify one of eight priority levels (0-7) as defined by 802.1D-2004.

**DSCP:** Specify one of 64 code point values (0-63) as defined in IETF RFC 2474.

Click the “Add New Policy” button to insert a new policy to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

**5.12.3 Neighbours**

LLDP Neighbour Information						
Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 2	00-1D-60-BC-26-D3	00-1D-60-BC-26-D3				

**Local Port:** The local port that a remote LLDP-capable device is attached.

**Chassis ID:** An ID indicating the particular chassis in this system.

**Remote Port ID:** A remote port ID that LDPDUs were transmitted.

**System Name:** The system name assigned to the remote system.

**Port Description:** A remote port's description.

**System Capabilities:** This shows the neighbour unit's capabilities. When a capability is enabled, the capability is followed by (+). If disabled, the capability is followed by (-).

**Management Address:** The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. If the neighbor device allows management access, clicking on an entry in this field will re-direct the web browser to the neighbor's management interface.

### 5.12.4 LLDP-MED Neighbours

LLDP-MED Neighbour Information			
Port 2			
Device Type	Capabilities		
Endpoint Class I	LLDP-MED Capabilities		
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities	MAU Type
Supported	Enabled	1000BASE-T full duplex mode	Invalid MAU Type

This page displays information about LLDP-MED neighbours detected on the network.

### 5.12.5 Neighbours EEE Information

LLDP Neighbors EEE Information									
								Auto-refresh <input type="checkbox"/>	Refresh
Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync	
No LLDP EEE information found									

**Local Port:** The port for this switch on which the LLDP frame was received.

**Tx Tw:** The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.

**Rx Tw:** The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

**Fallback Receive Tw:** The link partner's fallback receive Tw.

**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.

**Resolved Rx Tw:** The resolved Rx Tw for this link.

**EEE in Sync:** This shows whether the switch and the link partner have agreed on wake times.

**Red:** Switch and link partner have not agreed on wakeup times.

**Green:** Switch and link partner have agreed on wakeup times.

### 5.12.6 Port Statistics

Global Counters	
Neighbour entries were last changed 2013-07-01T00:02:11+00:00 (2540 sec. ago)	
Total Neighbours Entries Added	1
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	87	8	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

#### Global Counters

**Total Neighbours Entries Added:** Shows the number of new entries added since the switch was rebooted, and for which the remote TTL has not yet expired.

**Total Neighbors Entries Deleted:** The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.

**Total Neighbors Entries Dropped:** The number of times which the remote database on this switch dropped an LLDPDU because the entry table was full.

**Total Neighbors Entries Aged Out:** The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

#### LLDP Statistics Local Counters

**Local Port:** The port number.

**Tx Frames:** The number of LLDP PDUs transmitted.

**Rx Frames:** The number of LLDP PDUs received.

**Rx Errors:** The number of received LLDP frames with some kind of error.

**Frames Discarded:** The number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular Type Length Value (TLV).

**TLVs Discarded:** Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded.

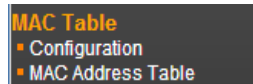
**TLVs Unrecognized:** The number of well-formed TLVs, but with an unknown type value.

**Org. Discarded:** The number of organizational TLVs discarded.

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

## 5.13 MAC Table

The “MAC Table” menu contains configuration and status sub menu. Select the configuration page to set up detailed configuration



### 5.13.1 Configuration

#### MAC Address Table Configuration

##### Aging Configuration

Disable Automatic Aging

Aging Time  seconds

##### MAC Table Learning

Port Members										
	1	2	3	4	5	6	7	8	9	10
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

##### Static MAC Table Configuration

			Port Members									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10
<input type="button" value="Add New Static Entry"/>												
<input type="button" value="Save"/> <input type="button" value="Reset"/>												

**Disable Automatic Aging:** Learned MAC addresses will appear in the table permanently.

**Aging Time:** Set up the aging time for a learned MAC to be appeared in MAC learning table. The allowed range is 10 to 1000000 seconds.

**MAC Learning Table:** Three options are available on each port.

**Auto:** On a given port, learning is automatically done once unknown SMAC is received.

**Disable:** Disable MAC learning function.

**Secure:** Only static MAC entries listed in “Static MAC Table Configuration” are learned. Others will be 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:** This table is used to manually set up static MAC entries. The total entries that can be entered are 64.

**VLAN ID:** Specify the VLAN ID for this entry.

**MAC Address:** Specify the MAC address for this entry.

**Port Members:** Check or uncheck the ports. If the incoming packet has the same destination MAC address as the one specified in VID, it will be forwarded to the checked port directly.

Click the “Add New Static Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.13.2 MAC Address Table

The MAC Address Table shows both static and dynamic MAC addresses learned from CPU or switch ports. You can enter the starting VLAN ID and MAC addresses to view the desired entries.

The screenshot shows the 'MAC Address Table' interface. At the top, there are search filters: 'Start from VLAN' set to 1, 'and MAC address' set to 00-00-00-00-00-00, and 'with 20 entries per page'. Below the filters is a table with the following data:

Type	VLAN	MAC Address	CPU	Port Members																
				1	2	3	4	5	6	7	8	9	10							
Static	1	00-02-AB-0D-FB-01	✓																	
Dynamic	1	00-1D-60-BC-26-D3		✓																
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-0D-FB-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-AB-00-10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

**Type:** Display whether the learned MAC address is static or dynamic.

**VLAN ID:** The VLAN ID associated with this entry.

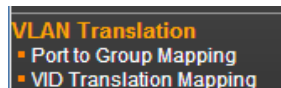
**MAC Address:** The MAC address learned on CPU or certain ports.

**Port Members:** Ports associated with this entry.

## 5.14 VLAN Translation

VLAN Translation is especially useful for users who want to translate the original VLAN ID to a new VLAN ID so as to exchange data across different VLANs and improve VLAN scaling. VLAN translation replaces an incoming C-VLAN tag with an S-VLAN tag instead of adding an additional tag. When configuring VLAN Translation, both ends of the link normally must be able to replace tags appropriately. In other words, both ends must be configured to translate the C-VLAN tag to S-VLAN tag and S-VLAN tag to C-VLAN tag appropriately in a network. Note that only access ports support VLAN translation. It is not recommended to configure VLAN Translation on trunk ports.

The “VLAN Translation” menu contains the following sub menus. Select the appropriate one to configure settings or view its status.



### 5.14.1 Port to Group Mapping

Port to Group mapping Table

Group ID	Port Members									
	1	2	3	4	5	6	7	8	9	10
10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Add New Entry

Save Reset

**Group ID:** The total VLAN Translation group can be used is 11 which is automatically created in Group Mapping Table when entering “Port to Group Mapping” page. A port can be mapped to any of the groups. Multiple ports can be mapped to a single group with the same Group ID.

**Note:** By default, each port is mapped to a group with a group ID equal to the port number. For example, port 2 is mapped to the group with ID is 2.

**Port Number:** Click the appropriate radio button to include a port into a group.

### 5.14.2 VID Translation Mapping

VLAN Translation Table

Delete	Group ID	VLAN ID	Translated to VID
<input type="button" value="Delete"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Add New Entry

Save Reset

**Group ID:** Indicate the Group ID that applies to this translation rule.

**VLAN ID:** Indicate the VLAN ID that will be mapped to a new VID.

**Translated to VID:** Indicate the new VID to which VID of ingress frames will be changed.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

## 5.15 VLANs

IEEE 802.1Q VLAN (Virtual Local Area Network) is a popular and cost-effectively way to segment your networking deployment by logically grouping devices with similar attributes irrespective of their physical connections. VLANs also segment the network into different broadcast domains so that packets are forwarded to ports within the VLAN that they belong. Using VLANs provides the following main benefits:

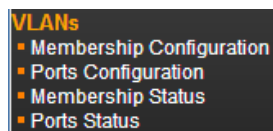
**VLANs provide extra security:** Devices that frequently communicate with each other are grouped into the same VLAN. If devices in a VLAN want to communicate with devices in a different VLAN, the traffic must go through a routing device or Layer 3 switching device.

**VLANs help control traffic:** Traditionally, when networks are not segmented into VLANs, congestion can be easily caused by broadcast traffic that is directed to all devices. To minimize the possibility of broadcast traffic damaging

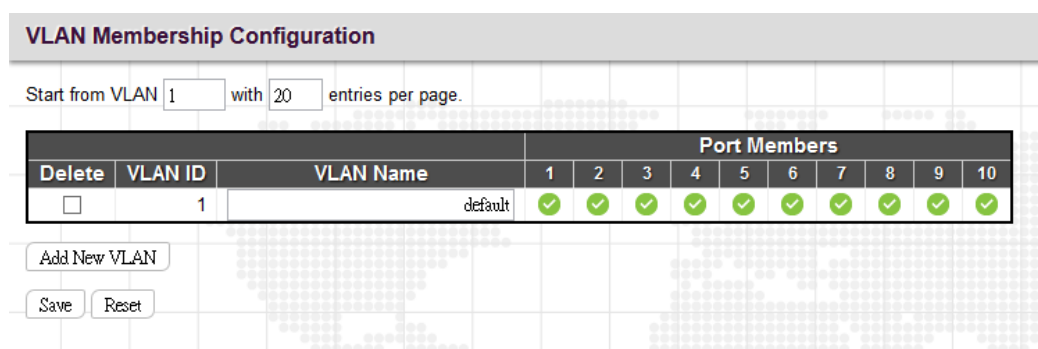
the entire network, VLANs can help group devices that communicate frequently with other in the same VLAN so as to divide the entire network into several broadcast domains.

VLANs make changes of devices or relocation more easily: In traditional networks, when moving a device geographically to a new location (for example, move a device in floor 2 to floor 4), the network administrator may need to change the IP or even subnet of the network or require re-cabling. However, by using VLANs, the original IP settings can remain the same and re-cabling can be reduced to minimal.

The “VLAN” menu contains the following sub menus. Select the appropriate one to set up the detailed configurations.



### 5.15.1 Membership Configuration



This configuration page is used to set up and modify VLAN membership. By default, the configuration page shows 20 VLAN entries. However, you can change the starting VLAN and the total of VLAN membership information shown on this page by using “Start from VLAN \_\_\_ with \_\_\_ entries per page” setting. Up to 4096 VLANs are supported on this Switch.

By default, all ports belong to “default” VLAN with VLAN ID=1.

**VLAN ID:** Specify the VLAN ID. Valid values are 1 to 4095.

**VLAN Name:** Provide a description or a name for this VLAN. This field can be left blank. Both alphabets and numbers are allowed. However, if you want to input a description or name, make sure that the field is entered with at least one alphabet. The maximum length of the VLAN Name string is 32.

**Port Members:**

To include a port in a VLAN, check the box as

To include a port in a forbidden port list, check the box as

To remove or exclude the port from the VLAN, make sure the box is unchecked

By default, no ports are members, and for every new VLAN entry all boxes are unchecked.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

5.15.2 Ports Configuration

Ethertype for Custom S-ports 0x88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
All	<input type="text" value=""/>	<input type="checkbox"/>	<input type="text" value=""/>	<input type="text" value=""/>	1	<input type="text" value=""/>
1	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
2	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
3	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
4	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
5	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
6	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
7	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
8	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
9	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
10	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid

Save Reset

**Ethertype for Custom S-ports:** Specify ether type used for customer s-ports.

**VLAN Port Configuration**

**Port:** The port number. "All" settings apply to all ports.

**Port Type:** There are four port types available. Each port type's ingress and egress action is described in the following table.

Action Port Type	Ingress Action	Egress Action
Unaware	When a tagged frame is received on a port, 1. If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing are also affected by egress rule.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
C-port	When a tagged frame is received on a port, 1. If a tagged frame with TPID=0x8100, it is forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by C-port will be set to 0x8100.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-port	When a tagged frame is received on a port, 1. If a tagged frame with TPID=0x88AA, it is forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TPID of frame transmitted by S-port will be set to 0x88A8
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-custom port	When a tagged frame is received on a port, 1. If a tagged frame with TPID=0x88AA, it is forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TPID of frame transmitted by S-custom-port will be set to a self-customized value, which can be set by the user using the column of EtherType for Custom S-ports.
	When an untagged frame is received on a port, a tag (PVID) is attached and then forwarded.	



**Ingress Filtering:** If Ingress Filtering is enabled and the ingress port is not a member of a VLAN, the frame from the ingress port is discarded. By default, ingress filtering is disabled.

**Frame Type:** Select the accepted frame types. Available options include All (accept all frames), Tagged (accept only tagged frames), Untagged (accept only 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, frame type is set to All.

**Port VLAN:** Configures the VLAN identifier for the port. The allowed values are from 1 through 4095. The default value is 1. Note: The port must be a member of the same VLAN as the Port VLAN ID.

**Tx Tag:** Determines egress tagging of a port. Untag\_pvid - All VLANs except the configured PVID will be tagged. Tag\_all - All VLANs are tagged. Untag\_all - All VLANs are untagged.

### 5.15.3 Membership Status

VLAN Membership Status for Combined users										
Start from VLAN <input type="text" value="1"/> with <input type="text" value="20"/> entries per page. <input type="button" value="k&lt;"/> <input type="button" value="&gt;&gt;"/>										
Port Members										
VLAN ID	1	2	3	4	5	6	7	8	9	10
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

This page shows the current VLAN membership saved on the Switch.

**VLAN ID:** VLANs that are already created.

**Port members:** Display member ports on the configured VLANs.

### 5.15.4 Port Status

VLAN Port Status for Static user							
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

This page shows the current VLAN settings on a per-port basis saved on the Switch.

**Port:** The port number.

**PVID:** The port VLAN ID assigned to a port.

**Port Type:** Display the selected port type on a port.

**Ingress Filtering:** Display whether Ingress Filtering is enabled or disabled.

**Frame Type:** Display the accepted frame type on a port.

**Tx Tag:** Display the Egress action on a port.

**UVID:** Display the untagged VLAN ID. A port's UVID determines the packet's behavior at the egress side. If the VID of

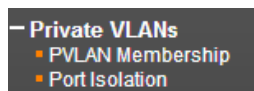
Ethernet frames leaving a port match the UVID, these frames will be sent untagged.

**Conflicts:** Display whether conflicts exist or not. When a software module requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

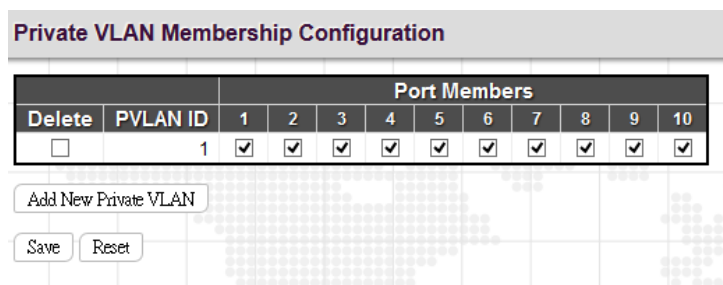
- \*Functional conflicts between features.
- \*Conflicts due to hardware limitations.
- \*Direct conflicts between user modules.

## 5.16 Private VLANs

The “Private VLANs” menu contains the following sub menus. Select the appropriate one to configure its detailed settings.



### 5.16.1 PVLAN Membership



This page is used to configure private VLANs. New Private VLANs can be added here and existing VLANs can be modified. Private VLANs are based on the source port mask and there are no connections to VLANs which 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.

**PVLAN ID:** Specify the PVLAN ID. Valid values are 1 to 4095.

**Port Members:** Select the checkbox, if you would like a port to belong to a certain Private VLAN. Uncheck the checkbox to remove a port from a Private VLAN.

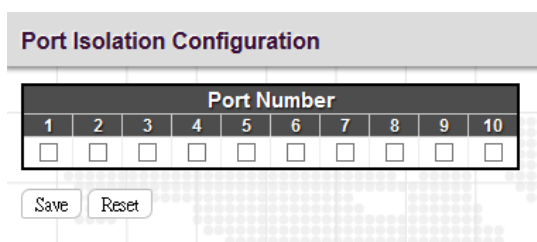
Click the “Add New Private VLAN” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.16.2 Port Isolation

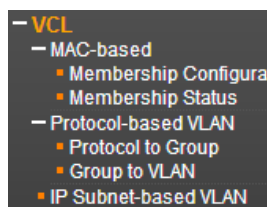


Private VLAN is used to group ports together so as to prevent communications within PVLAN. Port Isolation is used to prevent communications between customer ports in a same Private VLAN. The port that is isolated from others cannot forward any unicast, multicast or broadcast traffic to any other ports in the same PVLAN.

**Port Number:** Select the checkbox if you want a port or ports to be isolated from other ports.

## 5.17 VCL

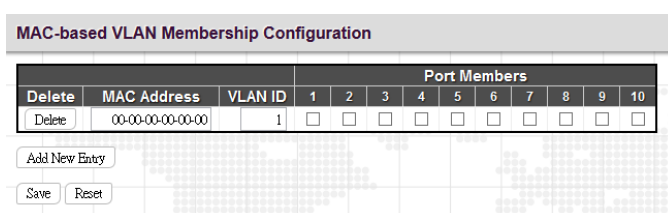
The “VCL” menu contains the following sub menus.



### 5.17.1 MAC-based

MAC-based VLAN configuration page is to set up VLANs based on source MAC addresses. When ingress untagged frames are received by a port, source MAC address is processed to decide which VLAN these untagged frames belong. When source MAC addresses does not match the rules created, untagged frames are assigned to the receiving port’s native VLAN ID (PVID).

#### 5.17.1.1 Membership Configuration



**MAC Address:** Indicate the source MAC address. Please note that the source MAC address can only map to one VLAN ID.

**VLAN ID:** Map this MAC address to the associated VLAN ID.

**Port Members:** Ports that belong to this VLAN.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.17.1.2 Membership Status

MAC-based VLAN Membership Status for User Static											
MAC Address	VLAN ID	Port Members									
		1	2	3	4	5	6	7	8	9	10
No data exists for the user											

This page shows the status of current VCL rules.

**MAC Address:** Display the configured MAC addresses.

**VLAN ID:** Display the VLAN ID of this membership entry.

**Port Members:** Display ports that accept the configured MAC address.

### 5.17.2 Protocol-based VLAN

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

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

#### 5.17.2.1 Protocol to Group

**Protocol to Group Mapping Table**

Delete	Frame Type	Value		Group Name
Delete	Ethernet	Etype: 0x0800		

Add New Entry

Save Reset

**Protocol to Group Mapping Table**

Delete	Frame Type	Value		Group Name
Delete	SNAP	OUI: 0x00-E0-2B	PID: 0x0001	

Add New Entry

Save Reset

**Protocol to Group Mapping Table**

Delete	Frame Type	Value		Group Name
Delete	LLC	DSAP: 0xFF	SSAP: 0xFF	

Add New Entry

Save Reset

**Frame Type:** There are three frame types available for selection; these are “Ethernet”, “SNAP”, and “LLC”. The value field will change accordingly.

**Value:** This field specifically indicates the protocol type. This value field varies depending on the frame type you selected.

**Ethernet:** Ether Type (etype) value. By default, it is set to 0x0800. The range allowed is 0x0600 to 0xffff.

**SNAP:** This includes OUI (Organizationally Unique Identifier) and PID (Protocol ID) values.

**OUI:** A value in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value in the ranges of 0x00-0xff.

**PID:** If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type field value for the protocol running on top of SNAP. If the OUI is that of 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 the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

**LLC (Logical Link Control):** This includes DSAP (Destination Service Access Point) and SSAP (Source Service Access Point) values. By default, the value is 0xff. Valid range is 0x00 to 0xff.

**Group Name:** Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

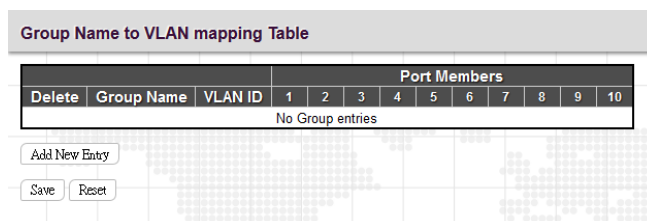
Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.17.2.2 Group to VLAN



**Group Name:** Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

**VLAN ID:** Indicate the VLAN ID.

**Port Members:** Assign ports to this rule.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

### 5.17.3 IP Subnet-based VLAN

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

IP Subnet-based VLAN Membership Configuration					Port Members									
Delete	VCE ID	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10
Delete	0	0.0.0.0	24	1	<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"/>

**VCE ID:** Index of the entry. Valid range is 0-256.

**IP Address:** Indicate the IP address for this rule.

**Mask Length:** Indicate the network mask length.

**VLAN ID:** Indicate the VLAN ID

**Port Members:** Assign ports to this rule.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

## 5.18 Voice VLAN

Nowadays, in the enterprise network, VoIP devices are commonly deployed to save operational cost due to its easy-to-setup feature and convenience. However, while deploying VoIP devices, it is recommended that VoIP traffic is separated from data traffic. By isolating traffic, VoIP traffic can be assigned to have the highest priority while forwarding so that higher voice quality can be achieved without encountering situations like excessive packet delays, packet loss, and jitters. Moreover,

This switch provides Voice VLAN feature that enables voice traffic to be forwarded on the voice VLAN. The user can also overwrite traffic priority by assigning higher traffic class value to voice traffic. Voice traffic can be detected on a port by using LLDP (IEEE 802.1ab) to discover VoIP devices attached to the switch or from devices' OUI (Organizationally Unique Identifier). When voice packets are detected on a port, the switch automatically assigns the port as a tagged member of the Voice VLAN and forward packets based on configurations set in Voice VLAN configuration page.

The Voice VLAN section provides that following two sub menus:

- Voice VLAN
  - Configuration
  - OUI

### 5.18.1 Configuration

**Voice VLAN Configuration**

<b>Mode</b>	Disabled
<b>VLAN ID</b>	1000
<b>Aging Time</b>	86400 seconds
<b>Traffic Class</b>	7 (High)

**Port Configuration**

Port	Mode	Security	Discovery Protocol
All	◊	◊	◊
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

#### Voice VLAN Configuration

**Mode:** Enable or disable Voice VLAN function on this switch.

**VLAN ID:** Assign a VLAN ID to this Voice VLAN. Only one Voice VLAN is supported on the switch. By default, VLAN 1000 is set. The allowed range is 1~4095.

---

**Note:**

1. The Voice VLAN cannot be the same as management VLAN, MVR VLAN, or the native VLAN assigned to any port.
  2. MSTP must be disabled before the Voice VLAN is enabled or the Voice VLAN port mode is set to Auto or Forced. This prevents the spanning tree's ingress filter from dropping VoIP traffic tagged for the Voice VLAN.
- 

**Aging Time:** The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. By default, the aging time is set to 86400 seconds. The allowed aging time is 10 – 10,000,000 seconds.

**Traffic Class:** Select the traffic class value which defines a service priority for traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new traffic class when the Voice VLAN feature is active on a port. By default, 7 (Highest priority) is used. The allowed range is 0 (Lowest) – 7 (Highest).

#### Port Configuration

**Port:** The port number. "All" rules apply to all ports.

**Mode:** Select whether a particular is enabled with Voice VLAN feature or not. There are three options available:

**Disabled:** Disable Voice VLAN feature on a particular port.

**Auto:** Enable the Voice VLAN auto detection mode. When voice (VoIP) traffic is detected on a port, the port will be added as a tagged member to the Voice VLAN. When Auto mode is selected, you need to further decide a method for detecting voice traffic in "Discovery Protocol" field, either OUI or LLDP (802.1ab).

**Forced:** Enable Voice VLAN feature on a particular port.

**Security:** Enable or disable security filtering feature on a per port basis. When enabled, any non-VoIP packets received on a port with Voice VLAN ID will be discarded. VoIP traffic is identified by source MAC addresses configured in the telephony OUI list or through LLDP which is used to discover VoIP devices attached to the switch.

**Discovery Protocol:** Select a method for detecting VoIP traffic. By default, OUI is used.

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

**LLDP:** Use LLDP (IEEE 802.1ab) to discover VoIP devices attached to a port. LLDP checks that the “telephone bit” in the system capability TLV is turned on or not.

**Both:** Use both OUI table and LLDP to detect VoIP traffic on a port.

### 5.18.2 OUI

Voice VLAN OUI Table		
Delete	Telephony OUI	Description
<input type="checkbox"/>	00-01-e3	Siemens AG phones
<input type="checkbox"/>	00-03-6b	Cisco phones
<input type="checkbox"/>	00-0f-e2	H3C phones
<input type="checkbox"/>	00-60-b9	Philips and NEC AG phones
<input type="checkbox"/>	00-d0-1e	Pingtel phones
<input type="checkbox"/>	00-e0-75	Polycorn phones
<input type="checkbox"/>	00-e0-bb	3Com phones

**Telephony OUI:** Specify your VoIP device’s OUI. It must be 6 characters long and the input format is “xx-xx-xx” (x is hexadecimal digit)

**Description:** Specify a descriptive comments or information to this entry.

Click the “Add New Entry” button to insert a new entry to the list.

Click the “Delete” button to remove a newly-inserted entry or select the checkbox to remove a saved entry during the next save.

Click the “Save” button to save settings or changes.

Click the “Reset” button to restore changed settings to the default settings.

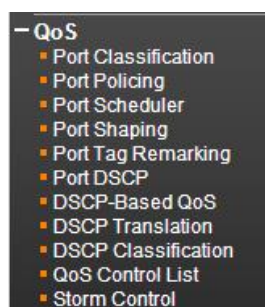


## 5.19 QoS

Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria and receives preferential treatments.

QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. To set up the priority of packets in this switch, go to “Port Classification” page.

The “QoS” menu contains the following sub menus.



### 5.19.1 Port Classification

QoS Ingress Port Classification						
Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
All	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>		<input type="checkbox"/>
1	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Disabled	<input type="checkbox"/>
2	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Disabled	<input type="checkbox"/>
3	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Disabled	<input type="checkbox"/>
4	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Disabled	<input type="checkbox"/>
5	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Disabled	<input type="checkbox"/>
6	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Disabled	<input type="checkbox"/>
7	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Disabled	<input type="checkbox"/>
8	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Disabled	<input type="checkbox"/>
9	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Disabled	<input type="checkbox"/>
10	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Disabled	<input type="checkbox"/>

Save    Reset

**Port:** The port number. “All” rules will apply to all ports.

**QoS class:** Indicate the default QoS class. A QoS class of 0 has the lowest priority. By Default, 0 is used.

**DP Level:** Select the default Drop Precedence Level.

**PCP:** Select the appropriate value for the default Priority Code Point (or User Priority) for untagged frames.

**DEI:** Select the appropriate value for the default Drop Eligible Indicator for untagged frames.

**Tag Class:** This field displays classification mode for tagged frames on this port:

**Disabled:** Use the default QoS class and DP level for tagged frames.

**Enabled:** Use the mapped versions of PCP and DEI for tagged frames.

**DSCP Based:** Select the checkbox to enable DSCP based QoS (Ingress Port).

### 5.19.2 Port Policing

**QoS Ingress Port Policers**

Port	Enabled	Rate	Unit	Flow Control
All	<input type="checkbox"/>	500	▾	<input type="checkbox"/>
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"/>

Save Reset

This page allows users to set each port’s allowed bandwidth.

**Port:** The port number. “All” settings apply to all ports.

**Enabled:** Select the checkbox to enable port policing function on a port.

**Rate:** Indicate the rate for the policer. By default, 500kbps is used. The allowed range for kbps and fps is 100 to 1000000. The allowed range for Mbps and kfps is 1 to 3300Mbps.

**Unit:** Select the unit of measure for the policer.

**Flow Control:** If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

### 5.19.3 Port Scheduler

**QoS Egress Port Schedulers**

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
<a href="#">1</a>	Strict Priority	-	-	-	-	-	-
<a href="#">2</a>	Strict Priority	-	-	-	-	-	-
<a href="#">3</a>	Strict Priority	-	-	-	-	-	-
<a href="#">4</a>	Strict Priority	-	-	-	-	-	-
<a href="#">5</a>	Strict Priority	-	-	-	-	-	-
<a href="#">6</a>	Strict Priority	-	-	-	-	-	-
<a href="#">7</a>	Strict Priority	-	-	-	-	-	-
<a href="#">8</a>	Strict Priority	-	-	-	-	-	-
<a href="#">9</a>	Strict Priority	-	-	-	-	-	-
<a href="#">10</a>	Strict Priority	-	-	-	-	-	-

**Port:** Click the port to set up detailed settings for port scheduler.

**Mode:** Display scheduler mode selected.

**Weight:** Display the weight in percentage assigned to Q0~Q5.

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode:

Queue Shaper				Port Shaper		
Enable	Rate	Unit	Excess	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		

Diagram: A vertical oval labeled "STRICT" with arrows pointing to it from the Queue Shaper section. A Port Shaper section is also present with a rate of 500 kbps.

Save Reset Cancel

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode:

Queue Shaper				Queue Scheduler		Port Shaper		
Enable	Rate	Unit	Excess	Weight	Percent	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	17	17%	<input type="checkbox"/>		

Diagram: A vertical oval labeled "DWRR" and another labeled "STRICT" with arrows pointing to them from the Queue Shaper section. A Port Shaper section is also present with a rate of 500 kbps.

Save Reset Cancel

This page allows you to set up the Schedulers and Shapers for a specific port.

**Scheduler Mode:** The device offers two modes to handle queues.

**Strict mode:** This gives egress queues with higher priority to be transmitted first before lower priority queues are serviced.

**Weight mode:** Deficit Weighted Round-Robin (DWRR) queuing which specifies a scheduling weight for each queue. (Options: Strict, Weighted; Default: Strict) DWRR services the queues in a manner similar to WRR, but the next queue is serviced only when the queue's Deficit Counter becomes smaller than the packet size to be transmitted.

**Queue Shaper/Port Shaper/Queue Shaper**

**Enable:** Select the checkbox to enable queue shaper on a certain queue for this selected port.

**Rate:** Indicate the rate for the queue shaper. By default, 500kbps is used. Allowed range for kbps is 100 to 100000. Allowed range for Mbps is 1 to 3300Mbps.

**Unit:** Select the unit of measure for the queue shaper.

**Excess:** Select the checkbox to allow excess bandwidth.

**Queue Schedule**

**Queue Scheduler:** When Scheduler Mode is set to Weighted, the user needs to indicate a relative weight for each queue. DWRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

**Weight:** Assign a weight to each queue. This weight sets the frequency at which each queue is polled for service and subsequently affects the response time software applications assigned a specific priority value.

**Percent:** The weight as a percentage for this queue.

**Port Shaper:** Set the rate at which traffic can egress this queue.

**Enable:** Select the checkbox to enable Port shaper.

**Rate:** Indicate the rate for Port Shaper. By default, 500kbps is used. Allowed range for kbps is 100 to 1000000. Allowed range for Mbps is 1 to 3300Mbps.

**Unit:** Select the rate of measure

### 5.19.4 Port Shaping

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

This displays each port's queue shaper and port shaper's rate.

Click the port number to modify or reset queue shaper and port shaper's rates. See "Port Scheduler" for detailed explanation on each configuration option.

### 5.19.5 Port Tag Remarking

QoS Egress Port Tag Remarking	
Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified

Click the port number that you want change settings.

QoS Egress Port Tag Remarking Port 2 Port 2 ▾

Tag Remarking Mode Classified ▾

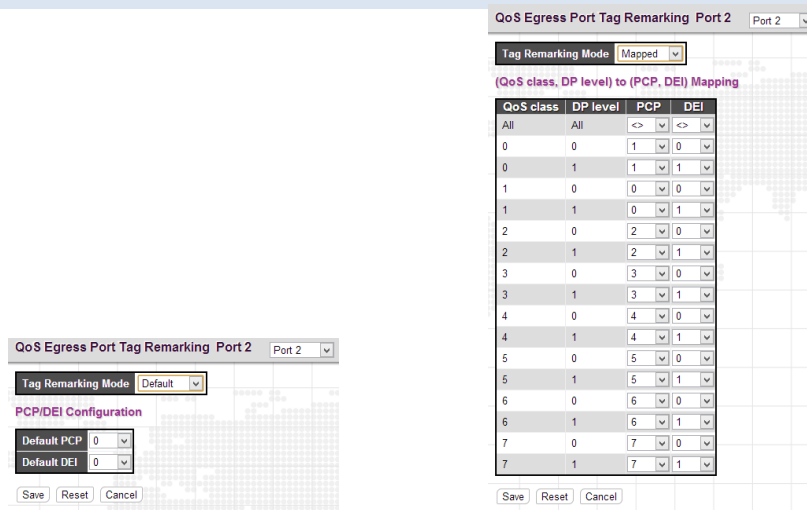
Save Reset Cancel

**Tag Remarking Mode:** Select the appropriate remarking mode used by this port.

**Classified:** Use classified PCP/DEI values.

**Default:** Use default PCP/DEI values (Default PCP:0; Default DEI:0).

**Mapped:** Use the mapping of the classified QoS class values and DP levels to PCP/DEI values.

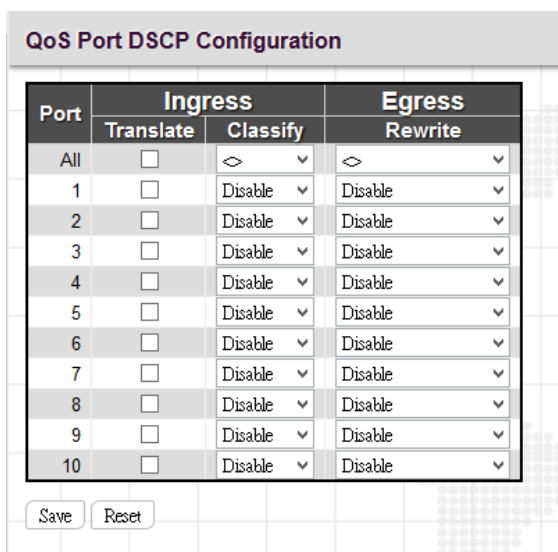


**QoS class/DP level:** Show the mapping options for QoS class values and DP levels (drop precedence).

**PCP:** Remarks matching egress frames with the specified Priority Code Point (or User Priority) value. (Range: 0-7; Default: 0)

**DEI:** Remarks matching egress frames with the specified Drop Eligible Indicator. (Range: 0-1; Default: 0)

### 5.19.6 Port DSCP



**Port:** List the number of each. "All" settings apply to all ports.

**Ingress Translate:** Select the checkbox to enable ingress translation of DSCP values based on the selected classification method.

**Ingress Classify:** Select the appropriate classification method:

**Disable:** No ingress DSCP classification is performed.

**DSCP=0:** Classify if incoming DSCP is 0.

**Selected:** Classify only selected DSCP for which classification is enabled in DSCP Translation table

**All:** Classify all DSCP.

**Egress Rewrite:** Configure port egress rewriting of DSCP values.

**Disable:** Egress rewriting is disabled.

**Enable:** Enable egress rewriting is enabled but with remapping.

**Remap DP aware:** Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. Depending on the frame's DP level, the remapped DSCP value is either taken from the DSCP Translation table, Egress Remap DP0 or DP1 field.

**Remap DP unaware:** Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. The remapped DSCP value is always taken from the DSCP Translation table, Egress Remap DP0 field.

### 5.19.7 DSCP-Based QoS

DSCP-Based QoS Ingress Classification			
DSCP	Trust	QoS Class	DPL
All	<input type="checkbox"/>	<>	<>
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

**DSCP:** DSCP value in ingress packet. DSCP range is from 0 to 63.

**Trust:** Select the checkbox to indicate that DSCP value is trusted. Only trusted DSCP values are mapped to a specific QoS class and drop precedence level (DPL). Frames with untrusted DSCP values are treated as non-IP frames.

**QoS Class:** Select the QoS class to the corresponding DSCP value for ingress processing. By default, 0 is used. Allowed range is 0 to 7.

**DPL:** Select the drop precedence level to the corresponding DSCP value for ingress processing. By default, 0 is used. The value "1" has the higher drop priority.

5.19.8 DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
All	<>	<input type="checkbox"/>	<>	<>
0 (BE)	0 (BE)	<input type="checkbox"/>	0 (BE)	0 (BE)
1	1	<input type="checkbox"/>	1	1
2	2	<input type="checkbox"/>	2	2
3	3	<input type="checkbox"/>	3	3
4	4	<input type="checkbox"/>	4	4
5	5	<input type="checkbox"/>	5	5
6	6	<input type="checkbox"/>	6	6
7	7	<input type="checkbox"/>	7	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)	8 (CS1)
9	9	<input type="checkbox"/>	9	9
10 (AF11)	10 (AF11)	<input type="checkbox"/>	10 (AF11)	10 (AF11)
11	11	<input type="checkbox"/>	11	11
12 (AF12)	12 (AF12)	<input type="checkbox"/>	12 (AF12)	12 (AF12)
13	13	<input type="checkbox"/>	13	13
14 (AF13)	14 (AF13)	<input type="checkbox"/>	14 (AF13)	14 (AF13)
15	15	<input type="checkbox"/>	15	15
16 (CS2)	16 (CS2)	<input type="checkbox"/>	16 (CS2)	16 (CS2)
17	17	<input type="checkbox"/>	17	17
18 (AF21)	18 (AF21)	<input type="checkbox"/>	18 (AF21)	18 (AF21)
19	19	<input type="checkbox"/>	19	19
20 (AF22)	20 (AF22)	<input type="checkbox"/>	20 (AF22)	20 (AF22)
21	21	<input type="checkbox"/>	21	21
22 (AF23)	22 (AF23)	<input type="checkbox"/>	22 (AF23)	22 (AF23)
23	23	<input type="checkbox"/>	23	23
24 (CS3)	24 (CS3)	<input type="checkbox"/>	24 (CS3)	24 (CS3)
25	25	<input type="checkbox"/>	25	25
26 (AF31)	26 (AF31)	<input type="checkbox"/>	26 (AF31)	26 (AF31)
27	27	<input type="checkbox"/>	27	27

**DSCP:** DSCP value in ingress packet. DSCP range is from 0 to 63.

**Ingress Translate:** Enable Ingress Translation of DSCP values based on the specified classification method.

**Ingress Classify:** Enable classification at ingress side as defined in the QoS port DSCP Configuration Table.

**Egress Remap DP0:** Remap DP0 value to the selected DSCP value. DP0 indicates a drop precedence with a low priority.

**Egress Remap DP1:** Remap DP1 value to the selected DSCP value. DP1 indicates a drop precedence with a high priority.

5.19.9 DSCP Classification

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

Save Reset

Map DSCP values to QoS class and DPL value.






**QoS Class:** List of actual QoS class values.

**DPL:** List of actual DPL values

**DSCP:** Select the DSCP value to map QoS class and DPL value. DSCP value selected for "\*" will map to all QoS class and DPL value.

### 5.19.10 QoS Control List

Quality of Service control list is used to establish policies for handling ingress packets based on frame type, MAC address, VID, PCP, DEI values. Once a QCE is mapped to a port, traffic matching the first entry in the QoS Control List is assigned to the QoS class, drop precedence level, and DSCP value defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port.

QoS Control List Configuration											
QCE#	Port	Frame Type	SMAC	DMAC	VID	PCP	DEI	Action			
								Class	DPL	DSCP	
1	1.2	Ethernet	Any	MC	Any	Any	Any	0	Default	Default	    

This page displays rules created in QoS control list (QCL) only. The maximum number of QCL is 256 on this device.

**QCE#:** Display Quality Control Entry index.

**Port:** Display the port number that uses this QCL.

**Frame Type:** Display the frame type to look for in incoming frames. Possible frame types are Any, Ethernet, LLC SNAP, IPv4, IPv6.

**SMAC:** Source MAC address.

**DMAC:** Destination MAC address. Possible values are Any, Broadcast, Multicast, Unicast.

**VID:** Display VLAN ID (1~4095)

**PCP:** Display PCP value.

**DEI:** Display DEI value.


**Action:** Display the classification action taken on ingress frames when the configured parameters are matched in the frame's content. If a frame matches the QCL, the following actions will be taken.


**Class:** If a frame matches the QCL, it will be put in the queue corresponding to the specified QoS class.


**DPL:** The drop precedence level will be set to the specified value.


**DSCP:** The DSCP value will be set to the specified value.

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 row.


: 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.



Once  is clicked in display page, the following page will appear.

### QCE Configuration

**Port Members:** Select ports that use this rule.

### Key Parameters

**Tag:** Select VLAN tag type (Tag or Untag). By default, any type is used.

**VID:** Select VID preference. By default, any VID is used. Select “Specific”, if you would like to designate a VID to this QCL entry. Or Select “Range”, if you would like to map a range of VIDs to this QCL entry.

**PCP:** Select a PCP value (either specific value or a range of values are provided). By default, any is used.

**DEI:** Select a DEI value. By default, any is used.

**SMAC:** Select source MAC address type. By default, any is used. Select “Specific” to specify a source MAC (first three bytes of the MAC address or OUI).

**DMAC Type:** Select destination MAC address type. By default, any is used. Other options available are “UC” for unicast, “MC” for multicast, and “BC” for broadcast.

**Frame Type:** The frame types can be selected are listed below.

**Any:** By default, any is used which means that all types of frames are allowed.

**Ethernet:** This option can only be used to filter Ethernet II formatted packets. (Options: Any, Specific – 600-ffff hex; Default: ffff). Note that 800 (IPv4) and 86DD (IPv6) are excluded. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

**LLC:** LLC refers to Link Logical Control and further provides three options.

**SSAP:** SSAP stands for Source Service Access Point address. By default, any is used. Select specific to indicate a value (0x00 - 0xFF).

**DSAP:** DSAP stands for Destination Service Access Point address. By default, any is used. Select specific to indicate a value (0x00 to 0xFF).

**Control:** Control field may contain command, response, or sequence information depending on whether the LLC frame type is Unnumbered, Supervisory, or Information. By default, any is used. Select specific to indicate a value (0x00 to 0xFF).

**SNAP:** SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any) 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 that of 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 the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

#### **IPv4:**

**Protocol:** IPv4 frame type includes Any, TCP, UDP, Other. If “TCP” or “UDP” is selected, you might further define Sport (Source port number) and Dport (Destination port number).

**Source IP:** Select source IP type. By default, any is used. Select “Specific” to indicate self-defined source IP and submask format. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero

**IP Fragment:** By default, any is used. Datagrams sometimes may be fragmented to ensure they can pass through a network device that uses a maximum transfer unit smaller than the original packet’s size.

**DSCP:** By default, any is used. Select “Specific” to indicate a DSCP value. Select “Range” to indicate a range of DSCP value.

#### **IPv6:**

**Protocol:** IPv6 protocol includes Any, TCP, UDP, Other. If “TCP” or “UDP” is selected, you may need to further define Sport (Source port number) and Dport (Destination port number).

**Source IP:** Select source IP type. By default, any is used. Select “Specific” to indicate self-defined source IP and submask format.

**DSCP:** By default, any is used. Select “Specific” to indicate a DSCP value. Select “Range” to indicate a range of DSCP value.

#### **Action Parameters**

Specify the classification action taken on ingress frame if the parameters match the frame’s content. The actions taken include the following:

**Class:** If a frame matches the QCE, it will be put in the queue corresponding to the specified QoS class or placed in a queue based on basic classification rules.

**DPL:** If a frame matches the QCE, the drop precedence level will be set to the selected value or left unchanged.

**DSCP:** If a frame matches the QCE, the DSCP value will be set to the selected one.

### 5.19.11 Storm Control

Storm Control is used to keep a network from downgraded performance or a complete halt by setting up a threshold for traffic like broadcast, unicast and multicast. When a device on the network is malfunctioning or application programs are not well designed or properly configured, storms may occur and will degrade network performance or even cause a complete halt. The network can be protected from storms by setting a threshold for specified traffic on the device. Any specified packets exceeding the specified threshold will then be dropped.

Frame Type	Enable	Rate (pps)
Unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

Save Reset

**Enable:** Enable Unicast storm, Multicast storm or Broadcast storm protection.

**Rate (pps):** Select the packet threshold. The packets received exceed the selected value will be dropped.

## 5.20 Mirroring

**Mirror Configuration**

Port to mirror to: Disabled

**Mirror Port Configuration**

Port	Mode
All	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
CPU	Disabled

Save Reset

**Port to mirror:** Select the mirror port to which either source (rx) or destination (tx) traffic will be mirrored. Or disable port mirroring function.

**Port:** The port number. "All" rules apply to all ports.

**Mode:** There are four modes that can be used on each port.

**Disabled:** Disable the port mirroring function on a given port.

**Rx only:** Only frames received on this port are mirrored on the mirror port.

**Tx only:** Only frames transmitted on this port are mirrored on the mirror port.

**Enable:** Both frames received and transmitted re mirrored on the mirror port.

## 5.21 UPnP

UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100

Save Reset

**Mode:** Enable or disable UPnP operation.

**TTL:** TTL (Time to live) is used to configure how many steps an UPnP advertisement can travel before it disappears.

**Advertising Duration:** This defines how often an UPnP advertisement is sent. The duration is carried in Simple Service Discover Protocol (SSDP) packets which informs a control point how often it should receive a SSDP advertisement message from the switch. By default, the advertising duration is set to 100 seconds. However, due to the unreliable nature of UDP, it is recommended to set to the shorter duration since the shorter the duration, the fresher is UPnP status.

## 5.22 Diagnostics

The “Diagnostics” menu provides ping function to test the connectivity of a certain IP and VeriPHY cable diagnostics.



### 5.22.1 Ping

This Ping function is for ICMPv4 packets.

ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

**IP Address:** Enter the IP address that you wish to ping.

**Ping Length:** The size or length of echo packets.

**Ping Count:** The number of echo packets will be sent.

**Ping Interval:** The time interval between each ping request.

### 5.22.2 Ping6

This Ping function is for ICMPv6 packets.

**ICMPv6 Ping**

IP Address: 0:0:0:0:0:0:0:0

Ping Length: 56

Ping Count: 5

Ping Interval: 1

Start

**IP Address:** Enter the IP address that you wish to ping.

**Ping Length:** The size or length of echo packets.

**Ping Count:** The number of echo packets will be sent.

**Ping Interval:** The time interval between each ping request.

### 5.22.3 VeriPHY

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

**VeriPHY Cable Diagnostics**

Port: All

Start

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--

**Port:** Select All (all ports) or a port to perform cable diagnostics.

**Start:** Click the “Start” button to begin the diagnostics.

#### Cable Status

**Port:** The port number.

**Pair A/B/C/D:** The status of 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 A/B/C/D:** The length (in meters) of the cable pair.

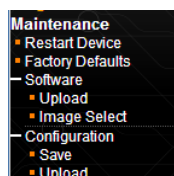
---

**Note:**

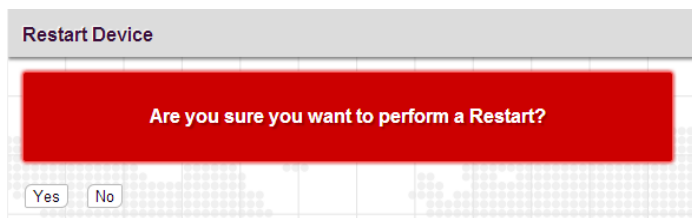
1. If a specific port is selected, the test will take approximately 5 seconds. If all ports are selected, it can run approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.
  2. VeriPHY is only accurate for cables of length 7 - 140 meters.
  3. 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.
  4. The EEE must be disabled at link partner.
- 

## 5.23 Maintenance

The “Maintenance” menu contains several sub menus. Select the appropriate sub menu to restart the device, set the device to the factory default or upgrade firmware image.

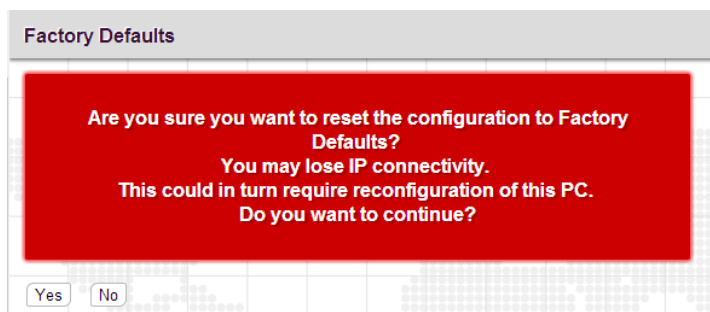


### 5.23.1 Restart Device



Click “Yes” button to reboot the switch.

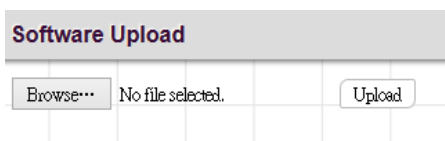
### 5.23.2 Factory Defaults



Click “Yes” button to reset your device to factory defaults settings. Please note that all changed settings will be lost. It is recommended that a copy of the current configuration is saved to your local device.

### 5.23.3 Software

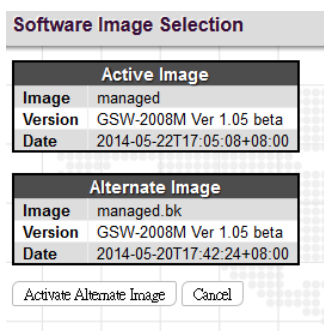
#### 5.23.3.1 Upload



Update the latest Firmware file.

Select a Firmware file from your local device and then click “Upload” to start updating.

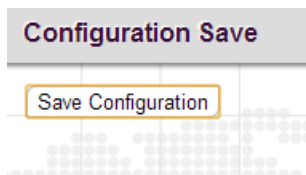
#### 5.23.3.2 Image Select



Select the image file to be used in this device.

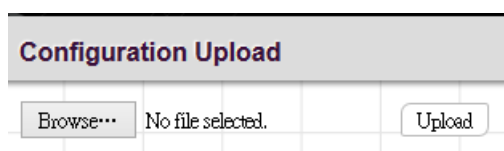
### 5.23.4 Configuration

#### 5.23.4.1 Save



Save the current running configurations in XML format in your local device. The user can also change setting using this file but only changed configurations will be taken effect in your device.

#### 5.23.4.2 Upload



Upload a configuration file to restore the previously saved settings.

## **Appendix A: Acronyms**

### **ACE**

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

### **ACL**

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights. ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

### **AES**

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

### **AMS**

AMS is an acronym for Auto Media Select. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the preferred media.

### **APS**

APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

### **ARP**

ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

### **ARP Inspection**

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

### **CC**

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

### **CCM**

CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

### **CDP**

CDP is an acronym for Cisco Discovery Protocol.

### **DEI**

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

### **DES**

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.



### **DHCP**

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

### **DHCP Relay**

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

### **DHCP Snooping**

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

### **DNS**

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

### **DoS**

DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

### **DSCP**

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

### **EEE**

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

### **EPS**

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

### **Ethernet Type**

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

### **FTP**

FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

### **Fast Leave**

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.

### **HTTP**

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP)

connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

### **HTTPS**

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection. HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logins. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is no longer considered an adequate degree of encryption for commercial exchange.

### **ICMP**

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

### **IEEE 802.1X**

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

### **IGMP**

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

#### **IGMP Querier**

A router sends IGMP Query messages onto a particular link. This router is called the Querier. There will be only one IGMP Querier that wins Querier election on a particular link.

### **IMAP**

IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server. IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server. The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

### **IP**

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network. IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

### **IPMC**

IPMC is an acronym for IP MultiCast. IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

### **IPMC Profile**

IPMC Profile is an acronym for IP MultiCast Profile. IPMC Profile is used to deploy the access control on IP multicast streams.

### **IP Source Guard**

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

### **LACP**

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

### **LLC**

The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

### **LLDP**

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

### **LLDP-MED**

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

### **LLQI**

LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

### **LOC**

LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

### **MAC Table**

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to ( based upon the DMAC address in the frame ). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address ( SMAC address ), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

### **MEP**

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

### **MD5**

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

### **Mirroring**

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

### **MLD**

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

### **MLD Querier**

A router sends MLD Query messages onto a particular link. This router is called the Querier. There will be only one MLD Querier that wins Querier election on a particular link.

### **MSTP**

In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

### **MVR**

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

### **NAS**

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

### **NetBIOS**

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

### **NFS**

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

### **NTP**

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

### **OAM**

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

### **Optional TLVs.**

A LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled the corresponding information is not included in the LLDP frame.

#### **OUI**

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

#### **PCP**

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

#### **PD**

PD is an acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

#### **PHY**

PHY is an abbreviation for Physical Interface Transceiver and is the device that implements the Ethernet physical layer (IEEE-802.3).

#### **PING**

Ping (Packet InterNet Grouper) is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

#### **PoE**

PoE is an acronym for Power Over Ethernet. Power over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN Access Points (AP), IP cameras and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

#### **Policer**

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

#### **POP3**

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

### **PPPoE**

PPPoE is an acronym for Point-to-Point Protocol over Ethernet. It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

### **Private VLAN**

In a private VLAN, PVLANS provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

### **PTP**

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

### **QCE**

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

### **QCI**

QCI is an acronym for QoS Class Identifier. This is a special identifier defining the quality of packet communication provided by LTE (Long Term Evolution, marketed as 4G LTE).

### **QCL**

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

### **QL**

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

### **QoS**

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

### **QoS class**

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

### **Querier Election**

Querier election is used to dedicate the Querier, the only one router sends Query messages, on a particular link. Querier election rule defines that IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

### **RARP**

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

### **RADIUS**

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

### **RDI**

RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP.

### **Router Port**

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

### **RSTP**

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

### **SAMBA**

Samba is a program running under UNIX-like operating systems (not the Brazilian dance) that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

### **sFlow**

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.

Additional information can be found at <http://sflow.org>.

### **SHA**

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

### **Shaper**

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

### **SMTP**

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

### **SNAP**

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

### **SNMP**

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

### **SNTP**

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

### **SPROUT**

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

### **SSID**

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

### **SSH**

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

### **SSM**

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

### **STP**

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

### **Switch ID**

Switch IDs (1-1) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

### **SyncE**

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

### **TACACS+**

TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

### **Tag Priority**

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame. The 3-bits provide 8 priority levels (0~7).

### **TCP**

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).



#### **TELNET**

TELNET is an acronym for TELEtype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

#### **TFTP**

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

#### **ToS**

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

#### **TLV**

TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

#### **TKIP**

TKIP is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

#### **UDP**

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

#### **UPnP**

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

#### **User Priority**

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

## **VLAN**

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

**VLAN unaware switching:** This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

**VLAN aware switching:** This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

**Provider switching:** This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

## **VLAN ID**

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

## **Voice VLAN**

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

## **WEP**

WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, and are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

## **WiFi**

WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

## **WPA**

WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

## **WPA-PSK**

WPA-PSK is an acronym for Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

## **WPA-Radius**

WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia).

**WPS**

WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

**WRED**

WRED is an acronym for Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

**WTR**

WTR is an acronym for Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.





[www.ctcu.com](http://www.ctcu.com)

**T** +886-2 2659-1021    **F** +886-2 2659-0237    **E** sales@ctcu.com