PLANET
Networking & Communication

User's Manual

24-Port 10/100/1000T 802.3at PoE
+ 2-Port 100/1000X SFP
Managed Switch
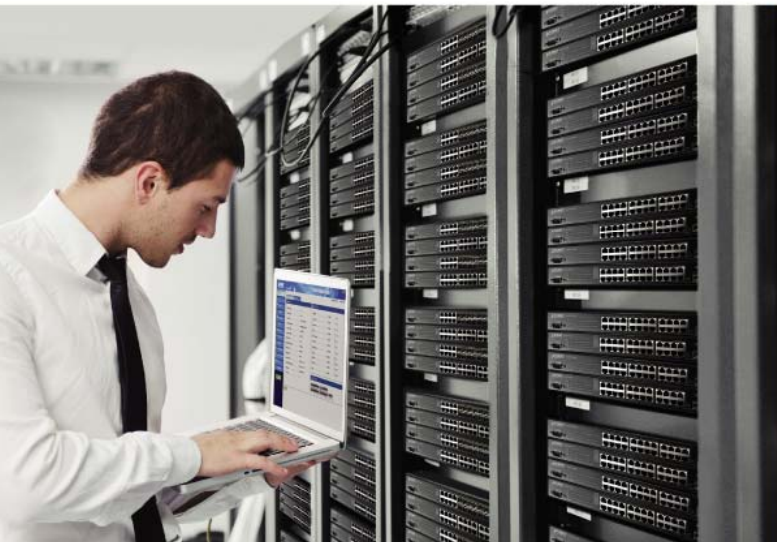
► GS-4210-24P2S

Trademarks

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

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

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy saving, please remove the power cable to disconnect the device from the power circuit. In view of saving the energy and reducing the unnecessary power consumption, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

PLANET 24-Port 10/100/1000T 802.3at PoE + 2-Port 100/1000X SFP Managed Switch User's Manual

FOR MODEL: GS-4210-24P2S

REVISION: 1.0 (July 2014)

Part No: EM-GS-4210-24P2S_v1.0

TABLE OF CONTENTS

1. INTRODUCTION

Thank you for purchasing PLANET 24-Port 10/100/1000T 802.3at PoE + 2-Port 100/1000X SFP Managed Switch, GS-4210-24P2S. "**PoE Managed Switch**" mentioned in this Guide refers to the GS-4210-24P2S.

1.1 Package Contents

Open the box of the PoE Managed Switch and carefully unpack it. The box should contain the following items:

- ◆ **The PoE Managed Switch x 1**

- ◆ **Quick Installation Guide x 1**

- ◆ **Rubber Feet x 4**

- ◆ **Power Cord x 1**

- ◆ **RS-232 to RJ-45 Console Cable x 1**

- ◆ **SFP Dust Cap x 2**

- ◆ **Rack-mount Accessory Kit x 1**

If any item is found missing or damaged, please contact your local reseller for replacement.

1.2 Product Description

Cost-Optimized Managed PoE+ Switch for Small and Medium Businesses

PLANET GS-4210-24P2S is an ideal Gigabit PoE Switch which provides cost-effective advantage to local area network and is widely accepted in the SMB office network. It offers **intelligent Layer 2 data packet switching and management functions**, **friendly web user interface** and **stable operation**. The model complies with **IEEE 802.3at Power over Ethernet Plus (PoE+)** at an affordable price. The GS-4210-24P2S is equipped with **24 10/100/1000Base-T** Gigabit Ethernet ports and 2 **100/1000Base-X** SFP interfaces with inner power system. Its **24** Gigabit Ethernet ports are integrated with 802.3at PoE+ injector function on all ports. It offers a rack-mountable, affordable, safe and reliable power solution for SMBs deploying Power over Ethernet networks, or requiring enhanced data security and network traffic management.

IEEE 802.3at/af Compliant Power Source Switch

The PoE in-line power following the **IEEE 802.3at/af standard** makes the GS-4210-24P2S able to deliver Gigabit speed data and up to **30 watts** of power per port to 24 PoE compliant powered devices (PDs) with a combined power output budget of up to 300 watts. The GS-4210-24P2S provides more flexibility in power requirement for all kinds of PDs with affordable installation costs.

High-performance Switch Architecture

The GS-4210-24P2S provides **24 10/100/1000Mbps** Gigabit Ethernet ports and **2 100/1000Base-X SFP** slots. It boasts a high-performance switch architecture capable of providing the non-blocking switch fabric and wire-speed throughput as high as 52Gbps, which greatly simplifies the tasks of upgrading the LAN for catering to increasing bandwidth demands.

Robust Layer 2 Features

The GS-4210-24P2S can be programmed for advanced switch management functions such as dynamic port link aggregation, 802.1Q VLAN, Spanning Tree protocol (STP), Rapid Spanning Tree protocol (RSTP) and Multiple Spanning Tree protocol (MSTP), IGMP Querier and IGMP Snooping. Via aggregation of supporting ports, the GS-4210-24P2S allows the operation of a high-speed trunk to combine with multiple ports such as a 32Gbps fat pipe and supports fail-over as well. The Link Layer Discovery Protocol (LLDP) feature is also included and used to discover basic information about neighboring devices on the local broadcast domain.

Efficient Traffic Control

The GS-4210-24P2S is loaded with robust QoS features and powerful traffic management to enhance services to business-class data, voice, and video solutions. The functionality includes broadcast / multicast / unicast **storm control**, per port **bandwidth control**, 802.1p / CoS / IP DSCP QoS priority and remarking. It guarantees the best performance at VoIP and video stream transmission, and empowers the enterprises to take full advantages of the limited network resources.

Enhanced and Secure Management

For efficient management, the GS-4210-24P2S is equipped with **console**, **Web**, **Telnet** and **SNMP** management interfaces. With the built-in Web-based management interface, the GS-4210-24P2S offers an easy-to-use, platform-independent management and configuration facility. By supporting standard Simple Network Management Protocol (SNMP), the switch can be managed via any standard management software. For text-based management, the switch can be accessed via Telnet and the console port. Moreover, the GS-4210-24P2S offers secure remote management by supporting **HTTPS** and **SNMPv3** connections which encrypt the packet content at each session.

Powerful Security

PLANET GS-4210-24P2S offers comprehensive Layer 2 to Layer 4 **Access Control List (ACL)** for enforcing security to the edge. It can be used to restrict network access by denying packets based on source and destination IP address, TCP/UDP ports or defined typical network applications. Its protection mechanism also comprises **802.1X port-based** authentication, which can be deployed with RADIUS to ensure the port level security and block illegal users. The **Port Security** allows limiting the number of users on a given port. The network administrators can now construct highly-secured corporate networks with considerably less time and effort than before.

Flexible Extension Solution

The two mini-GBIC slots built in the GS-4210-24P2S are compatible with the **100Base-FX** / **1000Base-SX/LX** SFP (Small Form-factor Pluggable) fiber transceiver to uplink to backbone switch and monitor center in long distance. The distance can be extended from 550 meters to 2km (multi-mode fiber) up to above 10/20/30/40/50/60/70/120 kilometers (single-mode fiber or WDM fiber). They are well suited for applications within the enterprise data centers and distributions.

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, **INSTALLATION**

The section explains the functions of the PoE Managed Switch and how to physically install the PoE Managed Switch.

Section 3, **SWITCH MANAGEMENT**

The section contains the information about the software function of the PoE Managed Switch.

Section 4, **WEB CONFIGURATION**

The section explains how to manage the PoE Managed Switch by Web interface.

Section 5, **COMMAND LINE INTERFACE**

The section describes how to use the Command Line interface (CLI).

Section 6, **CLI CONFIGURATION**

The section explains how to manage the PoE Managed Switch by Command Line interface.

Section 7 SWITCH OPERATION

The chapter explains how to do the switch operation of the PoE Managed Switch.

Section 8 TROUBLESHOOTING

The chapter explains how to troubleshoot the PoE Managed Switch.

Appendix A

The section contains cable information of the PoE Managed Switch.

1.4 Product Features

Physical Port

■ **24-port 10/100/1000Base-T** Gigabit RJ-45 copper

■ **2 100/1000Base-X** mini-GBIC/SFP slots

■ RJ-45 console interface for switch basic management and setup

■ Reset button for system factory default and reboot

Power over Ethernet

■ Complies with IEEE 802.3at High Power over Ethernet

■ Complies with IEEE 802.3af Power over Ethernet

■ Up to 24 ports of IEEE 802.3af / 802.3at devices powered

■ Supports PoE Power up to 30.8 watts for each PoE port

■ 300-watt PoE budget

■ Auto detects powered device (PD)

■ Circuit protection prevents power interference between ports

■ Remote power feeding up to 100m

■ PoE Management

– Total PoE power budget control
– Per port PoE function enable/disable
– PoE Port Power feeding priority
– Per PoE port power limitation
– PoE delay
– PD classification detection

Layer 2 Features

■ Prevents packet loss with back pressure (half-duplex) and IEEE 802.3x pause frame flow control (full-duplex)

■ High performance Store and Forward architecture, runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth

■ Supports **VLAN**

- IEEE 802.1Q tagged VLAN, up to 256 VLAN groups, out of 4094 VLAN IDs
- Protocol VLAN

■ Supports **Spanning Tree Protocol**

- STP (Spanning Tree Protocol)
- RSTP (Rapid Spanning Tree Protocol)
- MSTP (Multiple Spanning Tree Protocol)
- STP BPDU Guard, BPDU Filtering and BPDU Forwarding

■ Supports **Link Aggregation**

– IEEE 802.3ad Link Aggregation Control Protocol (LACP)
– Maximum 8 LACP groups, up to 16 ports per LACP group
– Cisco ether-channel (Static Trunk)
– Maximum 8 trunk groups, up to 8 ports per trunk group

■ Provides port mirror (many-to-1)

Quality of Service

■ Ingress / Egress Rate Limit per port bandwidth control

■ Storm Control support
  – Broadcast / Unknown-Unicast / Unknown-Multicast

■ Traffic classification
  - IEEE 802.1p CoS
  - DSCP / IP Precedence of IPv4 / IPv6 packets

■ Strict priority and Weighted Round Robin (WRR) CoS policies

Multicast

■ Supports IGMP Snooping v2 and v3

■ IGMP Querier mode support

■ IGMP Snooping port filtering

■ Up to 256 multicast groups

Security

■ Authentication
  – IEEE 802.1X port-based network access authentication
  – Built-in RADIUS client to co-operate with the RADIUS servers
  – DHCP Option 82
  – RADIUS / TACACS+ login user access authentication

■ Access Control List
  – IPv4 IP-based ACL
  – IPv4 IP-based ACE
  – MAC-based ACL
  – MAC-based ACE

■ MAC Security
  – Static MAC
  – MAC Filtering

■ Port Security for Source MAC address entries filtering

■ DHCP Snooping to filter distrusted DHCP messages

Management

■ Switch Management Interface
  - Local Command Line Interface
  - Web switch management
  - Telnet Command Line Interface
  - SNMP v1, v2c and v3
  - HTTPs secure access

■ Built-in Trivial File Transfer Protocol (TFTP) client

■ Static and DHCP for IP address assignment

■ System Maintenance
  - Firmware upload / download via HTTP / TFTP

- Configuration upload / download through HTTP / TFTP
- Hardware reset button for system reboot or reset to factory default

■ SNTP Network Time Protocol

■ Link Layer Discovery Protocol (LLDP) Protocol and LLDP-MED

■ SNMP trap for interface Link Up and Link Down notification

■ Event message logging to remote Syslog server

■ Four RMON groups (history, statistics, alarms and events)

■ PLANET Smart Discovery Utility

1.5 Product Specifications

Product	GS-4210-24P2S
Hardware Specifications	
Copper Ports	24 x 10/100/1000Base-T RJ45 Auto-MDI/MDI-X Ports
PoE Injector Port	24 802.3af / 802.3at PoE Injector Ports
SFP/mini-GBIC Slots	2 100/1000Base-X SFP interfaces, supporting 100/1000Mbps dual mode
Console	1 x RS-232-to-RJ45 serial port (115200, 8, N, 1)
Switch Architecture	Store-and-Forward
Switch Fabric	52Gbps / non-blocking
Switch Throughput@64 bytes	38.6Mpps @64 bytes
MAC Address Table	8K entries
Shared Data Buffer	4.1 megabits
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex
Jumbo Frame	9216 bytes
Reset Button	< 5 sec: System reboot > 5 sec: Factory default
LED	**System:** 　Power (**Green**) **10/100/1000T RJ45 Interfaces** (Port 1 to Port 24): 　1000 LNK / ACT (**Green**), 10/100 LNK/ACT (**Orange**), PoE (**Orange**) 100/1000Mbps SFP Interfaces (Port 25 to Port 26): 　1000 LNK / ACT (**Green**), 100 LNK/ACT (**Orange**)
Thermal Fan	2
Power Requirements	100~240V AC, 50/60Hz, 4A (max.)
Power Consumption / Dissipation	Max. 330 watts / 1122 BTU
Dimensions (W x D x H)	445 x 207 x 45 mm (1U height)
Weight	2.8kg
Enclosure	Metal
Power over Ethernet	
PoE Standard	IEEE 802.3af Power over Ethernet / PSE IEEE 802.3at Power over Ethernet Plus / PSE
PoE Power Output	Per Port 52V DC, 300mA. Max. 15.4 watts (IEEE 802.3af) Per Port 52V DC, 600mA. Max. 30 watts (IEEE 802.3at)
PoE Power Budget	300 watts
Number of PDs, 7 watts	24
Number of PDs, 15.4 watts	19
Number of PDs, 30 watts	9
Layer 2 Functions	
Port Mirroring	TX / RX / Both Many-to-1 monitor

VLAN	802.1Q tagged-based VLAN Up to 256 VLAN groups, out of 4094 VLAN IDs Protocol VLAN
Link Aggregation	IEEE 802.3ad LACP supports 8 groups of 16-port trunk and static trunk supports 8 groups of 8-port trunk
Spanning Tree Protocol	STP / RSTP / MSTP
Multicast	IGMP (v2/v3) Snooping IGMP Querier Up to 256 multicast groups
Access Control List	IPv4 IP-based ACL / MAC-based ACL / IPv4 IP-based ACE / MAC-based ACE

QoS	8 mapping ID to 8 level priority queues
	  - Port Number
	  - 802.1p priority
	  - DSCP field in IP Packet
	Traffic classification based, Strict priority and WRR

Security	IEEE 802.1X – port-based authentication Built-in RADIUS client to co-operate with RADIUS server RADIUS / TACACS+ user access authentication MAC filter Static MAC address DHCP Snooping and DHCP Option82 STP BPDU Guard, BPDU Filtering and BPDU Forwarding
Management Functions	
Basic Management Interfaces	RJ45 Console / Web browser / Telnet / SNMP v1, v2c, v3 Firmware upgrade by HTTP / TFTP protocol through Ethernet network Remote / Local Syslog System log LLDP protocol SNTP
Secure Management Interfaces	HTTPs, SNMP v3
SNMP MIBs	RFC 3635 Ethernet-like MIB RFC 2863 Interface Group MIB RFC 2819 RMON (1, 2, 3, 9) RFC 1493 Bridge MIB
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX/100Base-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000Base-T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port Trunk with LACP IEEE 802.1D Spanning Tree protocol IEEE 802.1w Rapid Spanning Tree protocol IEEE 802.1s Multiple Spanning Tree protocol IEEE 802.1p Class of Service

	IEEE 802.1Q VLAN Tagging
	IEEE 802.1x Port Authentication Network Control
	IEEE 802.1ab LLDP
	IEEE 802.3af Power over Ethernet
	IEEE 802.3at High Power over Ethernet
	RFC 768 UDP
	RFC 793 TFTP
	RFC 791 IP
	RFC 792 ICMP
	RFC 2068 HTTP
	RFC 1112 IGMP version 1
	RFC 2236 IGMP version 2
	RFC 3376 IGMP version 3
Environment	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

2. INSTALLATION

This section describes the hardware features and installation of the PoE Managed Switch on the desktop or rack mount. For easier management and control of the PoE Managed Switch, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the PoE Managed Switch, please read this chapter completely.

2.1 Hardware Description

2.1.1 Switch Front Panel

The front panel provides a simple interface monitoring the PoE Managed Switch. Figure 2-1-1 shows the front panel of the PoE Managed Switch.

Front Panel

Figure 2-1-1: GS-4210-24P2S Front Panel

■ **Gigabit TP Interface (802.3af / 802.3at PoE Injector)**

10/100/1000Base-T Copper, RJ-45 Twist-Pair: Up to 100 meters.

■ **100/1000Base-X SFP Slots**

Each of the SFP (Small Form-factor Pluggable) slot supports Dual-speed, 1000Base-SX / LX or 100Base-FX

- For 1000Base-SX/LX SFP transceiver module: From 550 meters (Multi-mode fiber), up to 10/30/40/50/70/120 kilometers (Single-mode fiber).

- For 100Base-FX SFP transceiver module: From 2 kilometers (Multi-mode fiber), up to 20/40/60 kilometers (Single-mode fiber).

■ **Console Port**

The console port is a RJ-45 port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP Address setting, factory reset, port management, link status and system setting. Users can use the attached DB9 to RJ-45 console cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

■ **Reset Button**

At the middle of front panel, the reset button is designed for reboot the PoE Managed Switch without turn off and on the power. The following is the summary table of Reset button function:

Reset Button Pressed and Released	Function
> 5 seconds: Factory Default	Reset the PoE Managed Switch to Factory Default configuration. The PoE Managed Switch will then reboot and load the default settings as below: ○　　　Default Username: **admin** ○　　　Default Password: **admin** ○　　　Default IP address: **192.168.0.100** ○　　　Subnet mask: **255.255.255.0** ○　　　Default Gateway: **192.168.0.254**

2.1.2 LED Indications

The front panel LEDs indicates instant status of port links, data activity, PoE status and system power; helps monitor and troubleshoot when needed. Figure 2-1-2 shows the LED indications of the PoE Managed Switch.

LED Indication
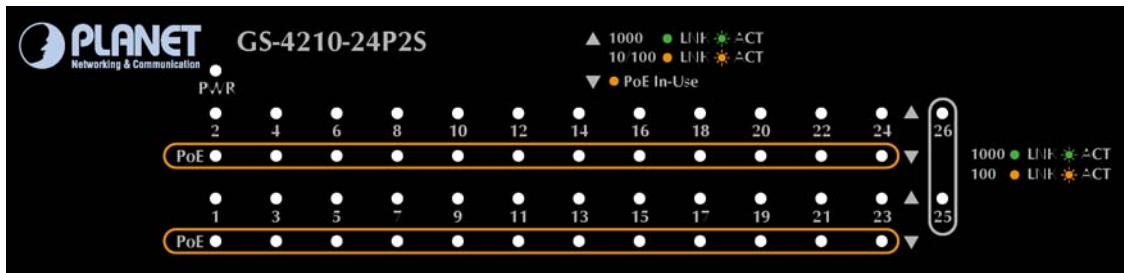
Figure 2-1-2: GS-4210-24P2S LED Panel

■ **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate that the Switch has power.

■ **10/100/1000Base-T Interfaces**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights:**	To indicate the link through that port is successfully established at 1000Mbps.
		Blink:	To indicate that the switch is actively sending or receiving data over that port.
10/ 100 LNK/ACT	**Orange**	**Lights:**	To indicate the link through that port is successfully established at 10Mbps or 100Mbps.
		Blink:	To indicate that the switch is actively sending or receiving data over that port.
PoE In-Use	**Orange**	**Lights:**	To indicate the port is providing 52V DC in-line power.
		Off:	To indicate the connected device is not a PoE Powered Device (PD)

■ **100 / 1000Base-X SFP Interfaces**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights:**	To indicate the link through that port is successfully established at 1000Mbps.
		Blink:	To indicate that the switch is actively sending or receiving data over that port.
100 LNK/ACT	**Orange**	**Lights**:	To indicate the link through that port is successfully established at 100Mbps.
		Blink:	To indicate that the switch is actively sending or receiving data over that port.

2.1.3 Switch Rear Panel

The rear panel of the PoE Managed Switch indicates an AC inlet power socket, which accepts input power from 100 to 240V AC, 50-60Hz, 4A. Figure 2-1-3 shows the rear panel of this PoE Managed Switch.

Rear Panel
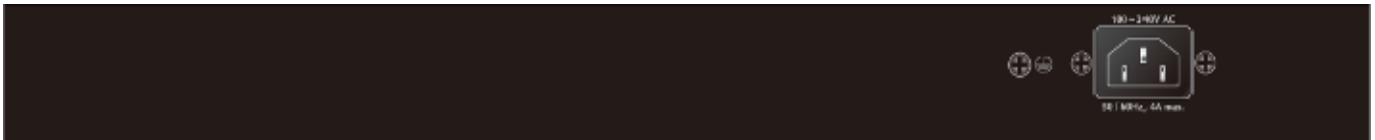
Figure 2-1-3: Rear Panel of GS-4210-24P2S

■ **AC Power Receptacle**

For compatibility with electric service in most areas of the world, the PoE Managed Switch's power supply automatically adjusts to line power in the range of 100-240V AC and 50/60Hz, 4A.

Plug the female end of the power cord firmly into the receptalbe on the rear panel of the PoE Managed Switch. Plug the other end of the power cord into an electric service outlet and the power will be ready.

Power Notice: The device is a power-required device, which means it will not work till it is powered. If your networks should be active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime.

Power Notice: In some areas, installing a surge suppression device may also help to protect your PoE Managed Switch from being damaged by unregulated surge or current to the PoE Managed Switch or the power adapter.

23

2.2 Installing the Switch

This section describes how to install your PoE Managed Switch and make connections to the PoE Managed Switch. Please read the following topics and perform the procedures in the order being presented. To install your PoE Managed Switch on a desktop or shelf, simply complete the following steps.

2.2.1 Desktop Installation

To install the PoE Managed Switch on desktop or shelf, please follow these steps:

Step1: Attach the rubber feet to the recessed areas on the bottom of the PoE Managed Switch.

Step2: Place the PoE Managed Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-1-4.
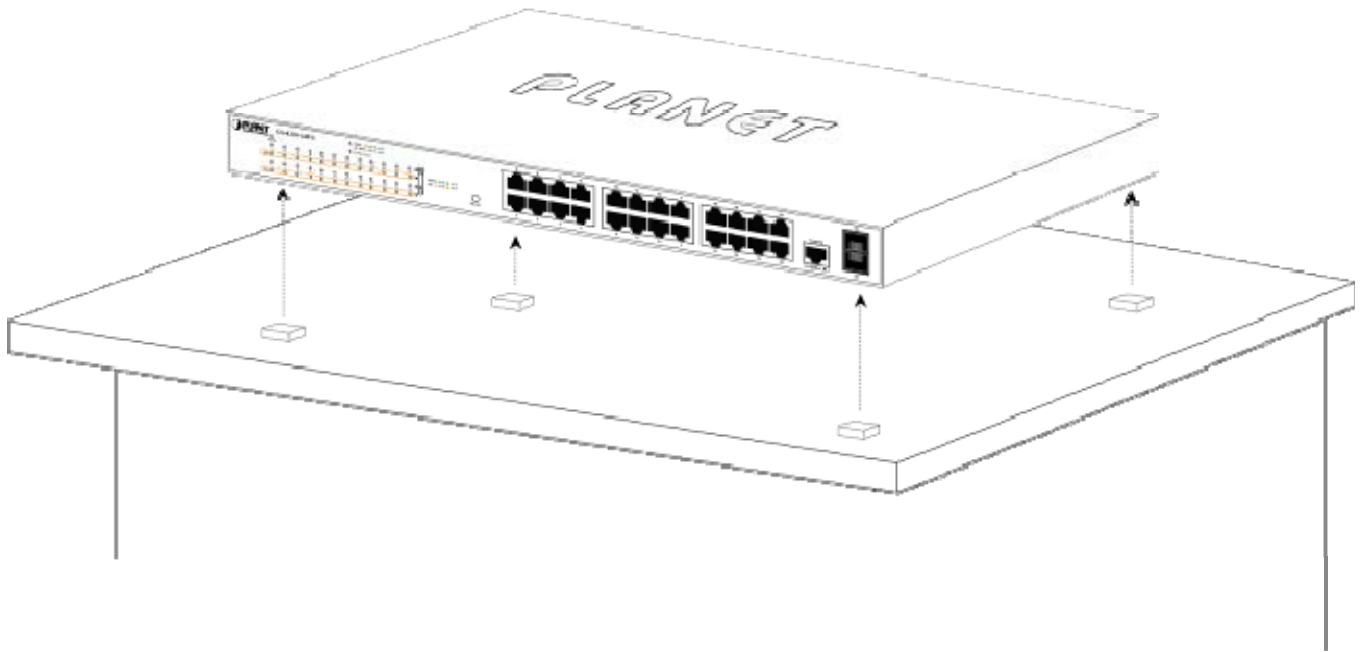
Figure 2-1-4: Place the PoE Managed Switch on the desktop

Step3: Keep enough ventilation space between the PoE Managed Switch and the surrounding objects.

> **Note**
>
> When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Section 4, and specifications.

Step4: Connect the PoE Managed Switch to network devices.

Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the PoE Managed Switch. Connect the other end of the cable to the network devices such as printer server, workstation or router.

> **Note**
>
> Connection to the PoE Managed Switch requires UTP Category 5 network cabling with RJ-45 tips. For more information, please see the Cabling Specification in Appendix A.

Step5: Supply power to the PoE Managed Switch.

Connect one end of the power cable to the PoE Managed Switch.

Connect the power plug of the power cable to a standard wall outlet.

When the PoE Managed Switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the PoE Managed Switch in a 19-inch standard rack, please follow the instructions described below.

Step1: Place the PoE Managed Switch on a hard flat surface, with the front panel positioned towards the front side.

Step2: Attach the rack-mount bracket to each side of the PoE Managed Switch with supplied screws attached to the package.

Figure 2-1-5 shows how to attach brackets to one side of the PoE Managed Switch.
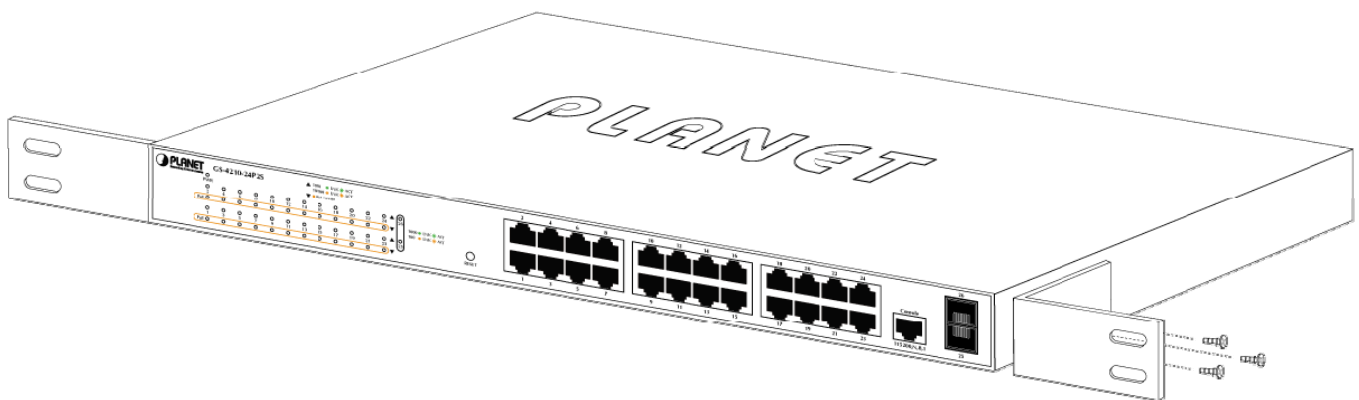
Figure 2-1-5: Attach Brackets to the PoE Managed Switch

You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

Step3: Secure the brackets tightly.

Step4: Follow the same steps to attach the second bracket to the opposite side.

Step5: After the brackets are attached to the PoE Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-1-6.
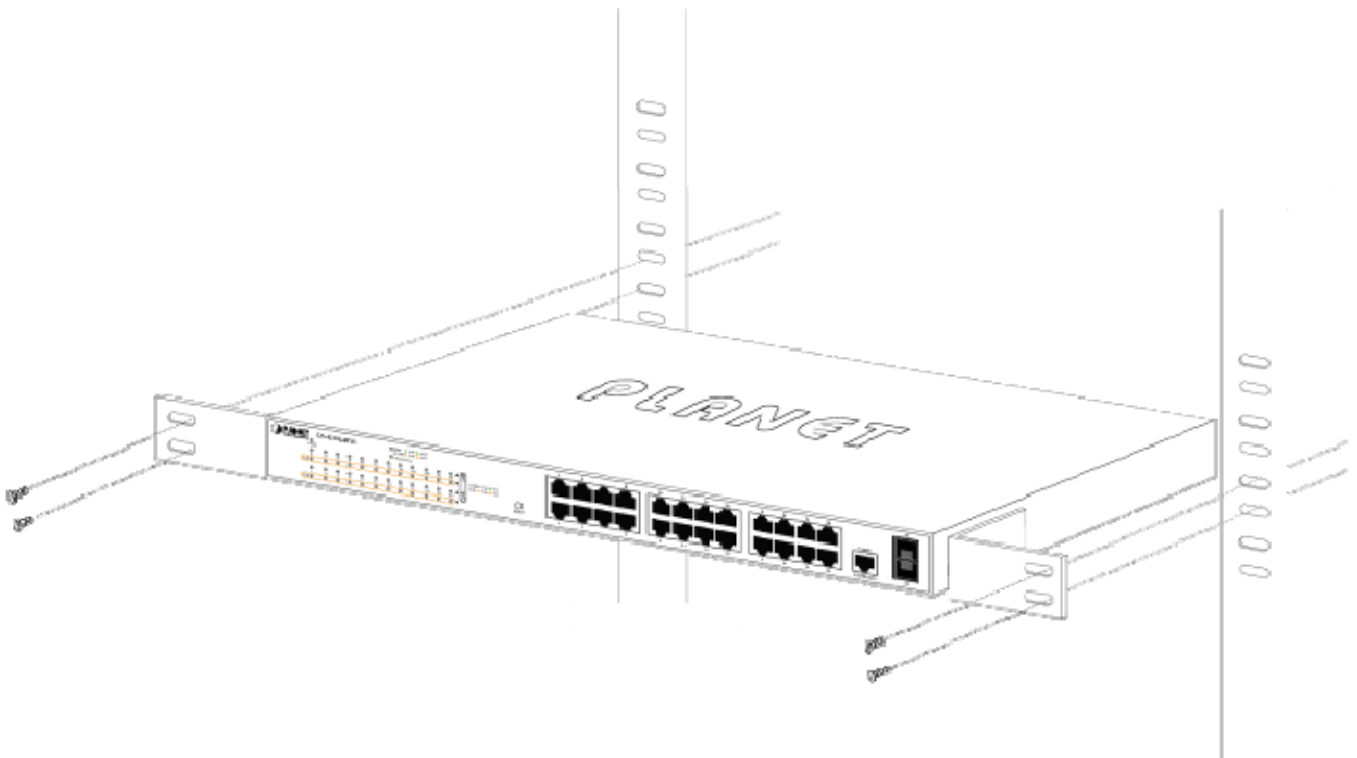
Figure 2-1-6: Mounting PoE Managed Switch in a Rack

Step6: Proceeds with Steps 4 and 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the PoE Managed Switch.

2.2.3 Installing the SFP transceiver

The sections describe how to insert an SFP transceiver into an SFP slot.

The SFP transceivers are hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP port without having to power down the PoE Managed Switch, as the Figure 2-1-7 shows.
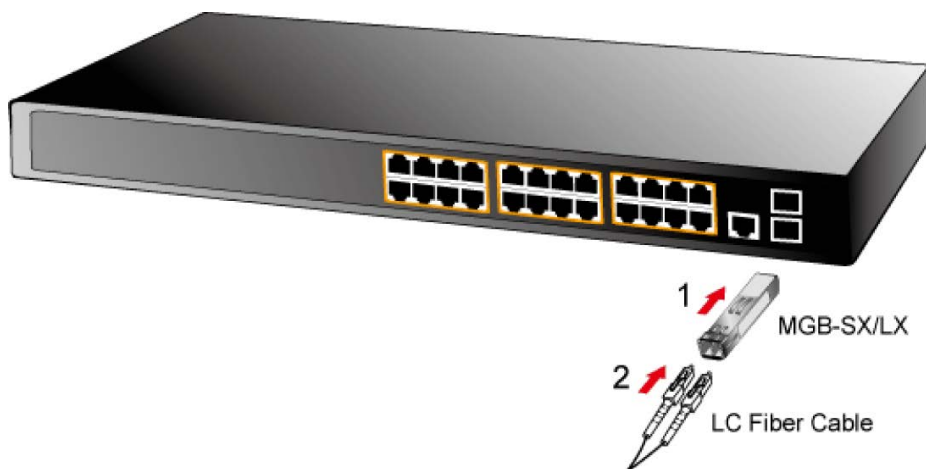
Figure 2-1-7: Plug In the SFP Transceiver

■   **Approved PLANET SFP Transceivers**

PLANET PoE Managed Switch supports both Single mode and Multi-mode SFP transceiver. The following list of approved PLANET SFP transceivers is correct at the time of publication:

Gigabit SFP Transceiver Modules

- ■   **MGB-GT**   SFP-Port 1000Base-T Module
- ■   **MGB-SX**   SFP-Port 1000Base-SX mini-GBIC module
- ■   **MGB-LX**   SFP-Port 1000Base-LX mini-GBIC module -10KM
- ■   **MGB-L30**   SFP-Port 1000Base-LX mini-GBIC module -30KM
- ■   **MGB-L50**   SFP-Port 1000Base-LX mini-GBIC module -50KM
- ■   **MGB-L70**   SFP-Port 1000Base-LX mini-GBIC module -70KM
- ■   **MGB-L120**   SFP-Port 1000Base-LX mini-GBIC module -120KM
- ■   **MGB-LA10**   SFP-Port 1000Base-LX (WDM,TX:1310nm) -10KM
- ■   **MGB-LB10**   SFP-Port 1000Base-LX (WDM,TX:1550nm) -10KM
- ■   **MGB-LA20**   SFP-Port 1000Base-LX (WDM,TX:1310nm) -20KM
- ■   **MGB-LB20**   SFP-Port 1000Base-LX (WDM,TX:1550nm) -20KM
- ■   **MGB-LA40**   SFP-Port 1000Base-LX (WDM,TX:1310nm) -40KM
- ■   **MGB-LB40**   SFP-Port 1000Base-LX (WDM,TX:1550nm) -40KM

Fast Ethernet SFP Transceiver Modules

- ■   **MFB-FX**   SFP-Port 100Base-FX Transceiver -2KM
- ■   **MFB-F20**   SFP-Port 100Base-FX Transceiver -20KM
- ■   **MFB-F40**   SFP-Port 100Base-FX Transceiver -40KM
- ■   **MFB-F60**   SFP-Port 100Base-FX Transceiver -60KM
- ■   **MFB-FA20**   SFP-Port 100Base-BX Transceiver (WDM,TX:1310nm) -20KM
- ■   **MFB-FB20**   SFP-Port 100Base-BX Transceiver (WDM,TX:1550nm) -20KM

	It is recommended to use PLANET SFP on the PoE Managed Switch. If you insert an SFP transceiver that is not supported, the PoE Managed Switch will not recognize it.
Note	
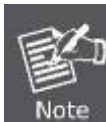
	In the installation steps below, this Manual uses Gigabit SFP transceiver as an example. However, the steps for Fast Ethernet SFP transceiver are similar.
Note	

1.   Before we connect PoE Managed Switch to the other network device, we have to make sure both sides of the SFP transceivers are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.

2.   Check whether the fiber-optic cable type matches with the SFP transceiver requirement.

   ➢   To connect to 1000Base-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.

   ➢   To connect to 1000Base-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

■ **Connect the Fiber Cable**

1. Insert the duplex LC connector into the SFP transceiver.

2. Connect the other end of the cable to a device with SFP transceiver installed.

3. Check the LNK/ACT LED of the SFP slot on the front of the PoE Managed Switch. Ensure that the SFP transceiver is operating correctly.

4. Check the Link mode of the SFP port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to **"1000 Force"** or **"100 Force"**.

■ **Remove the Transceiver Module**

1. Make sure there is no network activity anymore.

2. Remove the Fiber-Optic Cable gently.

3. Lift up the lever of the MGB module and turn it to a horizontal position.

4. Pull out the module gently through the lever.
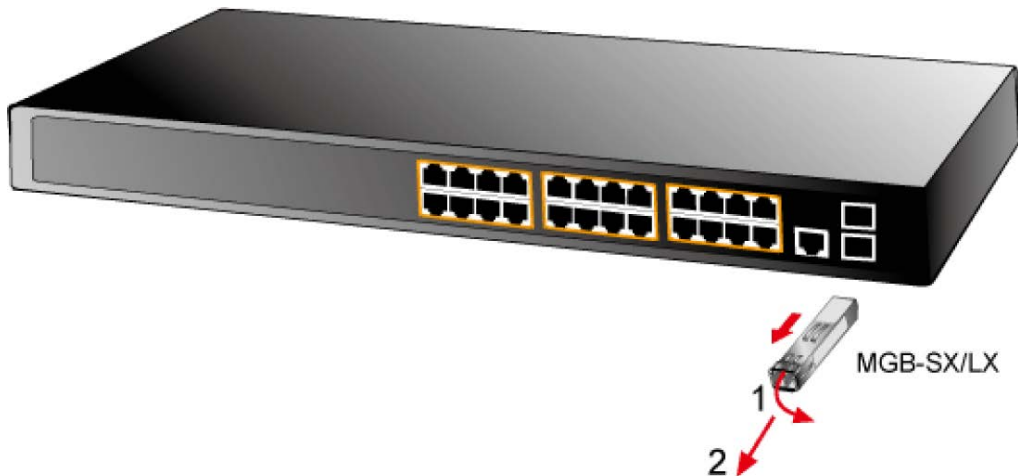
Figure 2-1-8: How to Pull Out the SFP Transceiver

	Never pull out the module without lifting up the lever of the module and turning it to a horizontal position. Directly pulling out the module could damage the module and the SFP module slot of the PoE Managed Switch.
Note	

3. SWITCH MANAGEMENT

This chapter explains the methods that you can use to configure management access to the PoE Managed Switch. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Administration Console Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- **Workstations** running Windows 2000/XP, 2003, Vista/7/8, 2008, MAC OS9 or later, Linux, UNIX or other platforms are compatible with **TCP/IP** protocols.
- **Workstation** is installed with **Ethernet NIC** (Network Interface Card)
- **Serial Port** connect (Terminal)
  - The above PC with COM Port (DB9 / RS-232) or USB-to-RS-232 converter
- Ethernet Port connection
  - Network cables -- Use standard network (UTP) cables with RJ45 connectors.
- The above Workstation is installed with **WEB Browser** and **JAVA runtime environment** Plug-in

It is recommended to use Internet Explore 8.0 or above to access PoE Managed Switch.

3.2 Management Access Overview

The PoE Managed Switch gives you the flexibility to access and manage it using any or all of the following methods:

- An administration **console**

- **Web browser** interface

- An external **SNMP-based network management application**

The administration console and Web browser interface support are embedded in the PoE Managed Switch software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Console	• No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 2000/XP, 2003, Vista/7/8, 2008 operating systems • Secure	• Must be near the switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1: Comparison of Management Methods

3.3 Administration Console

The administration console is an internal, character-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the PoE Managed Switch's console port.

There are two ways to use this management method: via direct access or modem port access. The following sections describe these methods. For more information about using the console, refer to **Chapter 5 Command Line Interface Console Management**.
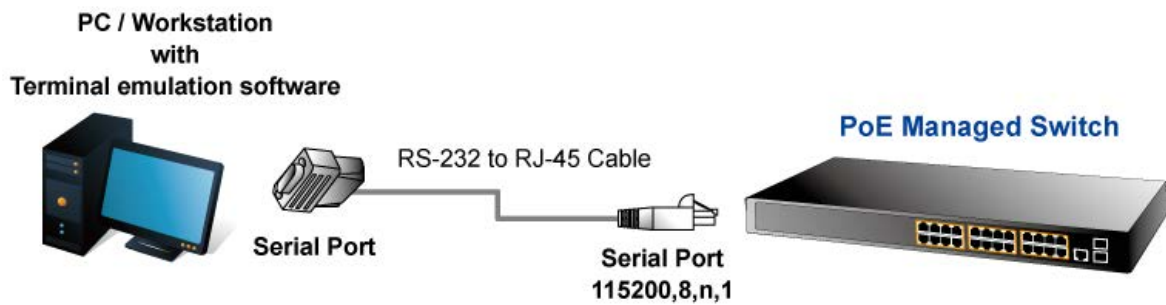
Figure 3-1: Console Management

Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as **HyperTerminal**) to the PoE Managed Switch console (serial) port. When using this management method, a **straight RS-232 to RJ-45 cable** is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:

The default parameters are:

- **115200 bps**
- **8 data bits**
- **No parity**
- **1 stop bit**
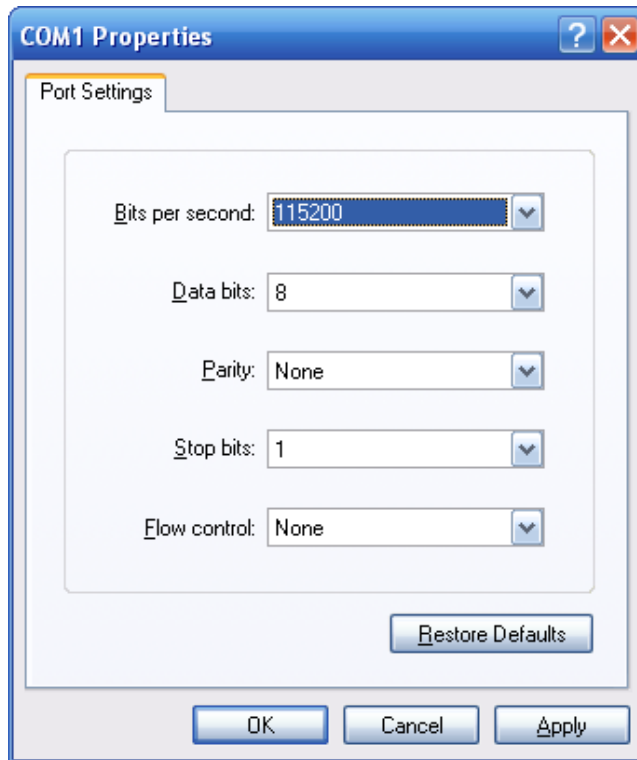
Figure 3-2: Terminal Parameter Settings

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

3.4 Web Management

The PoE Managed Switch offers management features that allow users to manage the PoE Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After you set up your IP address for the PoE Managed Switch, you can access the PoE Managed Switch's Web interface applications directly in your Web browser by entering the IP address of the PoE Managed Switch.
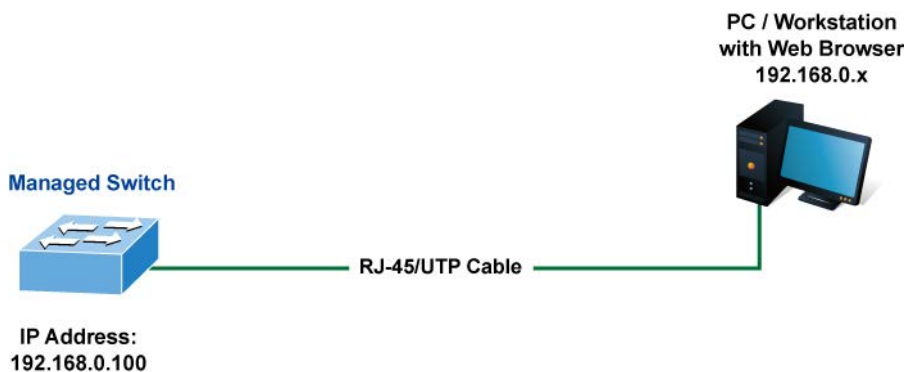
Figure 3-3: Web Management

32

You can then use your Web browser to list and manage the PoE Managed Switch configuration parameters from one central location, just as if you were directly connected to the PoE Managed Switch's console port. Web Management requires either **Microsoft Internet Explorer 8.0** or later, **Google Chrome**, **Safari** or **Mozilla Firefox 1.5** or later.
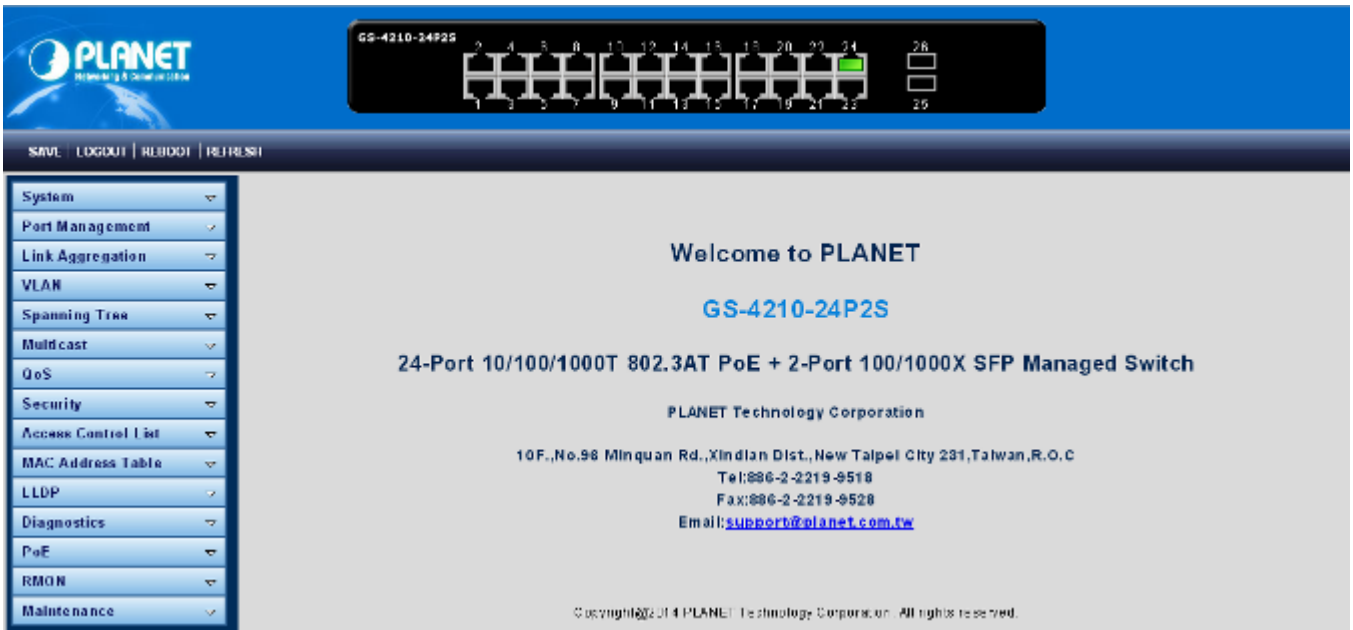
Figure 3-4: Web Main Screen of PoE Managed Switch

3.5 SNMP-based Network Management

You can use an external SNMP-based application to configure and manage the PoE Managed Switch, such as SNMPc Network Manager, HP Openview Network Node Management (NNM) or What's Up Gold. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string. If the SNMP Network management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default gets and sets community strings for the PoE Managed Switch are public.
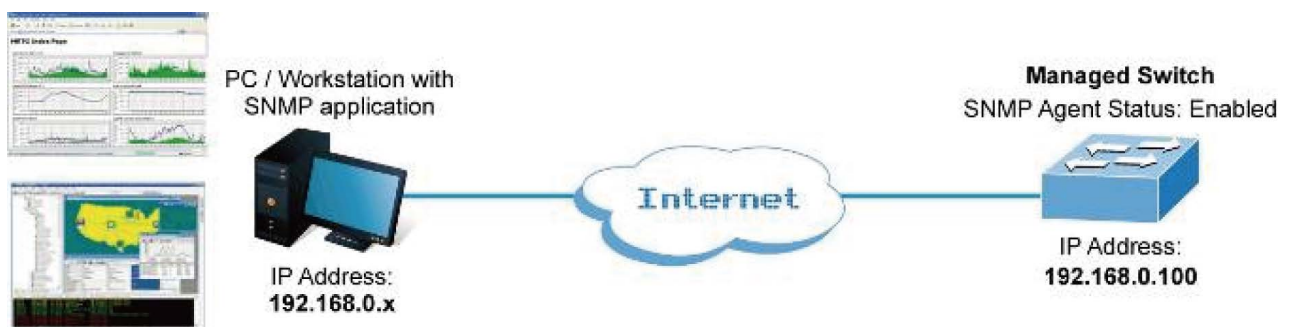
Figure 3-5: SNMP Management

3.6 PLANET Smart Discovery Utility

For easily listing the PoE Managed Switch in your Ethernet environment, the Planet Smart Discovery Utility is an ideal solution.

The following installation instructions are to guide you to running the Planet Smart Discovery Utility.

1. Download the PLANET Smart Discovery Utility from PLANET Official Website.

2. Deposit the Planet Smart Discovery Utility in administrator PC.

3. Run this utility as the following screen appears.
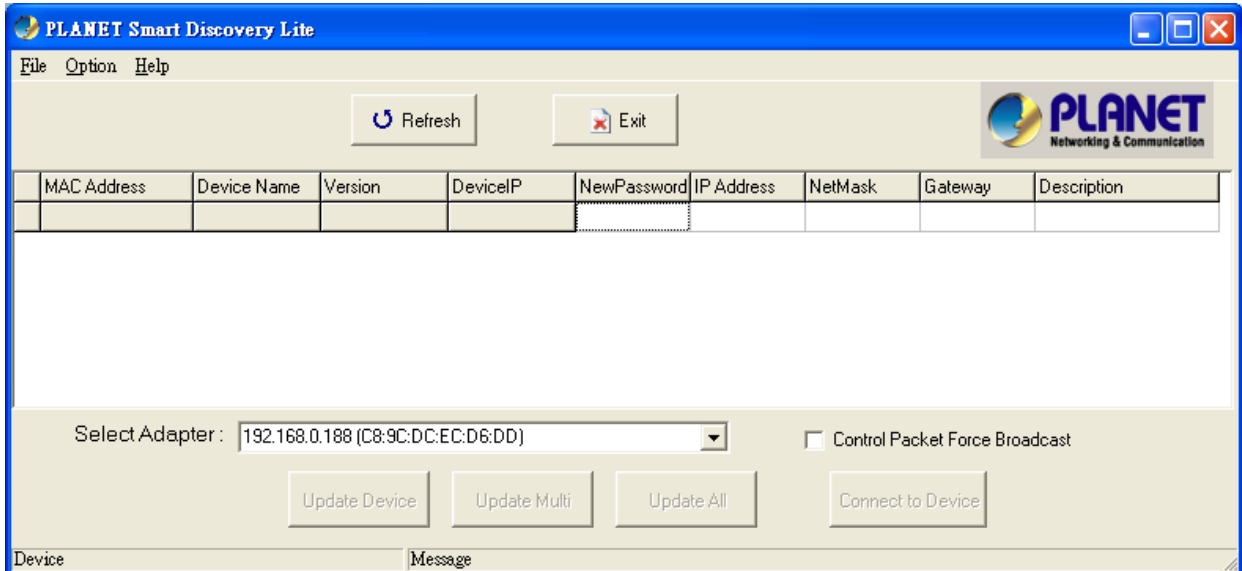
Figure 3-6: Planet Smart Discovery Utility Screen

> If there are two LAN cards or above in the same administrator PC, choose a different LAN card by using the **"Select Adapter"** tool.

4. Press **"Refresh"** button for the currently connected devices in the discovery list as the screen shows below:
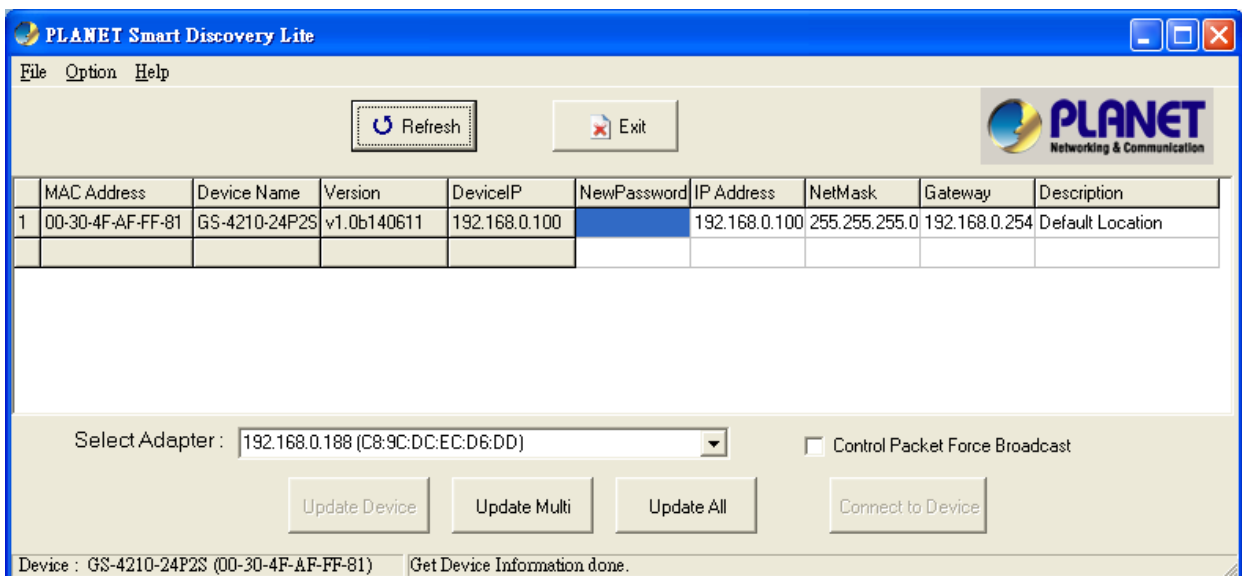
Figure 3-7: Planet Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC Address, Device Name, firmware version and Device IP Subnet address. It can also assign new password, IP Subnet address and description for the devices.

2. After setup is completed, press **"Update Device"**, **"Update Multi"** or **"Update All"** button to take effect. The meaning of the 3 buttons above are shown below:

    ■   **Update Device**: use current setting on one single device.

    ■   **Update Multi:** use current setting on choose multi-devices.

    ■   **Update All:** use current setting on whole devices in the list.

    The same functions mentioned above also can be found in **"Option"** tools bar.

3. To click the **"Control Packet Force Broadcast"** function, it allows you to assign a new setting value to the Web Smart Switch under a different IP subnet address.

4. Press **"Connect to Device"** button and the input usrname / password in web login screen and the web main screen appears in Figure 3-4.

5. Press **"Exit"** button to shut down the Planet Smart Discovery Utility.

4. WEB CONFIGURATION

This section introduces the configuration and functions of the Web-based management.

About Web-based Management

The PoE Managed Switch offers management features that allow users to manage the PoE Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-based Management supports Internet Explorer 8.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

	By default, IE8.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.
Note	

The PoE Managed Switch can be configured through an Ethernet connection, making sure the manager PC must be set on the same IP subnet address as the PoE Managed Switch.

For example, the default IP address of the PoE Managed Switch is *192.168.0.100*, then the manager PC should be set at **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the PoE Managed Switch to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.
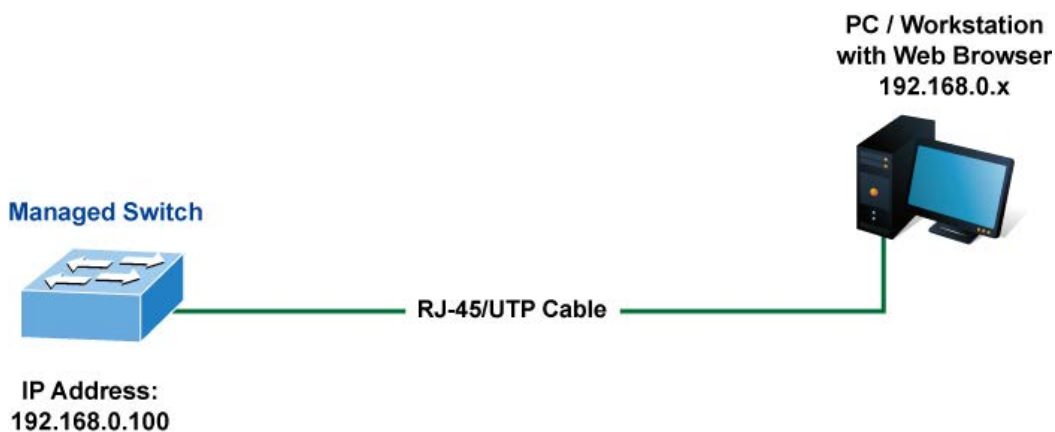
Figure 4-1-1: Web Management

■ **Logging on the PoE Managed Switch**

1. Use Internet Explorer 8.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address as following:

http://192.168.0.100

2.   When the following login screen appears, please enter the default username **"admin"** with password "**admin**" (or the username/password you have changed via console) to login the main screen of PoE Managed Switch. The login screen in Figure 4-1-2 appears.
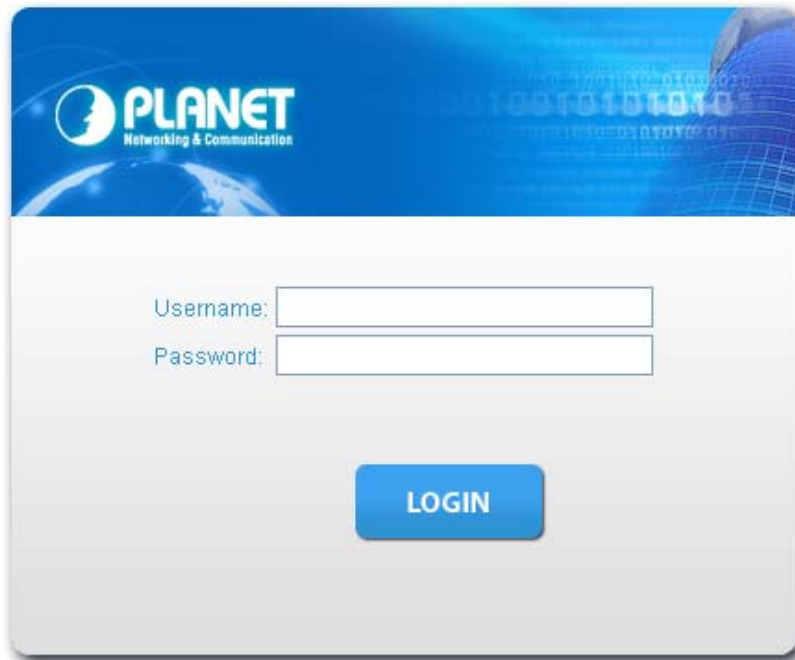
Figure 4-1-2: Login Screen

Default User name: **admin**

Default Password: **admin**

After entering the username and password, the main screen appears as Figure 4-1-3.
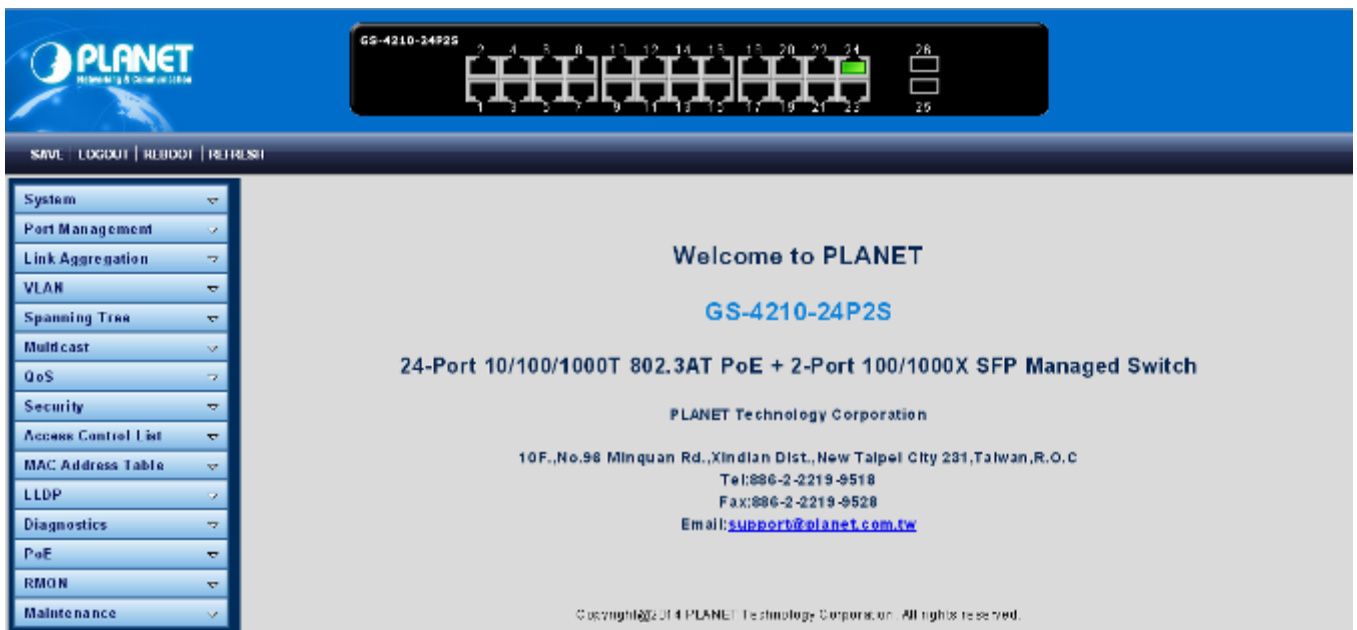
Figure 4-1-3: Web Main Screen of PoE Managed Switch

Now, you can use the Web management interface to continue the switch management or manage the PoE Managed Switch by Web interface. The Switch Menu on the left of the web page let you access all the commands and statistics the PoE Managed Switch provides.

Note	■ It is recommended to use Internet Explore 8.0 or above to access PoE Managed Switch. ■ The changed IP address takes effect immediately after clicking on the **Apply** button. You need to use the new IP address to access the Web interface.

Note	■ For security reason, please change and memorize the new password after this first setup. ■ Only accept command in lowercase letter under web interface.

4.1 Main Web Page

The PoE Managed Switch provides a Web-based browser interface for configuring and managing it. This interface allows you to access the PoE Managed Switch using the Web browser of your choice. This chapter describes how to use the PoE Managed Switch's Web browser interface to configure and manage it.
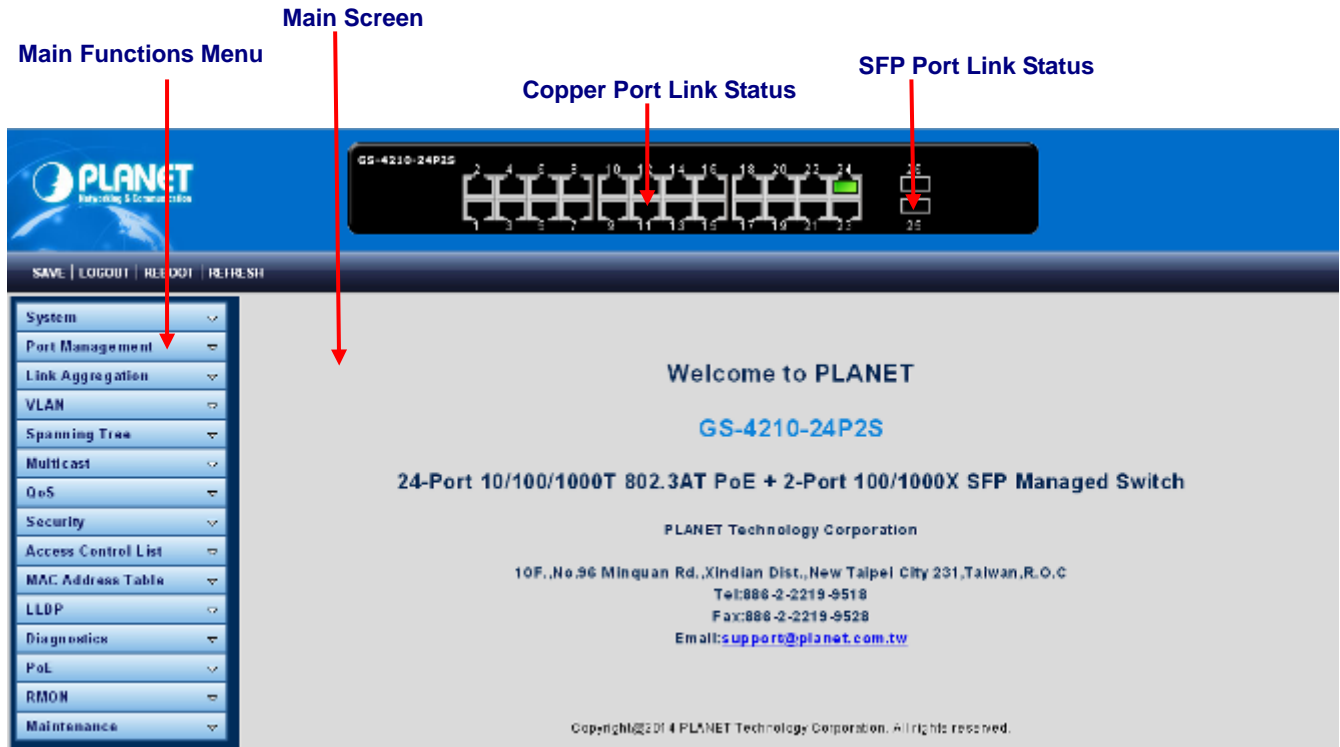
Figure 4-1-4: Web Main Page

Panel Display

The web agent displays an image of the PoE Managed Switch's ports. The Mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the **Port Status** page.

The port states are illustrated as follows:

State	Disabled	Down	Link
RJ-45 Ports			
SFP Ports			

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the PoE Managed Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can setup the PoE Managed Switch by select the functions those listed in the Main Function. The screen in Figure 4-1-5 appears.
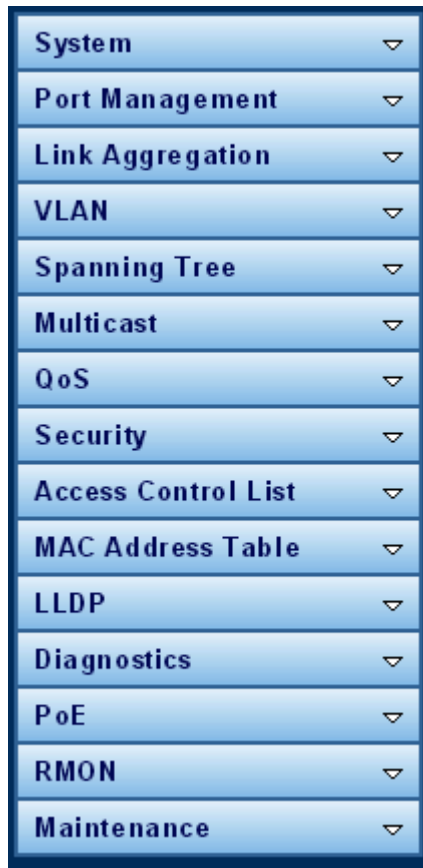
Figure 4-1-5: PoE Managed Switch Main Functions Menu

Buttons

SAVE : Click to save changes or reset to default.

LOGOUT : Click to logout the PoE Managed Switch.

REBOOT : Click to reboot the PoE Managed Switch.

REFRESH : Click to refresh the page.

4.1.1 Save Button

This save button allows save the running / startup / backup configuration or reset switch in default parameter. The screen in Figure 4-1-6 appears.
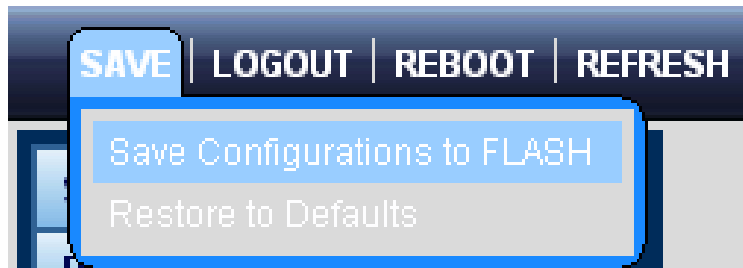
Figure 4-1-6: Save Button Screenshot

The page includes the following fields:

Object	Description
• **Save Confiurations to FLASH**	Click to save the configuration. For more detail infomraiton; please refer to the chapter 4.1.2.
• **Restore to Defaults**	Click to reset switch in default parameter. For more detail infomraiton; please refer to the chapter 4.15.1

4.1.2 Configuration Manager

The system file folder contains configuration settings. The screen in Figure 4-1-7 appears.
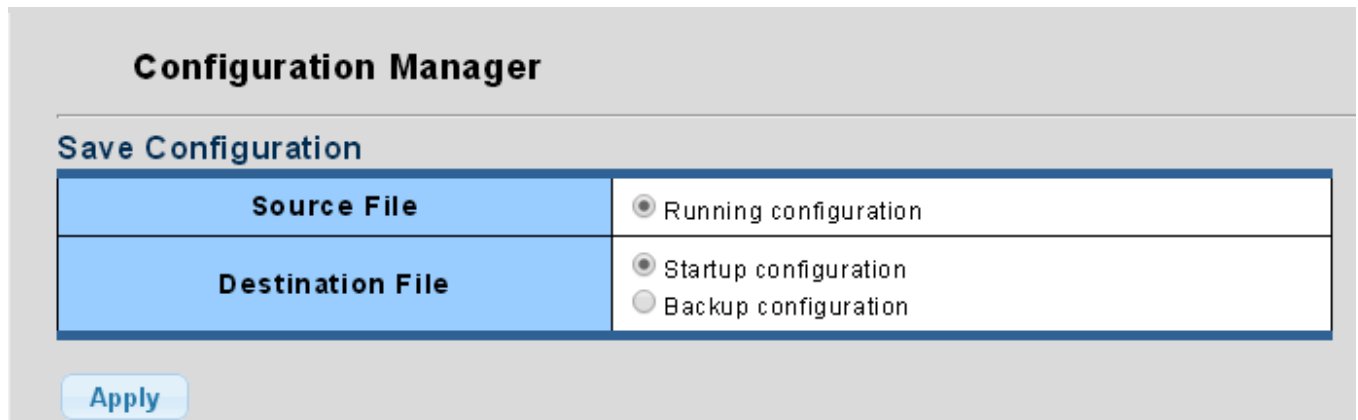
Figure 4-1-7: Save Button Screenshot

The page includes the following fields:

Object	Description
• **Running Configuration**	Refers to the running configuration sequence use in the switch. In switch, the running configuration file stores in the RAM. In the current version, the running configuration sequence running-config can be saved from the RAM to FLASH by save "**Source File = Running Configuration**" to "**Destination File = Startup Configuration**", so that the running configuration sequence becomes the start

	up configuration file, which is called configuration save. To prevent illicit file upload and easier configuration, switch mandates the name of running configuration file to be running-config.
• **Startup Configuration**	Refers to the configuration sequence used in switch startup. Startup configuration file stores in nonvolatile storage, corresponding to the so-called configuration save. If the device supports multi-config file, name the configuration file to be .cfg file, the default is startup.cfg. If the device does not support multi-config file, mandates the name of startup configuration file to be startup-config.
• **Backup Configuration**	The backup configuration is empty in FLASH; please save the backup configuration first by "**Maintenance** > **Backup Manager**".

Button

Apply : Click to save configuration.
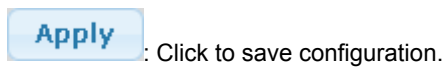
4.1.2.1 Saving Configuration
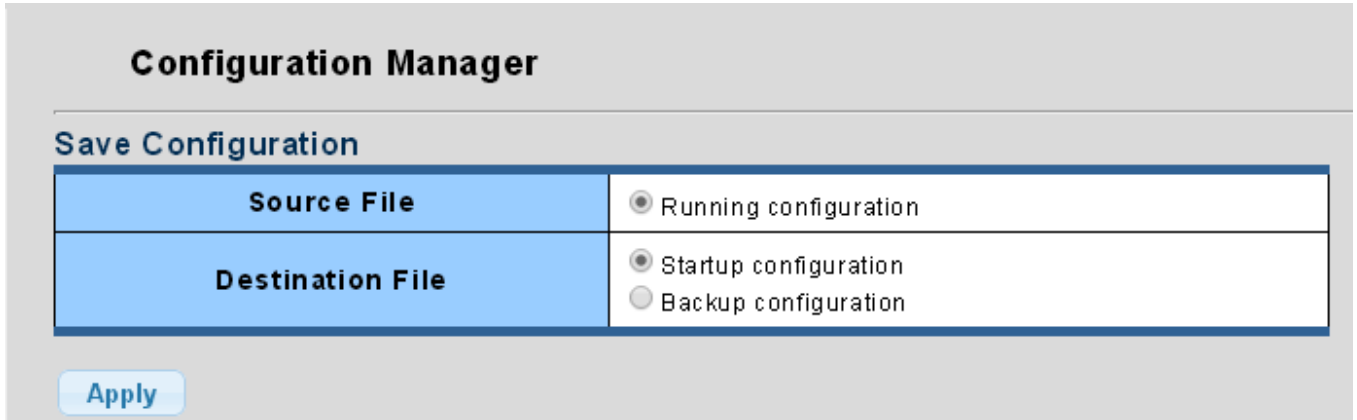
In the PoE Managed Switch, the running configuration file stores in the RAM. In the current version, the running configuration sequence of running-config can be saved from the RAM to FLASH by "**Save Configurations to FLASH**" function, so that the running configuration sequence becomes the startup configuration file, which is called configuration save.

To save all applied changes and set the current configuration as a startup configuration. The startup-configuration file will be loaded automatically across a system reboot.

1. Click"**SAVE > Save Configurations to FLASH**" to login **"Configuration Manager"** Page.
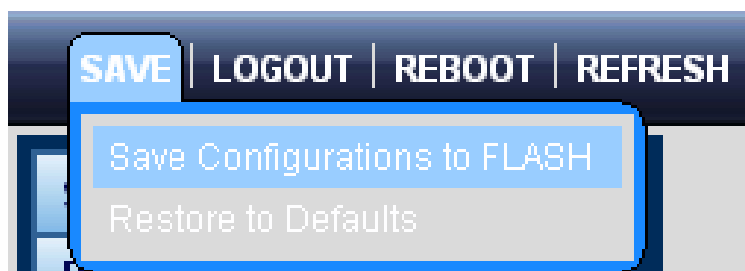
2. Select **"Source File = Running Configuration"** and **"Destination File = Startup Configuration"**.

Configuration Manager

Save Configuration

Source File	⦿ Running configuration
Destination File	⦿ Startup configuration ◯ Backup configuration

Apply

3. Press the "**Apply**" button to save running configuration to startup configuration.

4.2 System

Use the System menu items to display and configure basic administrative details of the PoE Managed Switch. Under System the following topics are provided to configure and view the system information: This section has the following items:

- ■ **System Information**   The switch system information is provided here.
- ■ **IP Configuration**   Configure the switch-managed IP information on this page.
- ■ **User Configuration**   Configure new user name & password on this page.
- ■ **Time Settings**   Configure SNTP on this page.
- ■ **Log Management**   The switch log information is provided here.
- ■ **SNMP Management**   Configure SNMP on this page.

4.2.1 System Information

The System Info page provides information for the current device information. System Info page helps a switch administrator to identify the hardware MAC address, software version and system uptime. The screen in Figure 4-2-1 appears

Information Name	Information Value
System Name	(Edit) GS-4210-24P2S
System Location	(Edit) Default Location
System Contact	(Edit) Default Contact
MAC Address	00:30:4F:AF:FF:81
IP Address	10.1.0.213
Subnet Mask	255.255.255.0
Gateway	10.1.0.254
Loader Version	2011.12.41872
Loader Date	May 22 2014 - 19:28:43
Firmware Version	v1.0b140611
Firmware Date	Wed Jun 11 10:13:28 CST 2014
System Object ID	1.3.6.1.4.1.10456.1.1539
System Up Time	0 days, 0 hours, 1 mins, 31 secs

Figure 4-2-1: System Information Page Screenshot

The page includes the following fields:

Object	Description
• **System Name**	Display the current system name.
• **System Location**	Display the current system location.
• **System Contact**	Display the current system contact.
• **MAC Address**	The MAC Address of PoE Managed Switch.
• **IP Address**	The IP Address of PoE Managed Switch.
• **Subnet Mask**	The subnet mask of PoE Managed Switch.

• **Gateway**	The gateway of PoE Managed Switch.
• **Loader Version**	The loader version of PoE Managed Switch.
• **Loader Date**	The loader date of PoE Managed Switch.
• **Firmware Version**	The firmware version of PoE Managed Switch.
• **Firmware Date**	The firmware date of PoE Managed Switch.
• **System Object ID**	The system object ID of the PoE Managed Switch.
• **System Up Time**	The period of time the device has been operational.

Button

Edit : Click to edit parameter.

4.2.2 IP Configuration

The IP Configuration includes the IP Address, Subnet Mask and Gateway. The Configured column is used to view or change the IP configuration. Fill up the IP Address, Subnet Mask and Gateway for the device. The screens in Figure 4-2-2 & Figure 4-2-3 appear.

IP Address

IP Address Setting

Mode	⦿ Static ○ DHCP
IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Gateway	192.168.0.254

Apply

Figure 4-2-2: IP Address Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the IP address mode operation. Possible modes are:
	Static: Enable NTP mode operation.
	When enable NTP mode operation, the agent forward and to transfer NTP messages between the clients and the server when they are not on the same subnet domain.
	DHCP: Enable DHCP client mode operation.

45

	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
• **IP Address**	Provide the IP address of PoE Managed Switch in dotted decimal notation.
• **Subnet Mask**	Provide the subnet mask of PoE Managed Switch dotted decimal notation.
• **Gateway**	Provide the IP address of the router in dotted decimal notation.

Button

Apply : Click to apply changes.
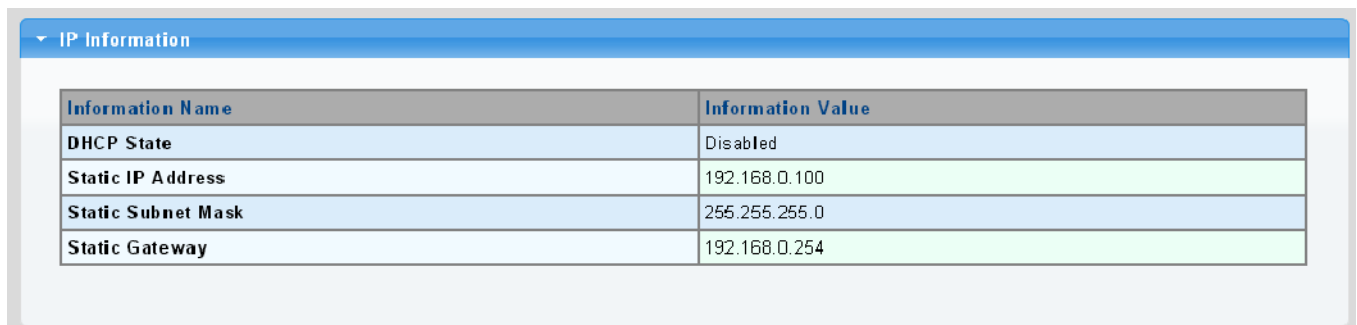
Figure 4-2-3: IP Information Page Screenshot

The page includes the following fields:

Object	Description
• **DHCP State**	Display the current DHCP state.
• **Static IP Address**	Display the current IP address.
• **Static Subnet Mask**	Display the current subnet mask.
• **Static Gateway**	Display the current gateway.

4.2.3 User Configuration

This page provides an overview of the current users and privilege type. Currently the only way to login as another user on the web server is to close and reopen the browser. After setup completed, please press "**Apply**" button to take effect. Please login web interface with new user name and password, the screens in Figure 4-2-4 & Figure 4-2-5 appear.

Figure 4-2-4: Local User Information Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	The name identifying the user. Maximum length: **31** characters; Maximum number of users: **8**
• **Password Type**	The password types for the user. Options: • **Clear Text** • **Encrypted** • **No Password**
• **Password**	Enter the user's new password here. (Range: 0-30 characters plain text, case sensitive)
• **Retype Password**	Please enter the user's new password here again to confirm.

Button

Apply : Click to apply changes.

Figure 4-2-5: Local User Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	Display the current username.
• **Password Type**	Display the current password type.
• **Privilege Type**	Display the current privilege type.
• **Modify**	Click to modify the local user entry. **Delete** : Delete the current user

4.2.4 Time Settings

4.2.4.1 System Time

Configure SNTP on this page.

SNTP is an acronym for **Simple Network Time Protocol**, a network protocol for synchronizing the clocks of computer systems. You can specify SNTP Servers and set GMT Time zone. The SNTP Configuration screens in Figure 4-2-6 & Figure 4-2-7 appear.

Figure 4-2-6: SNTP Setup Page Screenshot

The page includes the following fields:

Object	Description
• **Enable SNTP**	**Enabled**: Enable SNTP mode operation. When enable SNTP mode operation, the agent forward and to transfer SNTP messages between the clients and the server when they are not on the same subnet domain. **Disabled**: Disable SNTP mode operation.
• **Manual Time**	To set time manually. • **Year** - Select the starting Year. • **Month** - Select the starting month. • **Day** - Select the starting day. • **Hours** - Select the starting hour. • **Minutes** - Select the starting minute. • **Seconds** - Select the starting seconds.
• **Time Zone**	Allow select the time zone according to current location of switch.
• **Daylight Saving Time**	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default: Disabled).
• **Daylight Saving Time Offset**	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440 Minutes)
• **Recurring From**	• **Day** - Select the starting day. • **Week** - Select the starting week number. • **Month** - Select the starting month. • **Hours** - Select the starting hour. • **Minutes** - Select the starting minute.
• **Recurring To**	• **Day** - Select the starting day. • **Week** - Select the starting week number. • **Month** - Select the starting month. • **Hours** - Select the starting hour. • **Minutes** - Select the starting minute.
• **Non-recurring From**	• **Year** - Select the starting Year. • **Month** - Select the starting month. • **Date** - Select the starting date. • **Hours** - Select the starting hour. • **Minutes** - Select the starting minute.

• **Non-recurring To**	• **Year** - Select the starting Year.
	• **Month** - Select the starting month.
	• **Date** - Select the starting date.
	• **Hours** - Select the starting hour.
	• **Minutes** - Select the starting minute.

Button

Apply : Click to apply changes.

System Time Information	
Information Name	**Information Value**
Current Date/Time	08:44:02 DFL(UTC+8) Jan 01 2000
SNTP	Disabled
Time Zone	UTC+8
Daylight Saving Time	Disabled
Daylight Saving Time Offset	
From	
To	
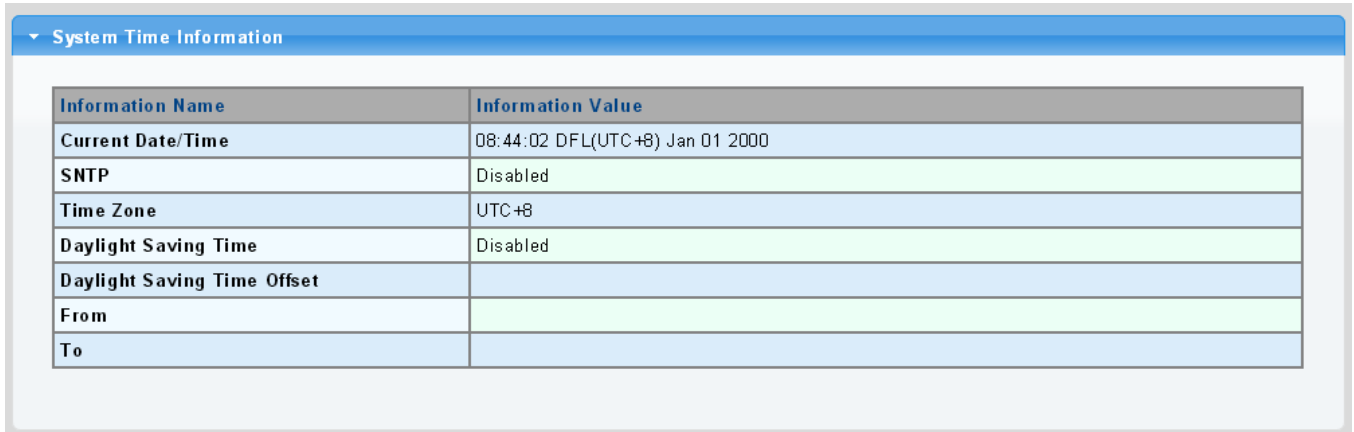
Figure 4-2-7: Time Information Page Screenshot

The page includes the following fields:

Object	Description
• **Current Date/Time**	Display the current date / time.
• **SNTP**	Display the current SNTP state.
• **Time Zone**	Display the current time zone.
• **Daylight Saving Time**	Display the current daylight saving time state.
• **Daylight Saving Time Offset**	Display the current daylight saving time offset state.
• **From**	Display the current daylight saving time from.
• **To**	Display the current daylight saving time to.

4.2.4.2 SNTP Configuration

The SNTP Server Configuration screens in Figure 4-2-8 & Figure 4-2-9 appear.

Figure 4-2-8: SNTP Setup Page Screenshot

The page includes the following fields:

Object	Description
• **SNTP / NTP Server Address**	Type the IP address or domain name of the SNTP / NTP server.
• **Server Port**	Type the port number of the server port. **Options:** 1-65535 **Default:** 123

Button

 : Click to apply changes.

Figure 4-2-9: SNTP Server Information Page Screenshot

The page includes the following fields:

Object	Description
• **SNTP Server Address**	Display the current SNTP server address.
• **SNTP Server Port**	Display the current SNTP server port.

4.2.5 Log Management

The PoE Managed Switch log management is provided here. The local logs allow you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 6 to be logged to RAM. The following table lists the event levels of the PoE Managed Switch:

Level	Severity Name	Description
7	**Debug**	Debugging messages
6	**Informational**	Informational messages only
5	**Notice**	Normal but significant condition, such as cold start
4	**Warning**	Warning conditions (e.g., return false, unexpected return)
3	**Error**	Error conditions (e.g., invalid input, default used)
2	**Critical**	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	**Alert**	Immediate action needed
0	**Emergency**	System unusable

4.2.5.1 Logging Service

The PoE Managed Switch system local log information is provided here. The local Log screens in Figure 4-2-10 & Figure 4-2-11 appear.
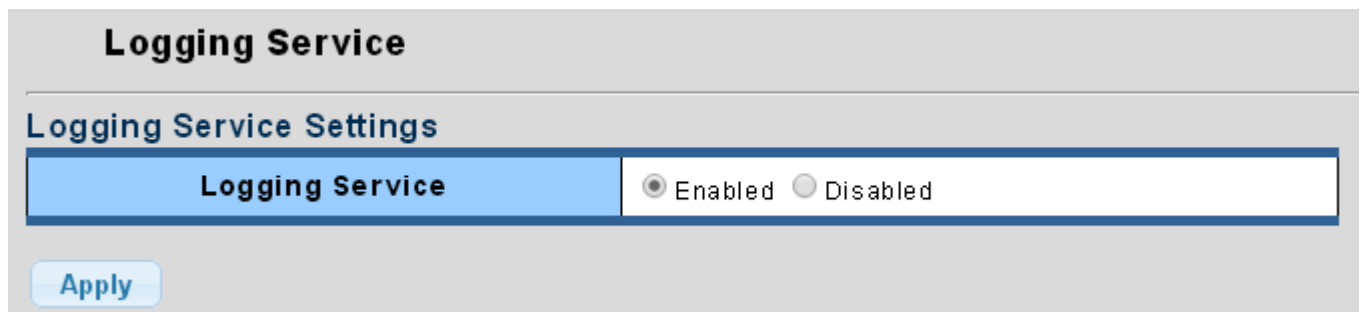
Figure 4-2-10: Logging Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Logging Service**	**Enabled**: Enable logging service operation.
	Disabled: Disable logging service operation.

Button

Apply : Click to apply changes.
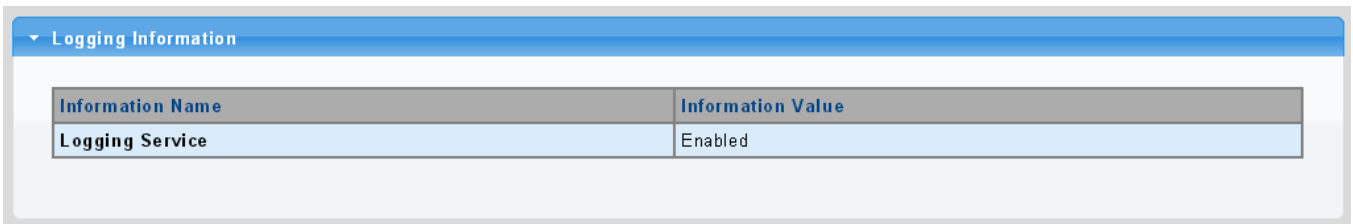
Figure 4-2-11: Logging Information Page Screenshot

The page includes the following fields:

Object	Description
• **Logging Service**	Display the current logging service status.

4.2.5.2 Local Logging

The PoE Managed Switch system local log information is provided here. The local Log screens in Figure 4-2-12 & Figure 4-2-13 appear.
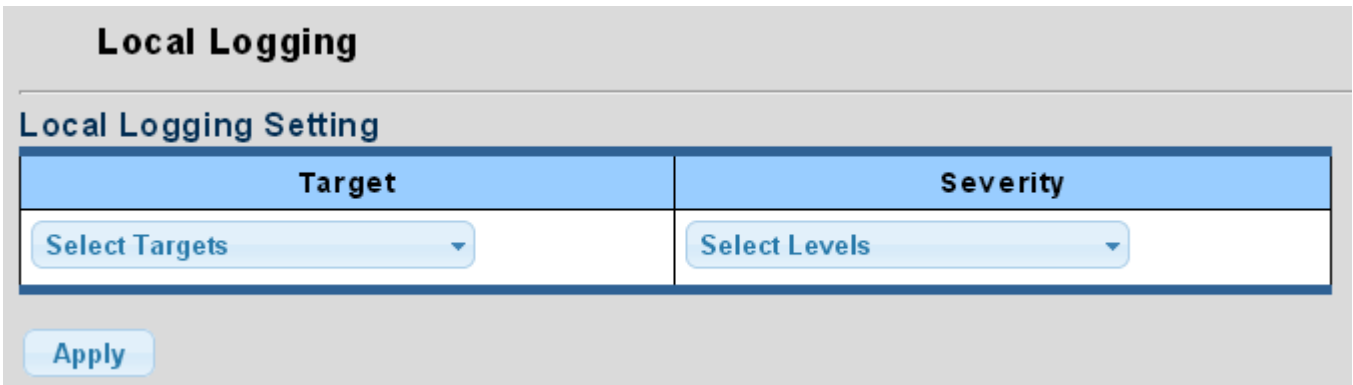
Figure 4-2-12: Local Log Target Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Target**	The target of the local log entry. The following target types are supported: ■ **Buffered**: Target the buffer of the local log. ■ **Flash**: Target the Flash of the local log.
• **Severity**	The severuty of the local log entry. The following severity types are supported: ■ **Emerg**: Emergency level of the system unsable for local log. ■ **Alert**: Alert level of the immediate action needed for local log. ■ **Crit**: Critical level of the critical conditions for local log. ■ **Error**: Error level of the error conditions for local log. ■ **Warning**: Warning level of the warning conditions for local log. ■ **Notice**: Notice level of the normal but significant conditions for local log. ■ **Info**: Informational level of the informational messages for local log. ■ **Debug**: Debug level of the debugging messages for local log.

Button

Apply : Click to apply changes.

Status	Target	Severity	Action
Enabled	Buffered	Emerg, Alert, Crit, Error, Warning, Notice, Info	Delete

▼ Local Logging Setting Status
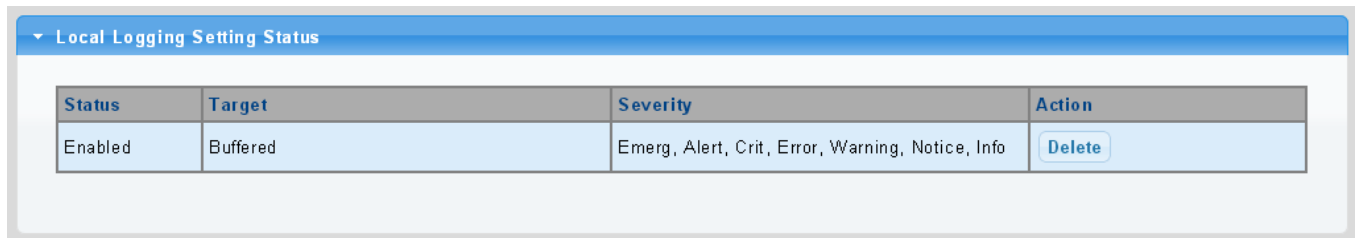
Figure 4-2-13: Local Log Setting Status Page Screenshot

The page includes the following fields:

Object	Description
• **Status**	Display the current local log state
• **Target**	Display the current local log target
• **Severity**	Display the current local log severity
• **Action**	Delete : Delete the current status

4.2.5.3 Remote Syslog

Configure remote syslog on this page. The Remote Syslog page allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.
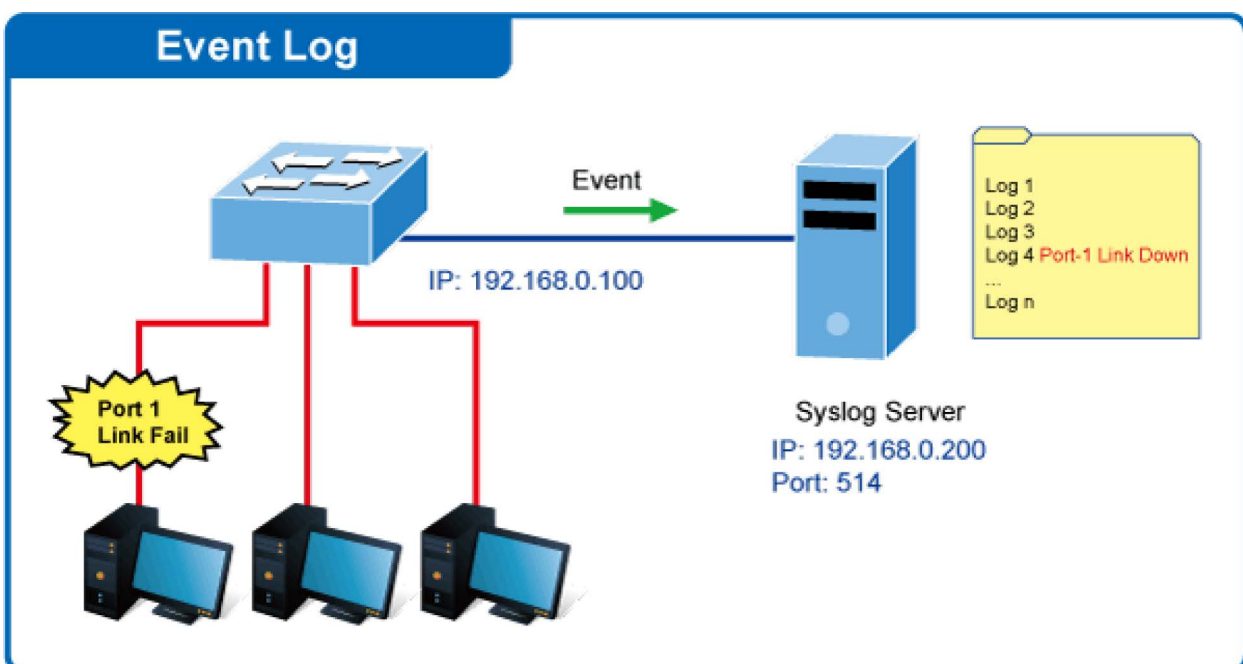
The Remote Syslog screens in Figure 4-2-14 & Figure 4-2-15 appear.

Remote Logging

Remote Logging Setting

Server Address	Server Port	Severity	Facility
	514 (1-65535)	Select Levels ▼	local0 ▼

Apply

Figure 4-2-14: Remote Log Target Page Screenshot

The page includes the following fields:

Object	Description
• **Server Address**	Provide the remote syslog IP address of this PoE Managed Switch.
• **Server Port**	Provide the port number of remote syslog server. **Options:** 1-65535 **Default Port no:** 514
• **Severity**	The severity of the local log entry. The following severity types are supported: ■ **Emerg**: Emergency level of the system unsable for local log. ■ **Alert**: Alert level of the immediate action needed for local log. ■ **Crit**: Critical level of the critical conditions for local log. ■ **Error**: Error level of the error conditions for local log. ■ **Warning**: Warning level of the warning conditions for local log. ■ **Notice**: Notice level of the normal but significant conditions for local log. ■ **Info**: Informational level of the informational messages for local log. ■ **Debug**: Debug level of the debugging messages for local log.
• **Facility**	**Local0~7**: local user 0~7

Button

Apply : Click to apply changes.

Remote Logging Setting Status

Status	Server Info	Severity	Facility	Action

Figure 4-2-15: Remote Log Setting Status Page Screenshot

The page includes the following fields:

Object	Description
• **Status**	Display the current remote syslog state
• **Server Info**	Display the current remote syslog server information
• **Severity**	Display the current remote syslog severity
• **Facility**	Display the current remote syslog facility
• **Action**	Delete : Delete the remote server entry

4.2.5.4 Logging Message

The switch log view is provided here. The Log View screens in Figure 4-2-16, Figure 4-2-17 & Figure 4-2-18 appear.
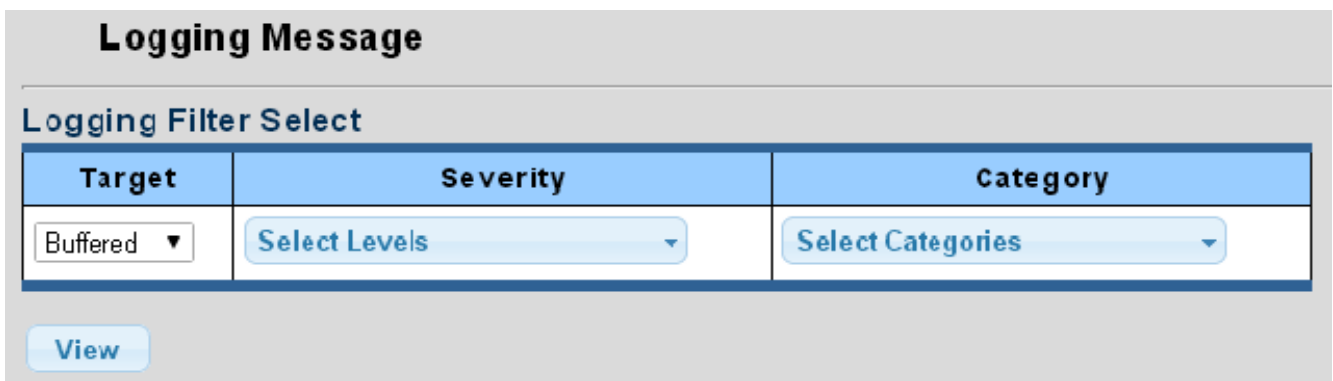
Figure 4-2-16: Log Information Select Page Screenshot

The page includes the following fields:

Object	Description
• **Target**	The target of the log view entry. The following target types are supported: ■ **Buffered**: Target the buffered of the log view. ■ **Flash**: Target the Flash of the log view.
• **Severity**	The severity of the log view entry. The following severity types are supported: ■ **Emerg**: Emergency level of the system unsable for log view. ■ **Alert**: Alert level of the immediate action needed for log view. ■ **Crit**: Critical level of the critical conditions for log view. ■ **Error**: Error level of the error conditions for log view. ■ **Warning**: Warning level of the warning conditions for log view. ■ **Notice**: Notice level of the normal but significant conditions for log view. ■ **Info**: Informational level of the informational messages for log view. ■ **Debug**: Debug level of the debugging messages for log view.
• **Category**	The category of the log view that are including: AAA, ACL, CABLE_DIAG, CDP, DAI, DHCP_SNOOPING, Dot1X, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP

Button

View : Click to view log.
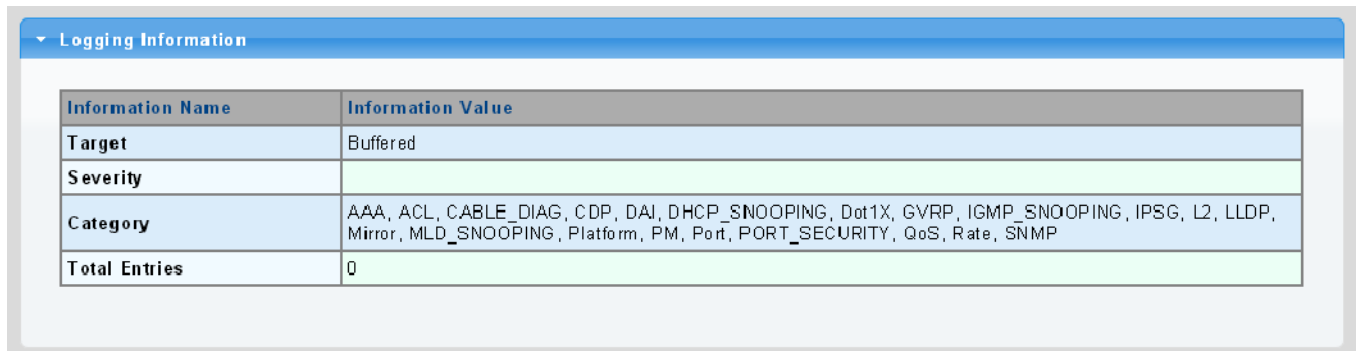
Figure 4-2-17: Logging Information Page Screenshot

The page includes the following fields:

Object	Description
• **Target**	Display the current log target.
• **Severity**	Display the current log severity.
• **Categery**	Display the current log category
• **Total Entries**	Display the current log entries
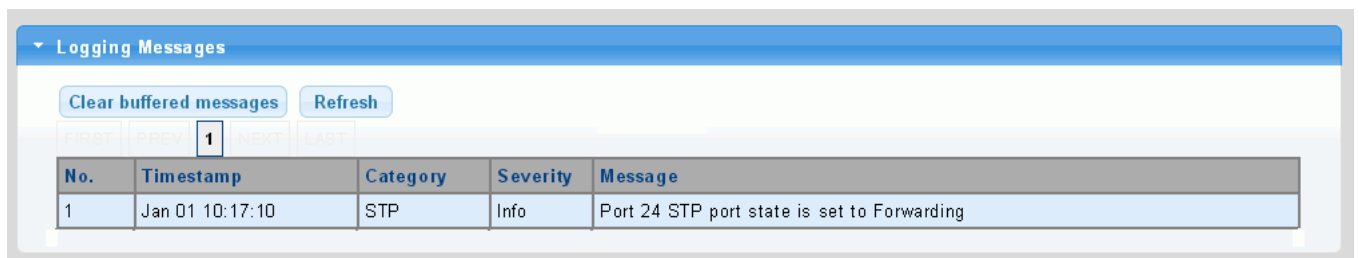
Figure 4-2-18: Logging Messages Page Screenshot

The page includes the following fields:

Object	Description
• **No.**	This is the number for logs.
• **Timestamp**	Display the time of log.
• **Category**	Display the category type.
• **Severity**	Display the severity type.
• **Message**	Display the log message.

Buttons

Clear buffered messages : Click to clear the log.

Refresh : Click to refresh the log.

4.2.6 SNMP Management

4.2.6.1 SNMP Overview

The **Simple Network Management Protocol (SNMP)** is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the **Transmission Control Protocol/Internet Protocol (TCP/IP)** protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of three key components: Network management stations (NMSs), SNMP agents, Management information base (MIB) and network-management protocol：

- ◦ **Network management stations (NMSs)**：Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.

- ◦ **Agents**：Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.

- ◦ **Management information base (MIB)**：A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.

- ◦ **network-management protocol**：A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- ◦ **Get --** Allows the NMS to retrieve an object instance from the agent.

- ◦ **Set --** Allows the NMS to set values for object instances within an agent.

- ◦ **Trap --** Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.
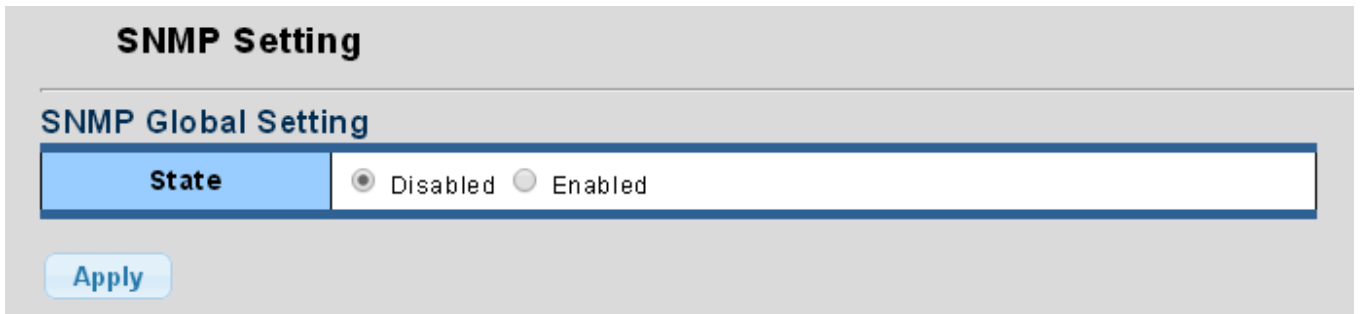
SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- ◦ **Write** = private
- ◦ **Read** = public

4.2.6.2 SNMP Setting

Configure SNMP setting on this page. The SNMP System global setting screens in Figure 4-2-19 & Figure 4-2-20 appear.

SNMP Setting

SNMP Global Setting

State	⦿ Disabled ◯ Enabled

Apply
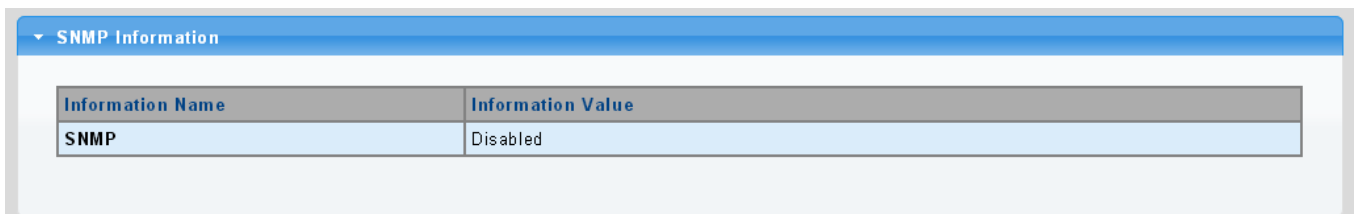
Figure 4-2-19: SNMP Global Setting Page Screenshot

The page includes the following fields:

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

Button

Apply : Click to apply changes.

SNMP Information

Information Name	Information Value
SNMP	Disabled
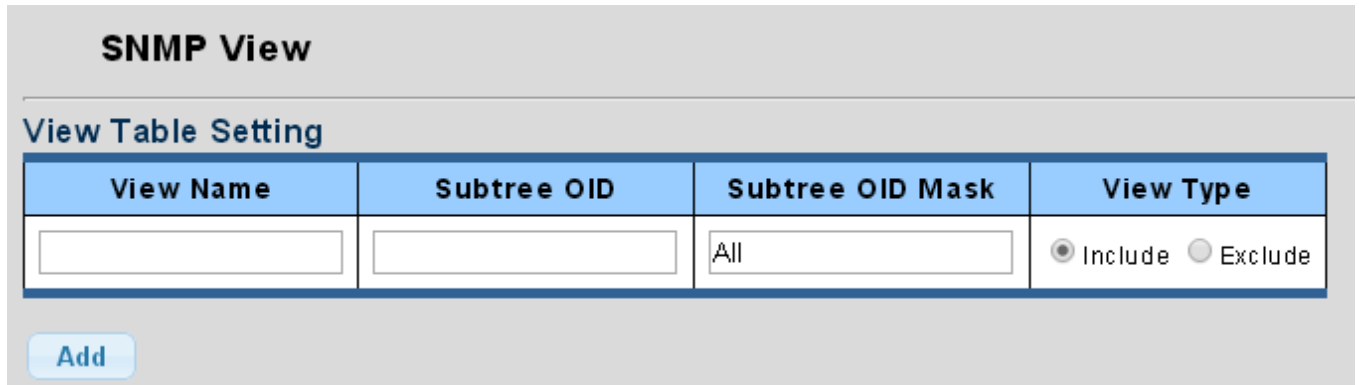
Figure 4-2-20: SNMP Information Page Screenshot

The page includes the following fields:

Object	Description
• **SNMP**	Display the current SNMP status

4.2.6.3 SNMP View

Configure SNMPv3 view table on this page. The entry index keys are **View Name** and **OID Subtree**. The SNMPv3 View Table Setting screens in Figure 4-2-21 and Figure 4-2-22 appear.
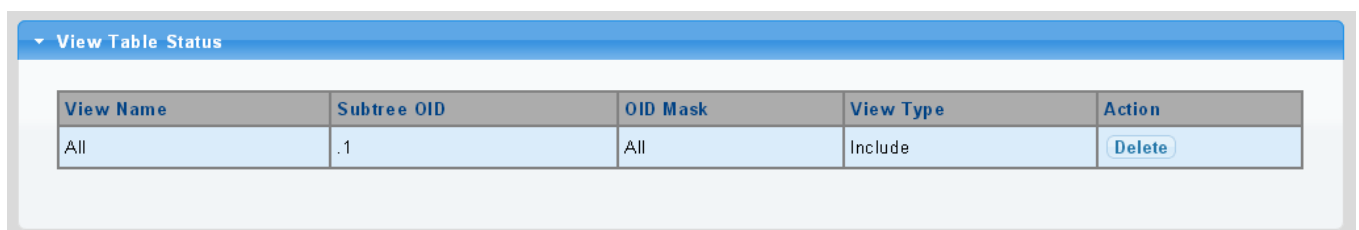
Figure 4-2-21: SNMPv3 View Table Setting Page Screenshot

The page includes the following fields:

Object	Description
• **View Name**	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 16.
• **Subtree OID**	The OID defining the root of the subtree to add to the named view. The allowed string content is digital number or asterisk(*).
• **Subtree OID Mask**	The bitmask identifies which positions in the specified object identifier are to be regarded as "wildcards" for the purpose of pattern-matching.
• **View Type**	Indicates the view type that this entry should belong to. Possible view type 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. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.

Button

Add : Click to add a new view entry.

Figure 4-2-22: SNMP View Table Status Page Screenshot

The page includes the following fields:

Object	Description
• **View Name**	Display the current SNMP view name
• **Subtree OID**	Display the current SNMP subtree OID
• **OID Mask**	Display the current SNMP OID mask
• **View Type**	Display the current SNMP view type
• **Action**	**Delete** : Delete the view table entry.

4.2.6.4 SNMP Access Group

Configure SNMPv3 access group on this page. The entry index keys are **Group Name**, **Security Model** and **Security Level**. The SNMPv3 Access Group Setting screens in Figure 4-2-23 & Figure 4-2-24 appear.
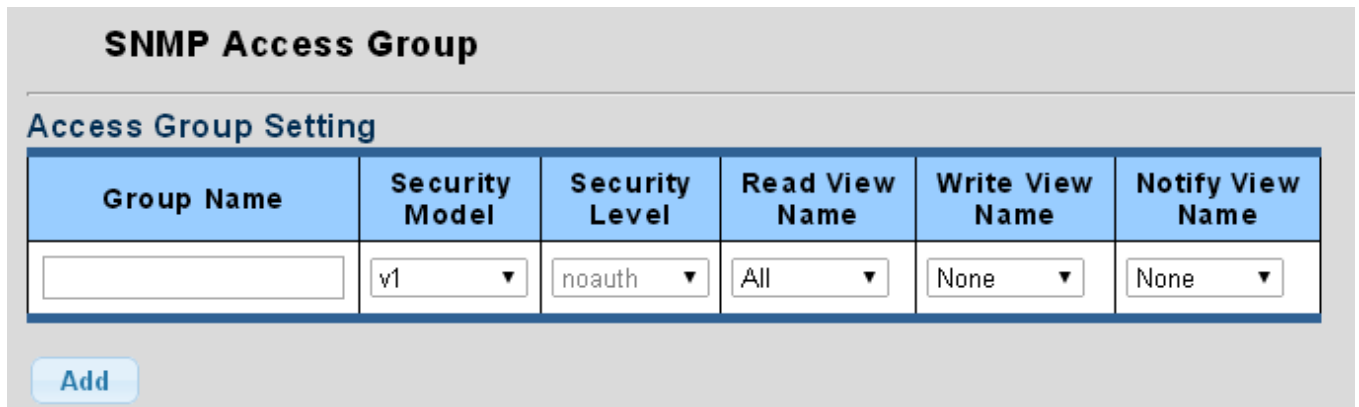
Figure 4-2-23: SNMPv3 Access Group Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 16.
• **Security Model**	Indicates the security model that this entry should belong to. Possible security models are: ■ **v1**: Reserved for SNMPv1. ■ **v2c**: Reserved for SNMPv2c. ■ **V3**: Reserved for SNMPv3 or User-based Security Model (USM)
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are: ■ **Noauth**: None authentication and none privacy security levels are assigned to the group. ■ **auth**: Authentication and none privacy.

	■ **priv**: Authentication and privacy. **Note: The Security Level applies to SNNPv3 only.**
• **Read View Name**	Read view name is the name of the view in which you can only view the contents of the agent. The allowed string length is 1 to 16.
• **Write View Name**	Write view name is the name of the view in which you enter data and configure the contents of the agent. The allowed string length is 1 to 16.
• **Notify View Name**	Notify view name is the name of the view in which you specify a notify, inform, or trap.

Button

Add : Click to add a new access entry.
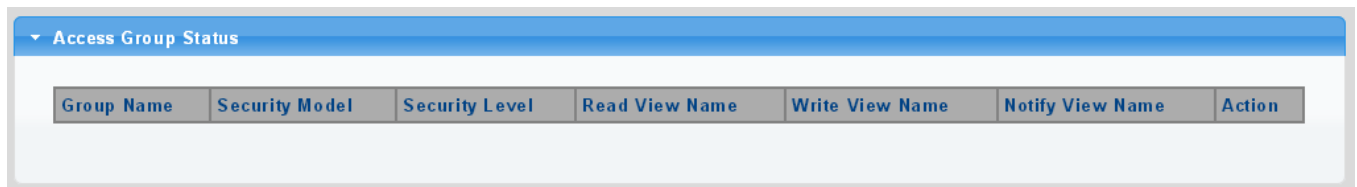
Figure 4-2-24: SNMP view Table Status Page Screenshot

The page includes the following fields:

Object	Description
• **Group Name**	Display the current SNMP access group name
• **Security Model**	Display the current security model
• **Security Level**	Display the current security level
• **Read View Name**	Display the current read view name
• **Write View Name**	Display the current write view name
• **Notify View Name**	Display the current notify view name
• **Action**	Delete : Delete the access group entry.

4.2.6.5 SNMP Community

Configure SNMP Community on this page. The SNMP Community screens in Figure 4-2-25 & Figure 4-2-26 appear.

Figure 4-2-25: Community Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Community Name**	Indicates the community read/write access string to permit access to SNMP agent. The allowed string length is 0 to 16.
• **Community Mode**	Indicates the SNMP community supported mode. Possible versions are: ■ **Basic**: Set SNMP community mode supported version 1 and 2c. ■ **Advanced**: Set SNMP community mode supported version 3.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 16.
• **View Name**	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 16.
• **Access Right**	Indicates the SNMP community type operation. Possible types are: **RO=Read-Only**: Set access string type in read-only mode. **RW=Read-Write**: Set access string type in read-write mode.

Button

Add : Click to add a new community name.

Figure 4-2-26: Community Status Page Screenshot

The page includes the following fields:

Object	Description
• **Community Name**	Display the current community type.
• **Group Name**	Display the current SNMP access group's name.
• **View Name**	Display the current view name.
• **Access Right**	Display the current access type.
• **Delete**	Delete : Delete the community entry.

4.2.6.6 SNMP User

Configure SNMPv3 users table on this page. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view. The entry index key is **User Name**. The SNMPv3 User Setting screens in Figure 4-2-27 & Figure 4-2-28 appear.

Figure 4-2-27: SNMPv3 Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 16.
• **Group**	The SNMP Access Group. A string identifying the group name that this entry should belong to.
• **Privilege Mode**	Indicates the security model that this entry should belong to. Possible security models are: ■ **NoAuth**: None authentication and none privacy. ■ **Auth**: Authentication and none privacy. ■ **Priv**: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means you must first ensure that the value is set correctly.
• **Authentication Protocol**	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: ■ **None**: None authentication protocol.

	■ **MD5**: An optional flag to indicate that this user using MD5 authentication protocol.
	■ **SHA**: An optional flag to indicate that this user using SHA authentication protocol.
	The value of security level cannot be modified if entry already exists. That means you must first ensure that the value is set correctly.
• **Authentication Password**	A string identifying the authentication pass phrase. For both MD5 and SHA authentication protocol, the allowed string length is 8 to 16.
• **Encryption Protocol**	Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are:
	■ **None**: None privacy protocol.
	■ **DES**: An optional flag to indicate that this user using DES authentication protocol.
• **Encryption Key**	A string identifying the privacy pass phrase. The allowed string length is 8 to 16.

Button

Add : Click to add a new user entry.
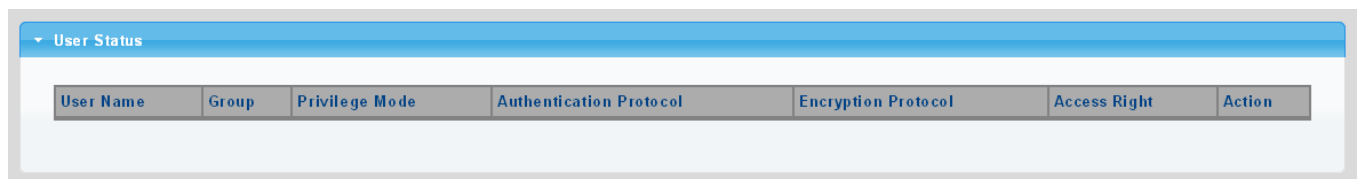
Figure 4-2-28: SNMPv3 Users Status Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	Display the current user name.
• **Group**	Display the current group.
• **Privilege Mode**	Display the current privilege mode.
• **Authentication Protocol**	Display the current authentication protocol.
• **Encryption Protocol**	Display the current encryption protocol.
• **Access Right**	Display the current access right.
• **Action**	**Delete** : Delete the user entry.

4.2.6.7 SNMPv1, 2 Notification Recipients

Configure SNMPv1 and 2 notification recipients on this page. The SNMPv1, 2 Notification Recipients screens in Figure 4-2-29 & Figure 4-2-30 appear.

Figure 4-2-29: SNMPv1, 2 Notification Recipients Page Screenshot

The page includes the following fields:

Object	Description
• **Server Address**	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
• **SNMP 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.
• **Notify Type**	Set the notify type in traps or informs.
• **Community Name**	Indicates the community access string when send SNMP trap packet.
• **UDP Port**	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is **1~65535**.
• **Time Out**	Indicates the SNMP trap inform timeout. The allowed range is **1** to **300**.
• **Retries**	Indicates the SNMP trap inform retry times. The allowed range is **1** to **255**.

Button

Add : Click to add a new SNMPv1, 2 host entry.

Figure 4-2-30: SNMPv1, 2 Host Status Page Screenshot

The page includes the following fields:

Object	Description
• **Server Address**	Display the current server address.
• **SNMP Version**	Display the current SNMP version.
• **Notify Type**	Display the current notify type.
• **Community Name**	Display the current community name.
• **UDP Port**	Display the current UDP port.
• **Time Out**	Display the current time out.
• **Retry**	Displays the current retry times.
• **Action**	**Delete** : Delete the SNMPv1, 2 host entry.

4.2.6.8 SNMPv3 Notification Recipients

Configure SNMPv3 notification recipients on this page. The SNMPv1, 2 Notification Recipients screens in Figure 4-2-31 & Figure 4-2-32 appear.

Figure 4-2-31: SNMPv3 Notification Recipients Page Screenshot

The page includes the following fields:

Object	Description
• **Server Address**	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
• **Notify Type**	Set the notify type in traps or informs.
• **User Name**	Indicates the user string when send SNMP trap packet.
• **UDP Port**	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message

		via this port, the port range is **1~65535**.
• **Time Out**		Indicates the SNMP trap inform timeout. The allowed range is **1** to **300**.
• **Retries**		Indicates the SNMP trap inform retry times. The allowed range is **1** to **255**.

Button

Add : Click to add a new SNMPv3 host entry.
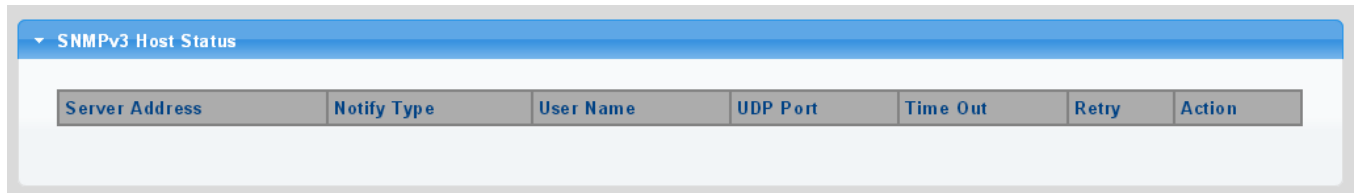
Figure 4-2-32: SNMPv3 Host Status Page Screenshot

The page includes the following fields:

Object	Description
• **Server Address**	Display the current server address.
• **Notify Type**	Displays the current notify type.
• **User Name**	Display the current user name.
• **UDP Port**	Display the current UDP port.
• **Time Out**	Display the current time out.
• **Retries**	Displays the current retry times.
• **Action**	**Delete** : Delete the SNMPv3 host entry.

4.2.6.9 SNMP Engine ID

Configure SNMPv3 Engine ID on this page. The entry index key is Engine ID. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. The SNMPv3 Engine ID Setting screens in Figure 4-2-33 & Figure 4-2-34 appear.

Figure 4-2-33: SNMPv3 Engine ID Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Engine ID**	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.

Button

 : Click to apply changes.

Figure 4-2-34: SNMPv3 Engine ID Status Page Screenshot

The page includes the following fields:

Object	Description
• **User Default**	Display the current status
• **Engine ID**	Display the current engine ID

69

4.2.6.10 SNMP Remote Engine ID

Configure SNMPv3 remote Engine ID on this page. The SNMPv3 Remote Engine ID Setting screens in Figure 4-2-35 & Figure 4-2-36 appear.

Figure 4-2-35: SNMPv3 Remote Engine ID Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Remote IP Address**	Indicates the SNMP remote engine ID address. It allows a valid IP address in dotted decimal notation ('x.y.z.w').
• **Engine ID**	An octet string identifying the engine ID that this entry should belong to.

Buttons

Add : Click to add a new Engine ID entry.

Figure 4-2-36: SNMPv3 Remote Engine ID Status Page Screenshot

The page includes the following fields:

Object	Description
• **Remote IP Address**	Display the current remote IP address
• **Remote Engine ID**	Display the current engine ID
• **Action**	Delete : Delete the remote IP address entry.

4.3 Port Management

Use the Port Menu to display or configure the PoE Managed Switch's ports. This section has the following items:

- **Port Configuration**   Configures port configuration settings
- **Port Counters**   Lists Ethernet and RMON port statistics
- **Bandwidth Utilization**   Display current bandwidth utilization
- **Port Mirroring**   Sets the source and target ports for mirroring
- **Jumbo Frame**   Set the jumbo frame on the switch
- **Port Error Disable Configuration**   Configures port error disable settings
- **Port Error Disabled Status**   Disable port error status

4.3.1 Port Configuration

This page displays current port configurations and status. Ports can also be configured here. The table has one row for each port on the selected switch in a number of columns, which are:

The Port Configuration screens in Figure 4-3-1 & Figure 4-3-2 appear.
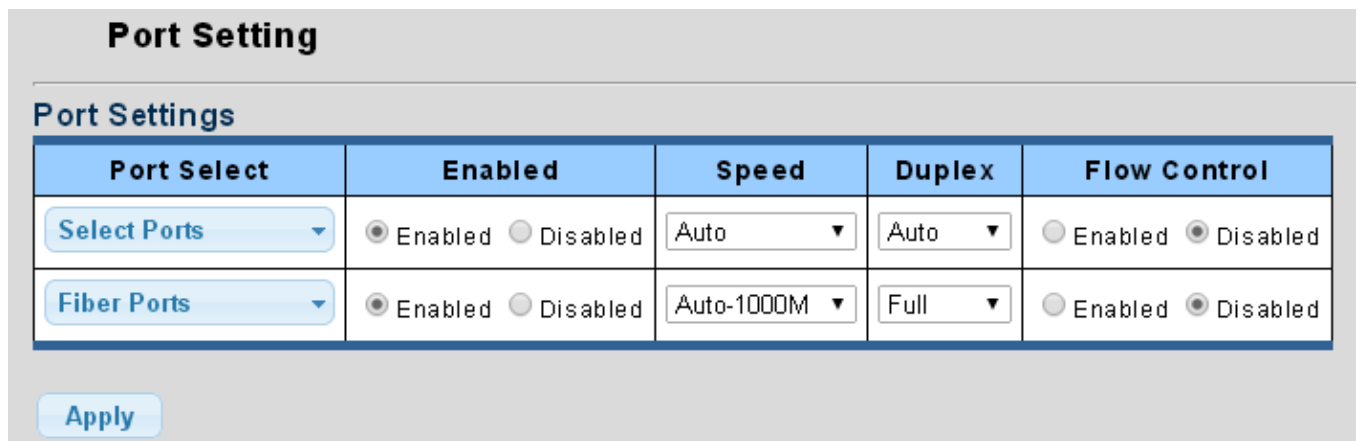
Figure 4-3-1: Port Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number for this drop down list.
• **Enabled**	Indicates the port state operation. Possible state are: **Enabled** - Start up the port manually. **Disabled** – Shut down the port manually.
• **Speed**	Select any available link speed for the given switch port. Draw the menu bar to select the mode. ■ **Auto** - Setup Auto negotiation.

	■ **Auto-10M** - Setup 10M Auto negotiation.
	■ **Auto-100M** - Setup 100M Auto negotiation.
	■ **Auto-1000M** - Setup 1000M Auto negotiation.
	■ **Auto-10/100M** - Setup 10/100M Auto negotiation.
	■ **10M** - Setup 10M Force mode.
	■ **100M** - Setup 100M Force mode.
	■ **1000M** - Setup 1000M Force mode.
• **Duplex**	Select any available link duplex for the given switch port. Draw the menu bar to select the mode.
	■ **Auto** - Setup Auto negotiation.
	■ **Full** - Force sets Full-Duplex mode.
	■ **Half** - Force sets Half-Duplex mode.
• **Flow Control**	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner.
	When a fixed-speed setting is selected, that is what is used.
	Current Rx column indicates whether pause frames on the port are obeyed.
	Current Tx column indicates whether pause frames on the port are transmitted.
	The Rx and Tx settings are determined by the result of the last Auto-Negotiation.
	Check the configured column to use flow control.
	This setting is related to the setting for Configured Link Speed.
	Possible state are:
	Enabled – Enable the flow control function.
	Disabled – Disable the flow control function.

Button

Apply : Click to apply changes.

▾ Port Status

Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
GE1	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE2	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE3	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE4	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE5	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE6	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE7	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE8	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE9	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE10	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE11	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE12	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE13	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE14	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE15	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE16	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE17	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE18	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE19	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE20	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE21	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE22	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE23	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE24	Edit	Enabled	UP	A-1000M	A-Full	Disabled	Disabled
GE25	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE26	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled

Figure 4-3-2: Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	This is the logical port number for this row.
• **Description**	Click **Edit** to indicate the port name.
• **Enable State**	Display the current port state.
• **Link Status**	Display the current link status.
• **Speed**	Display the current speed status of the port.
• **Duplex**	Display the current duplex status of the port.
• **Flow Control Configuration**	Display the current flow control configuration of the port.
• **Flow Control Status**	Display the current flow control status of the port.

4.3.2 Port Counters

This page provides an overview of traffic and trunk statistics for all switch ports. The Port Statistics screens in Figure 4-3-3, Figure 4-3-4, Figure 4-3-5 & Figure 4-3-6 appear.
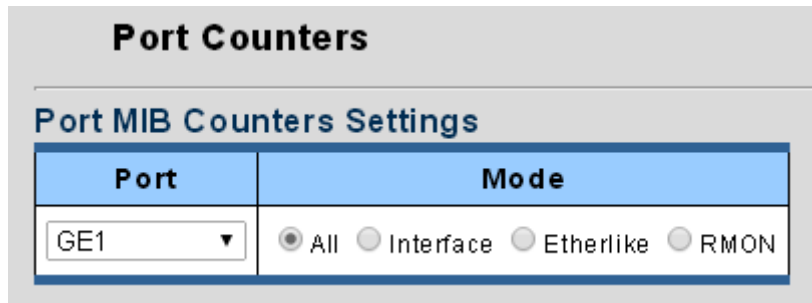
Figure 4-3-3: Port MIB Counters Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number for this drop down list.
• **Mode**	Select port counters mode. Options: ● All ● Interface ● Etherlike ● RMON
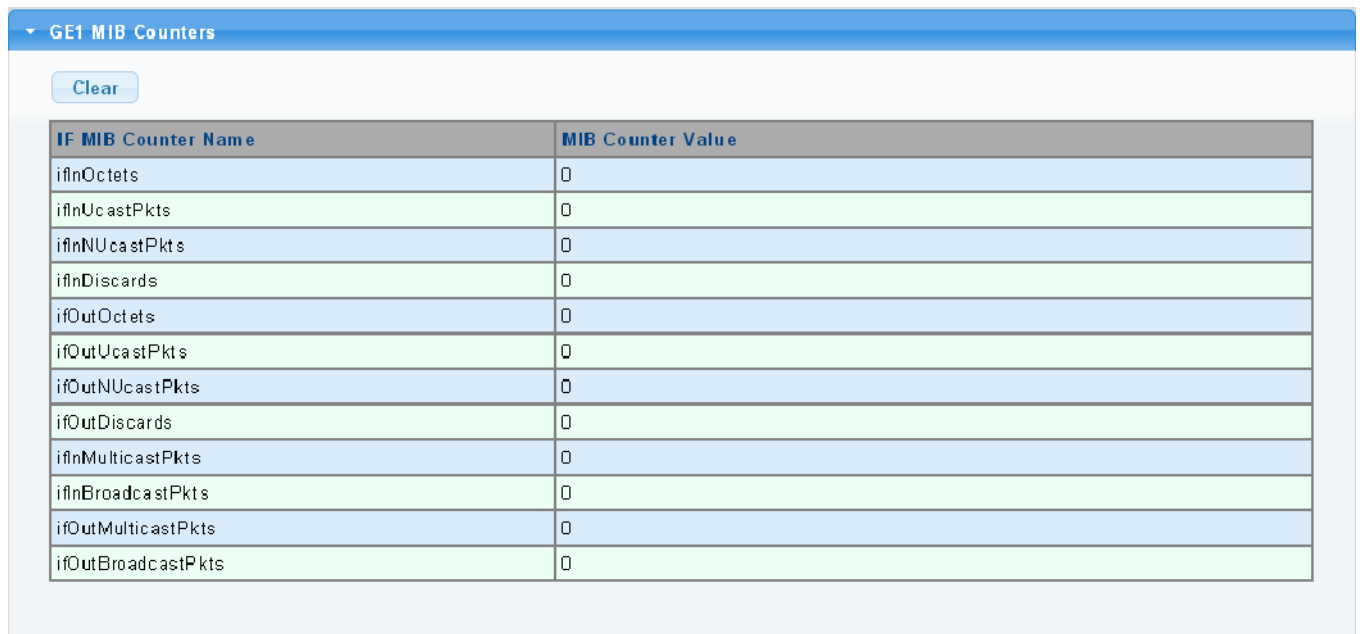
Figure 4-3-4: Interface Counters Page Screenshot

74

Object	Description
• **ifInOctets** **(Received Octets)**	The total number of octets received on the interface, including framing characters.
• **ifInUcastPkts** **(Received Unicast** **Packets)**	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
• **ifInNUcastPkts** **(Received Nuknown** **Unicast Packets)**	The number of packets received via the interfaces which were discarded because of an unknown or unsupported protocol.
• **ifInDiscards** **(Received Discards** **Packets)**	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
• **ifOutOctets** **(Transmit Octets)**	The total number of octets transmitted out of the interface, including framing characters.
• **ifOutUcastPkts** **(Transmit Unicast** **Packets)**	The total number of packets that higher-level protocols requested is transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
• **ifOutNUcastPkts** **(Transmit Nuknown** **Unicast Packets)**	The total number of packets that higher-level protocols requested betransmitted to a subnetwork-unicast address, including those that were discarded or not sent.
• **ifOutDiscards** **(Transmit Discards** **Packets)**	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to ahigher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
• **ifInMulticastPkts** **(Received Multicast** **Packets)**	The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were addressed to a multicast address at this sub-layer.
• **ifInBroadcastPkts** **(Received Broadcast** **Packets)**	The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were addressed to a broadcast address at this sub-layer.
• **ifOutMulticastPkts** **(Transmit Multicast** **Packets)**	The total number of packets that higher-level protocols requested betransmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
• **ifOutBroadcastPkts** **(Transmit Broadcast** **Packets)**	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

Figure 4-3-5: Ethernet link Counters Page Screenshot

Object	Description
• **dot3StatsAlignmentErrors**	The number of alignment errors (missynchronized data packets).
• **dot3StatsFCSErrors**	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
• **dot3StatsSingleCollisionFrames**	The number of successfully transmitted frames for which transmission isinhibited by exactly one collision.
• **dot3StatsMultipleCollisionFrames**	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
• **dot3StatsDeferredTransmissions**	A count of frames for which the first transmission attempt on a particularinterface is delayed because the medium was busy.
• **dot3StatsLateCollisions**	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
• **dot3StatsExcessiveCollisions**	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
• **dot3StatsFrameTooLongs**	A count of frames received on particular interfaces that exceed the maximum permitted frame size.
• **dot3StatsSymbolErrors**	The number of received and transmitted symbol errors.
• **dot3ControlInUnknownOpcodes**	The number of received control unknown opcodes
• **dot3InPauseFrames**	The number of received pause frames
• **dot3OutPauseFrames**	The number of transmitted pause frames

Figure 4-3-6: RMON Counters Page Screenshot

Object	Description
• **etherStatsDropEvents**	The total number of events in which packets were dropped due to lack of resources.
• **etherStatsOctets**	The total number of octets received and transmitted on the interface, including framing characters.
• **etherStatsPkts**	The total number of packets received and transmitted on the interface.
• **etherStatsBroadcastPkts**	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
• **etherStatsMulticastPkts**	The total number of good frames received that were directed to this multicast address.
• **etherStatsCRCAlignErrors**	The number of CRC/alignment errors (FCS or alignment errors).
• **etherStatsUnderSizePkts**	The total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed.
• **etherStatsOverSizePkts**	The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed.
• **etherStatsFragments**	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
• **etherStatsJabbers**	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS

	or alignment error.
• **etherStatsCollisions**	The best estimate of the total number of collisions on this Ethernet segment.
• **etherStatsPkts64Octets**	The total number of frames (including bad packets) received andtransmitted that were 64 octets in length (excluding framing bits but including FCS octets).
• **etherStatsPkts65to127Octets** • **etherStatsPkts128to255Octets** • **etherStatsPkts256to511Octets** • **etherStatsPkts512to1023Octets** • **etherStatsPkts1024to1518Octets**	The total number of frames (including bad packets) received andtransmitted where the numbers of octets fall within the specified range (excluding framing bits but including FCS octets).

4.3.3 Bandwidth Utilization

The **Bandwidth Utilization** page displays the percentage of the total available bandwidth being used on the ports. Bandwith utilization statistics can be viewed using a line graph. The Bandwidth Utilization screen in Figure 4-3-7 appears.

To view the port utilization, click on the **Port Management** folder and then the **Bandwidth Utilization** link:

Figure 4-3-7: Port Bandwidth Utilization Page Screenshot

The page includes the following fields:

Object	Description
• **Refresh Period**	This shows the period interval between last and next refresh. **Options:** ■ 2 sec ■ 5 sec ■ 10 sec
• **IFG**	Allow user to **enable** or **disable** this function

4.3.4 Port Mirroring

Configure port Mirroring on this page. This function provide to monitoring network traffic that forwards a copy of each incoming or outgoing packet from one port of a network Switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

- To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.
- The PoE Managed Switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.
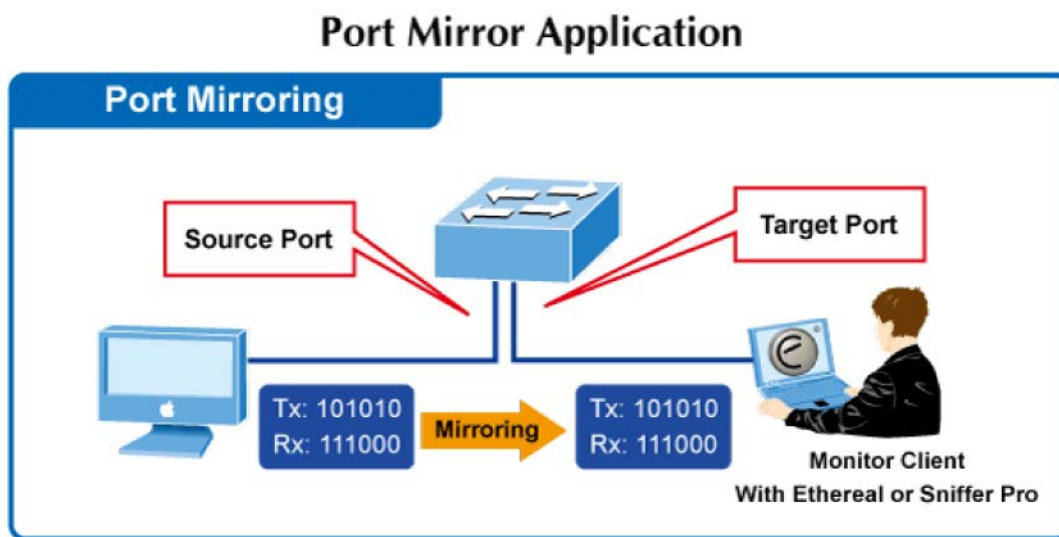
Figure 4-3-8: Port Mirror Application

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

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

Mirror Port Configuration

The Port Mirror Configuration screens in Figure 4-3-9 & Figure 4-3-10 appear.

Figure 4-3-9: Port Mirroring Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Session ID**	Set the port mirror session ID. Possible ID are: **1** to **4**.
• **Monitor Session State**	Enable or disable the port mirroring function.
• **Destination Port**	Select the port to mirror destination port.
• **Allow-ingress**	Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port.
• **Sniffer RX Ports**	Frames received at these ports are mirrored to the mirroring port. Frames transmitted are not mirrored.
• **Sniffer TX Ports**	Frames transmitted from these ports are mirrored to the mirroring port. Frames received are not mirrored.

Button

Apply : Click to apply changes.

Figure 4-3-10: Mirroring Status Page Screenshot

The page includes the following fields:

Object	Description
• **Session ID**	Display the session ID.
• **Destination Port**	This is the mirroring port entry.
• **Ingress State**	Display the ingress state.
• **Source TX Port**	Display the current TX ports.
• **Source RX Port**	Display the current RX ports.

4.3.5 Jumbo Frame

This page provides to select the maximum frame size allowed for the switch port. The Jumbo Frame screen in Figure 4-3-11 & Figure 4-3-12 appear.

Figure 4-3-11: Jumbo Frame Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Jumbo Frame (Bytes)**	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 64 bytes to 9216 bytes.

Button

 : Click to apply changes.

Figure 4-3-12: Jumbo Frame Information Page Screenshot

The page includes the following fields:

Object	Description
• **Jumbo**	Display the current maximum frame size.

4.3.6 Port Error Disabled Configuration

This page provides to set port error disable function. The Port Error Disable Configuration screens in Figure 4-3-13 & Figure 4-3-14 appear.

Figure 4-3-13: Error Disabled Recovery Page Screenshot

The page includes the following fields:

Object	Description
• **Recovery Interval**	The period (in seconds) for which a port will be kept disabled in the event of a port error is detected (and the port action shuts down the port). Default is 300 seconds.
• **BPDU Guard**	Enable or disable the port error disabled function to check status by BPDU guard.
• **Self Loop**	Enable or disable the port error disabled function to check status by self loop.
• **Broadcast Flood**	Enable or disable the port error disabled function to check status by broadcast flood.
• **Unknown Multicast Flood**	Enable or disable the port error disabled function to check status by unknown multicast flood.
• **Unicast Flood**	Enable or disable the port error disabled function to check status by unicast flood.
• **ACL**	Enable or disable the port error disabled function to check status by ACL.
• **Port Security Violation**	Enable or disable the port error disabled function to check status by port security violation.
• **DHCP Rate Limit**	Enable or disable the port error disabled function to check status by DHCP rate limit
• **ARP Rate Limt**	Enable or disable the port error disabled function to check status by ARP rate limit

Button

Apply : Click to apply changes.

Error Disable Information	
Information Name	**Information Value**
Recovery Interval	300
BPDU Guard	Disabled
Self Loop	Disabled
Broadcast Flood	Disabled
Unknown Multicast Flood	Disabled
Unicast Flood	Disabled
ACL	Disabled
Port Security Violation	Disabled
DHCP Rate Limit	Disabled
ARP Rate Limit	Disabled

Figure 4-3-14: Error Disabled Information Page Screenshot

The page includes the following fields:

Object	Description
• **Recovery Interval**	Display the current recovery interval time.
• **BPDU Guard**	Display the current BPDU guard status.
• **Self Loop**	Display the current self loop status.
• **Broadcast Flood**	Display the current broadcst flood status.
• **Unknown Multicast Flood**	Display the current unknown multicast flood status.
• **Unicast Flood**	Display the current unicast flood status.
• **ACL**	Display the current ACL status.
• **Port Security Violation**	Display the current port security violation status.
• **DHCP Rate Limit**	Display the current DHCP rate limit status.
• **ARP Rate Limt**	Display the current ARP rate limit status.

4.3.7 Port Error Disabled Status

This page provides disable that transitions a port into error disable and the recovery options. The ports were disabled by some protocols such as BPDU Guard, Loopback and UDLD. The Port Error Disable screen in Figure 4-3-15 appears.
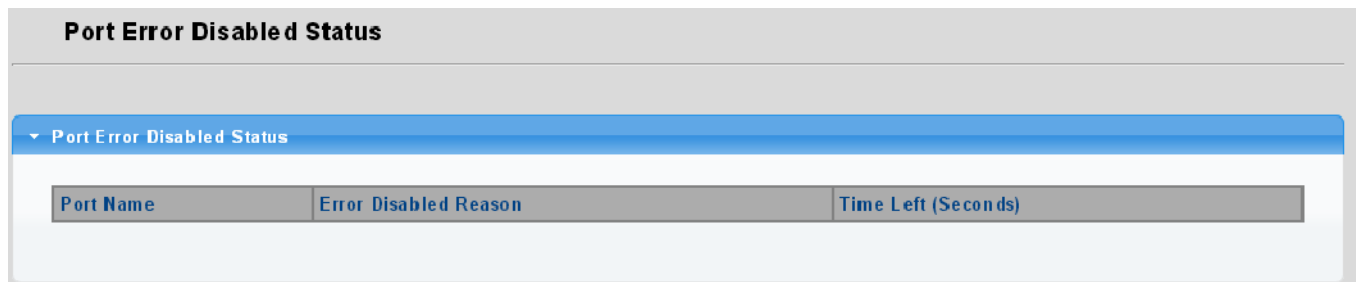
Figure 4-3-15: Port Error Disable Status Page Screenshot

The displayed counters are:

Object	Description
• **Port Name**	Displays the port for error disable status.
• **Error Disabled Reason**	Display the error disabled reason of the port.
• **Time Left (Seconds)**	Display the time left in seconds.

4.4 Link Aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Groups (LAGs). Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG, can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

Aggregated Links can be assigned manually (**Port Trunk**) or automatically by enabling Link Aggregation Control Protocol (**LACP**) on the relevant links.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, Duplex setting, etc.

The device supports the following Aggregation links :

- **Static LAGs** (**Port Trunk**) – Force aggregared selected ports to be a trunk group.

- **Link Aggregation Control Protocol** (**LACP**) LAGs - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.
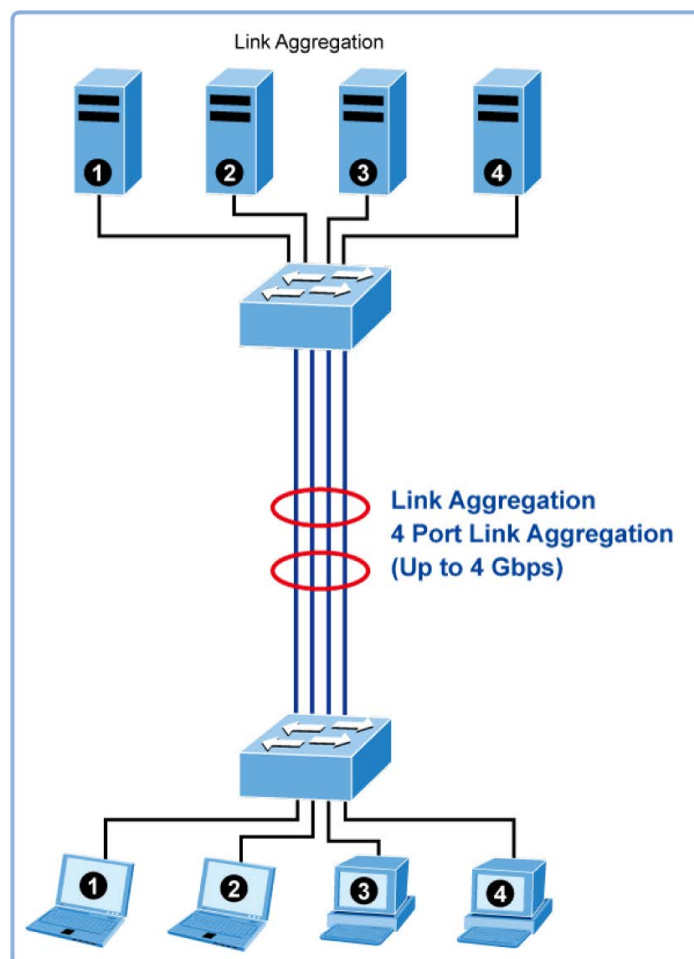
Figure 4-4-1: Link Aggregation

The **Link Aggregation Control Protocol (LACP)** provides a standardized means for exchanging information between Partner Systems that require high speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refer to the IEEE 802.3ad standard.

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 8 consecutive ports into a single dedicated connection between any two the Switch or other Layer 2 switches. However, before making any physical connections between devices, use the Link aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ-45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
- Ports can only be assigned to one link aggregation.
- The ports at both ends of a connection must be configured as link aggregation ports.
- None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
- Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of 8 ports to be aggregated at the same time. The PoE Managed Switch support Gigabit Ethernet ports (up to 8 groups). If the group is defined as a LACP static link aggregationing group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregationing group, then the number of ports must be the same as the group member ports.

Use the Link Aggregation Menu to display or configure the Trunk function. This section has the following items:

- **LAG Setting**   Configures load balance algorithm configuration settings
- **LAG Management**   Configures LAG configuration settings
- **LAG Port Setting**   Configures LAG port settings
- **LACP Setting**   Configures LACP priority settings
- **LACP Port Setting**   Configure LACP configuration settings
- **LAG Status**   Display LAG status / LACP information

4.4.1 LAG Setting

This page allows configuring load balance algorithm configuration settings. The LAG Setting screens in Figure 4-4-2 & Figure 4-4-3 appear.
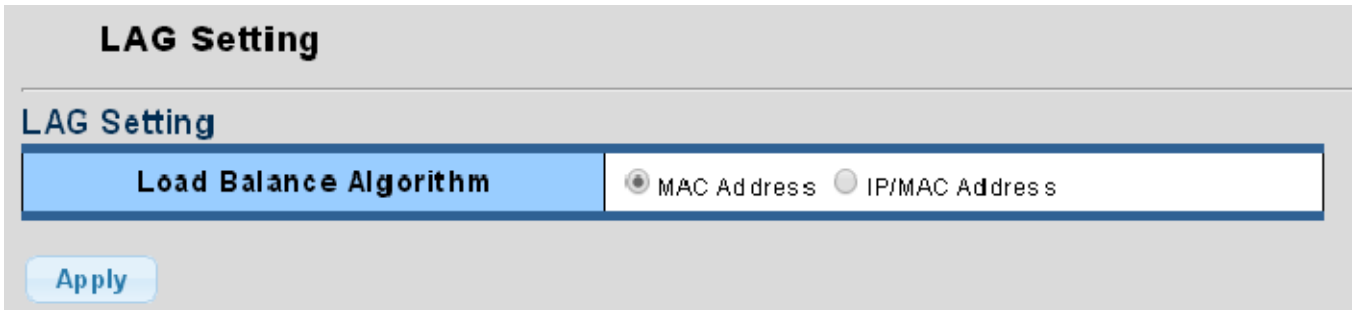
Figure 4-4-2: LAG Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Load Balance Algorithm**	Select load balance algorithm mode: ■ **MAC Address**: The MAC address can be used to calculate the port for the frame. ■ **IP/MAC Address**: The IP and MAC address can be used to calculate the port for the frame.

Button

Apply : Click to apply changes.
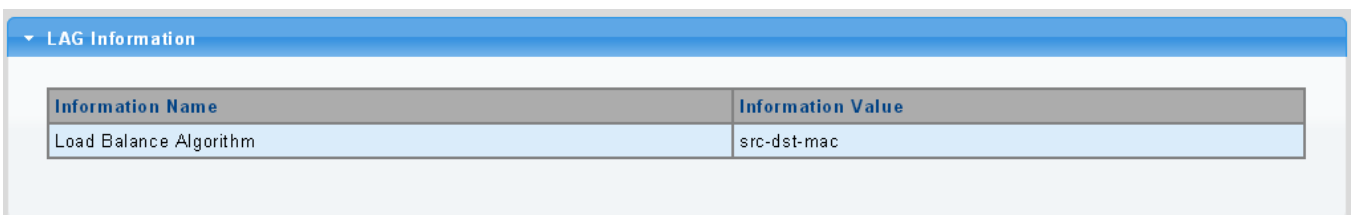
Figure 4-4-3: LAG Information Page Screenshot

The page includes the following fields:

Object	Description
• **Load Balance Algorithm**	Display the current load balance algorithn.

4.4.2 LAG Managment

This page is used to configure the LAG management. The LAG Management screens in & appear.

Figure 4-4-4: LAG Management Page Screenshot

The page includes the following fields:

Object	Description
• **LAG**	Select LAG number for this drop down list, the available range is 1 to 8.
• **Name**	Indicates per LAG name and the available range are 32 characters.
• **Type**	Indicates the trunk type. **Static**: Force aggregared selected ports to be a trunk group. **LACP**: LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.
• **Ports**	Select port number for this drop down list to esatablish Link Aggregation. The available range is 8 ports.

Figure 4-4-5: LAG Management Information Page Screenshot

The page includes the following fields:

Object	Description
• **LAG**	The LAG for the settings contained in the same row.
• **Name**	Display the current name.
• **Type**	Display the current type.
• **Link State**	Display the link state.
• **Active Member**	Display the active member.
• **Standby Member**	Display the standby member.
• **Modify**	Click [Edit] to modify LAG configuraiton.

4.4.3 LAG Port Setting

This page allows setting configuration for per LAG. The LAG Port setting screens in Figure 4-4-6 & Figure 4-4-7 appear.
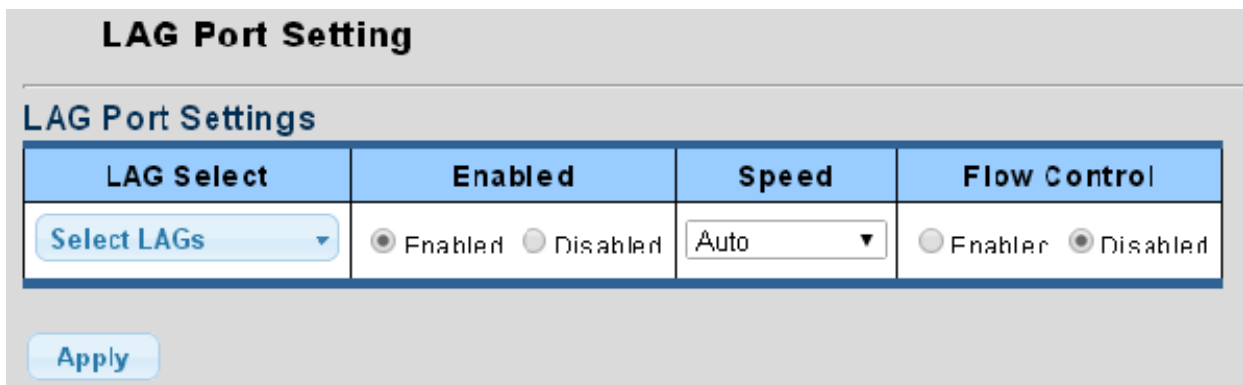
Figure 4-4-6: LAG Port Setting Information Page Screenshot

The page includes the following fields:

Object	Description
• **LAG Select**	Select LAG number for this drop down list.
• **Enabled**	Indicates the LAG Port Setting operation. Possible state are: **Enabled** - Start up the LAG manually. **Disabled** - Shutdown the LAG manually.
• **Speed**	Select any available link speed for the given switch port. Draw the menu bar to select the mode. ■ **Auto** - Setup Auto negotiation. ■ **Auto-10M** - Setup 10M Auto negotiation. ■ **Auto-100M** - Setup 100M Auto negotiation. ■ **Auto-1000M** - Setup 1000M Auto negotiation.

- ■ **Auto-10/100M** - Setup 10/100M Auto negotiation.
- ■ **10M** - Setup 10M Force mode.
- ■ **100M** - Setup 100M Force mode.
- ■ **1000M** - Setup 1000M Force mode.

• **Flow Control**	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. Current Rx column indicates whether pause frames on the port are obeyed. Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed. Possible state are: **Enabled** - Start up the Flow Control manually. **Disabled** - Shutdown the Flow Control manually.

Button

Apply : Click to apply changes.

LAG Port Status

LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
LAG1			Enabled		Auto	Auto	Disabled	Disabled
LAG2			Enabled		Auto	Auto	Disabled	Disabled
LAG3			Enabled		Auto	Auto	Disabled	Disabled
LAG4			Enabled		Auto	Auto	Disabled	Disabled
LAG5			Enabled		Auto	Auto	Disabled	Disabled
LAG6			Enabled		Auto	Auto	Disabled	Disabled
LAG7			Enabled		Auto	Auto	Disabled	Disabled
LAG8			Enabled		Auto	Auto	Disabled	Disabled

Figure 4-4-7: LAG Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **LAG**	The LAG for the settings contained in the same row.
• **Description**	Display the current description.
• **Port Type**	Display the current port type.
• **Enable State**	Display the current enable state.
• **Link Status**	Display the link status of per LAG group.

• **Speed**	Display the current speed.
• **Duplex**	Display the current duplex mode.
• **Flow Control Config**	Display the current flow control configuration.
• **Flow Control Status**	Display the current flow control status.

4.4.4 LACP Setting

This page is used to configure the LACP system priority setting. The LACP Setting screens in Figure 4-4-8 & Figure 4-4-9 appear.
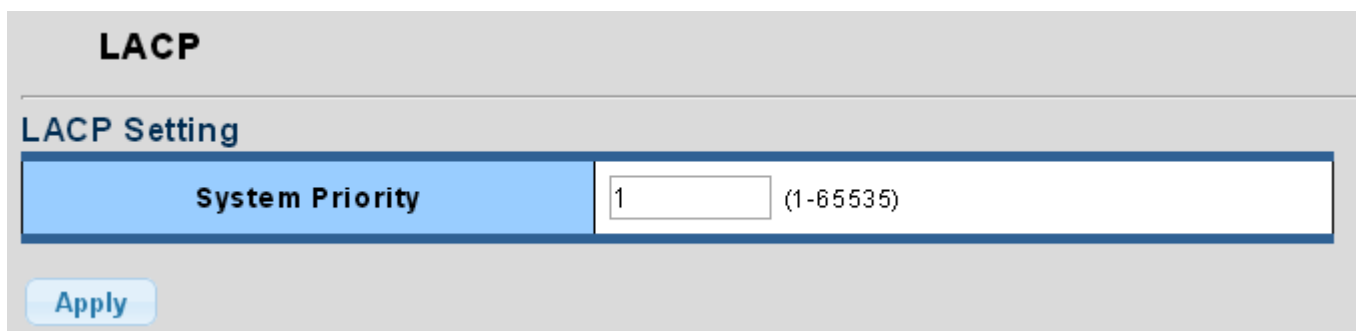
Figure 4-4-8: LACP Setting Page Screenshot

The page includes the following fields:

Object	Description
• **System Priority**	A value which is used to identify the active LACP. The PoE Managed Switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group. The available options are 1 to 65535.

Button

Apply : Click to apply changes.
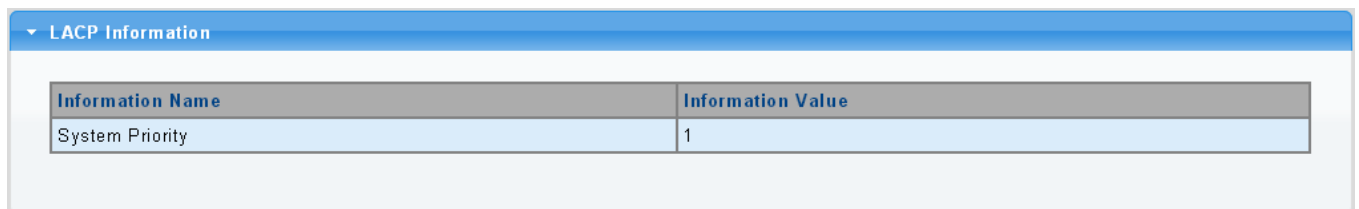
Figure 4-4-9: LACP Information Page Screenshot

The page includes the following fields:

Object	Description
• **System Priority**	Display the current system priority.

4.4.5 LACP Port Setting

This page is used to configure the LACP port setting. The LACP Port Setting screen in Figure 4-4-10 & Figure 4-4-11 appears.

LACP Port Setting

LACP Port Settings

Port Select	Priority	Timeout
Select Ports ▼	1 (1-65535)	○ Long ○ Short

Apply

Figure 4-4-10: LACP Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number for this drop down list to set LACP port setting.
• **Priority**	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. **Lower number means greater priority.**
• **Timeout**	The Timeout controls the period between BPDU transmissions. Short will transmit LACP packets each second, while Long will wait for 30 seconds before sending a LACP packet.

Button

Apply : Click to apply changes.

Figure 4-4-11: LACP Port Information Page Screenshot

The page includes the following fields:

Object	Description
• **Port Name**	The switch port number of the logical port.
• **Priority**	Display the current LACP priority parameter.
• **Timeout**	Display the current timeout parameter.

4.4.6 LAG Status

This page displays LAG status. The LAG Status screens in Figure 4-4-12 & Figure 4-4-13 appear.

Figure 4-4-12: LAG Status Page Screenshot

The page includes the following fields:

Object	Description
• **LAG**	Display the current trunk entry.
• **Name**	Display the current LAG name.
• **Type**	Display the current trunk type.
• **Link State**	Display the current link state.
• **Active Member**	Display the current active member.
• **Standby Member**	Display the current standby member.

LAG	Port	PartnerSysId	PnKey	AtKey	Sel	Mux	Receiv	PrdTx	AtState	PnState
LAG1	GE1	000000000000	03e8	03e8	U	DETACH	DFLT	FstPRD	A_G___F_	_TG_C_F_
LAG1	GE2	000000000000	03e8	03e8	U	DETACH	DFLT	FstPRD	A_G___F_	_TG_C_F_
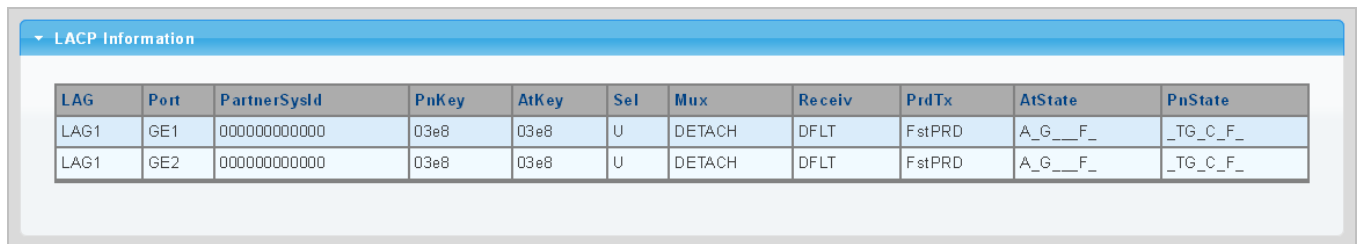
Figure 4-4-13: LACP Information Page Screenshot

The page includes the following fields:

Object	Description
• **LAG**	Display the current LAG ID.
• **Port**	Display the current port number.
• **PartnerSysId**	The system ID of link partner. This field would be updated when the port receives LACP PDU from link partner.
• **PnKey**	Port key of partner. This field would be updated when the port receives LACP PDU from link partner.
• **AtKey**	Port key of actor. The key is designed to be the same as trunk ID.
• **Sel**	LACP selection logic status of the port. ■ "**S**" means selected ■ "**U**" means unselected ■ "**D**" means standby
• **Mux**	LACP mux state machine status of the port. ■ "DETACH" means the port is in detached state ■ "WAIT" means waiting state ■ "ATTACH" means attach state ■ "CLLCT" means collecting state ■ "DSTRBT" means distributing state
• **Receiv**	LACP receive state machine status of the port. ■ "INIT" means the port is in initialize state ■ "PORTds" means port disabled state ■ "EXPR" means expired state ■ "LACPds" means LACP disabled state

	■ "DFLT" means defaulted state ■ "CRRNT" means current state.
• **PrdTx**	LACP periodic transmission state machine status of the port. ■ "no PRD" means the port is in no periodic state ■ "FstPRD" means fast periodic state ■ "SlwPRD" means slow periodic state ■ "PrdTX" means periodic TX state
• **AtState**	The actor state field of LACP PDU description. The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired". The contents could be true or false. If the contents are false, the web shows "_"; if the contents are true, the web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.
• **PnState**	The partner state field of LACP PDU description. The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired". The contents could be true or false. If the contents are false, the web shows "_"; if the contents are true, the web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.

4.5 VLAN

4.5.1 VLAN Overview

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.
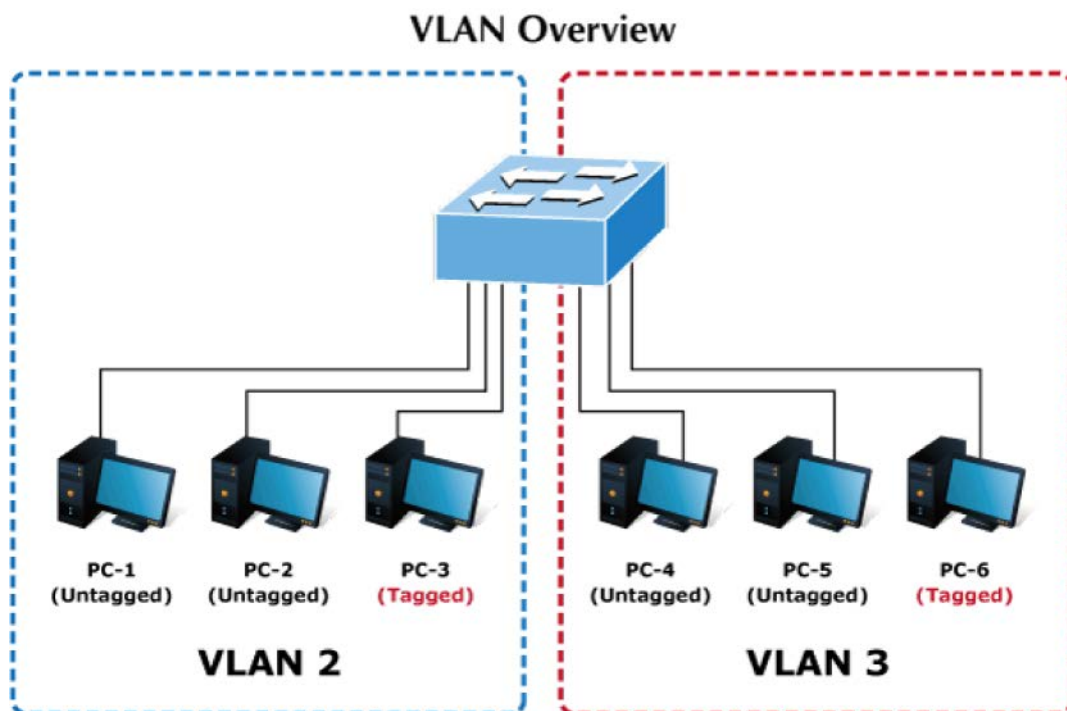
1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.

2. The PoE Managed Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

3. The PoE Managed Switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_ VLAN port member list. The DEFAULT_VLAN has a VID = 1.

This section has the following items:

- **Create VLAN**   Creates thn VLAN group.
- **Interface Settings**   Configures mode and PVID on the VLAN port.
- **Port to VLAN**   Configures the VLAN membership.
- **Port VLAN Membership**   Display the VLAN membership.
- **Protocol VLAN Group Setting**   Configures the protocol VLAN group.
- **Protocol VLAN Port Setting**   Configures the protocol VLAN port setting.

4.5.2 IEEE 802.1Q VLAN

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

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

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This PoE Managed Switch supports the following VLAN features:

- Up to 256 VLANs based on the IEEE 802.1Q standard
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices

■ **IEEE 802.1Q Standard**

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLAN allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either **tagging** or **untagging**.:

■ The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.

■ The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

■ 802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of **0x8100** in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of **VLAN ID (VID)**. The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag

User Priority	CFI	VLAN ID (VID)
3 bits	1 bits	12 bits

TPID (Tag Protocol Identifier)	TCI (Tag Control Information)
2 bytes	2 bytes

Preamble	Destination Address	Source Address	VLAN TAG	Ethernet Type	Data	FCS
	6 bytes	6 bytes	4 bytes	2 bytes	46-1500 bytes	4 bytes
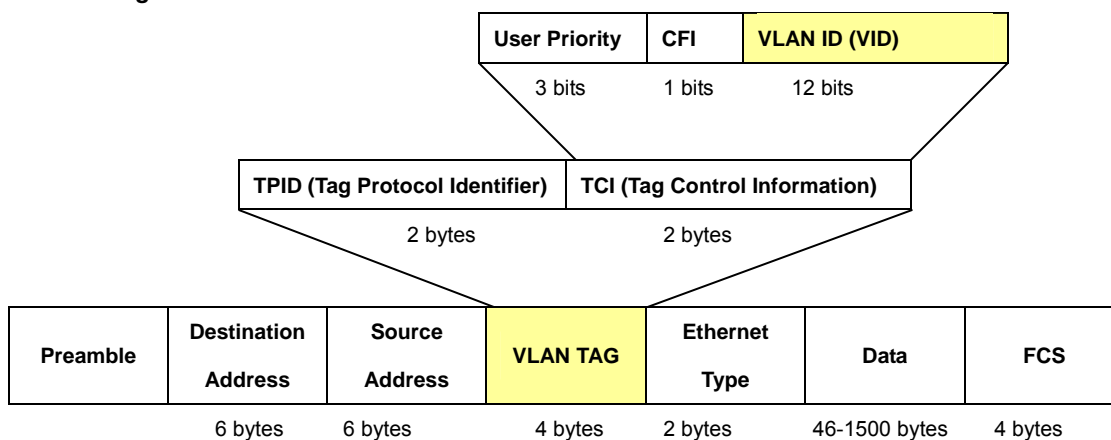
The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag

Dest. Addr.	Src. Addr.	Length/E. type	Data	Old CRC

Original Ethernet

Dest. Addr.	Src. Addr.	E. type	Tag	Length/E. type	Data	New CRC

New Tagged Packet
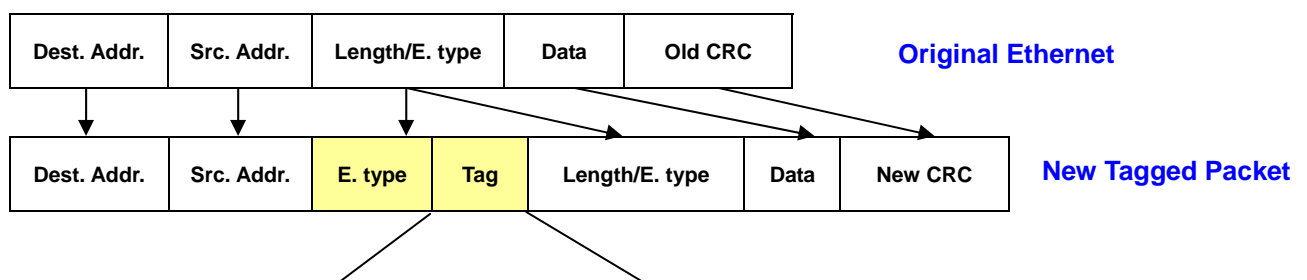
Priority	CFI	VLAN ID

■ Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLAN are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VID as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

■ Default VLANs

The Switch initially configures one VLAN, VID = 1, called **"default."** The factory default setting assigns all ports on the Switch to the **"default"**. As new VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

■ Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

> **Note**
> VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

■ VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

■ Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

■ Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

4.5.3 Create VLAN

Create/delete VLAN on this page. The screens in Figure 4-5-1 & Figure 4-5-2 appear.
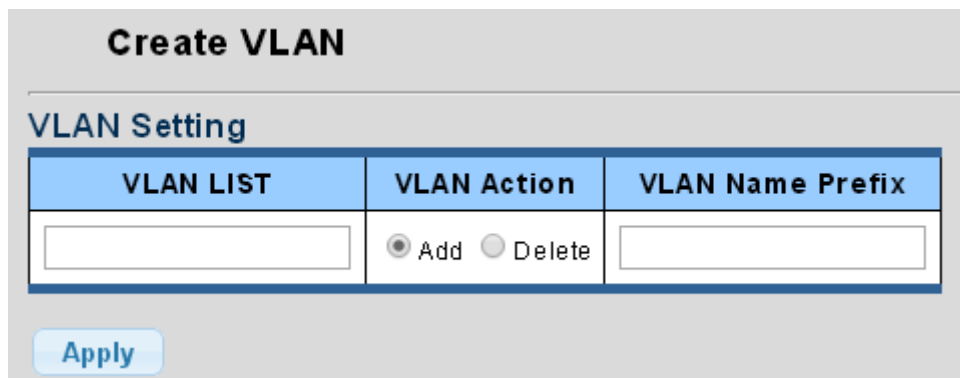
Figure 4-5-1: VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN List**	Indicates the ID of this particular VLAN.
• **VLAN Action**	This column allowed users to add or delete VLAN s.
• **VLAN Name Prefix**	Indicates the name of this particular VLAN, the options are 28 characters.

Button

Apply : Click to apply changes.

Figure 4-5-2: VLAN Table Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID entry.
• **VLAN Name**	Display the current VLAN ID name.
• **VLAN Type**	Display the current VLAN ID type.
• **Modify**	Click **Edit** to modify VLAN configuraiton.

4.5.4 Interface Settings

This Page is used for configuring the PoE Managed Switch port VLAN. The VLAN per Port Configuration Page contains fields for managing ports that are part of a VLAN. The port **default VLAN ID** (**PVID**) is configured on the VLAN Port Configuration Page. All untagged packets arriving to the device are tagged by the ports PVID.

Understand nomenclature of the Switch

■ **IEEE 802.1Q Tagged and Untagged**

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

- **Tagged:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

- **Untagged:** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Frame Income Frame Leave	Income Frame is **tagged**	Income Frame is **untagged**
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

Table 4-5-1: Ingress / Egress Port with VLAN VID Tag / Untag Table

■ **IEEE 802.1Q Tunneling (Q-in-Q)**

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

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.
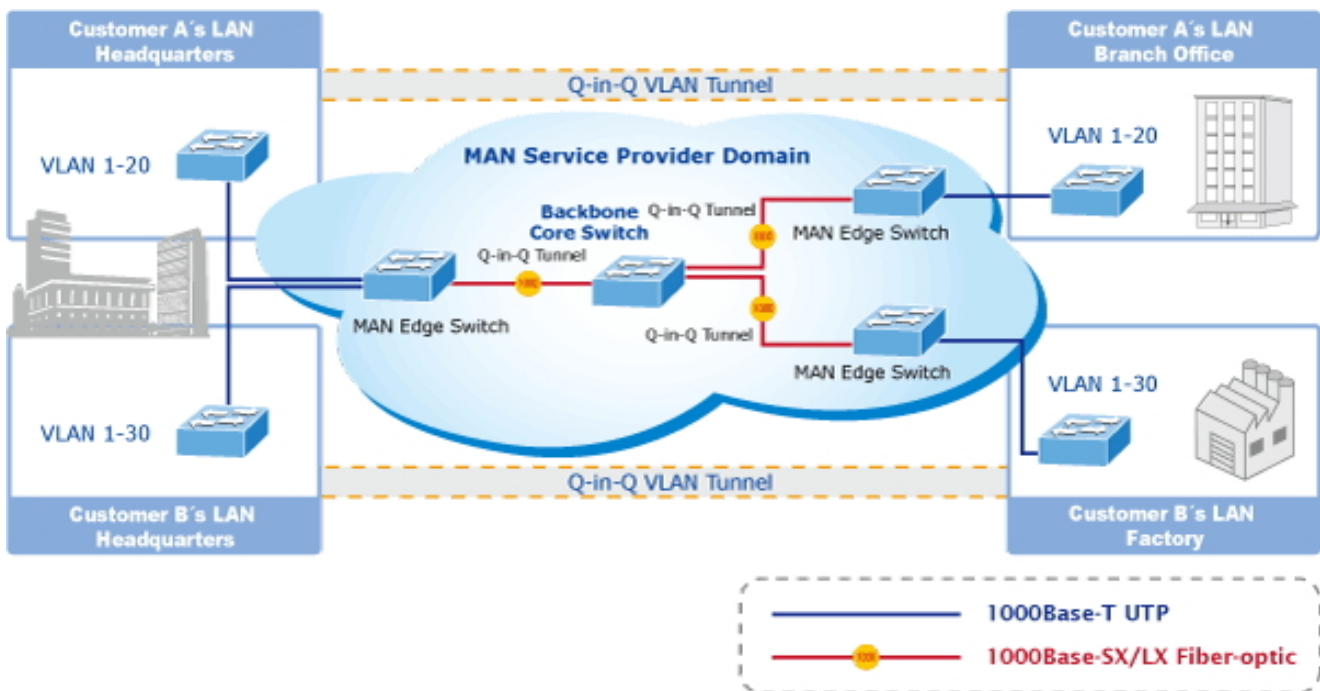
The PoE Managed Switch supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering

with the VLAN tags. All tags use EtherType **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

Edit Interface Setting

The Edit Interface Setting/Status screens in Figure 4-5-3 & Figure 4-5-4 appear.

Figure 4-5-3: Edit Interface Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number for this drop down list to set VLAN port setting.
• **Interface VLAN Mode**	Set the port in hybrid, access, trunk, tunnel mode. ■ **Hybrid** means the port allows the traffic of multi-VLANs to pass with tag or untag mode. ■ **Access** indicates the port belongs to one VLAN only. ■ **Trunk** means the port allows traffic of multiple VLAN. ■ **Tunnel** configures IEEE 802.1Q tunneling for a downlink port to another device within the customer network.
• **PVID**	Allow assign PVID for selected port. The PVID will be inserted into all untagged frames entering the ingress port. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped. The range for the PVID is **1-4094.**
• **Accepted Type**	Determines whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. Options: ■ **All** ■ **Tag Only** ■ **Untag Only** By default, the field is set to **All**.

• **Ingress Filtering**	• If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. • If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
• **Uplink**	Enable/disable uplink function in trunk port.
• **TPID**	Configure the type (TPID) of the protocol of switch trunk port.

Button

Apply : Click to apply changes.

Port VLAN Status						
Port	**Interface VLAN Mode**	**PVID**	**Accept Frame Type**	**Ingress Filtering**	**Uplink**	**TPID**
GE1	Trunk	1	ALL	Enabled	Disabled	0x8100
GE2	Trunk	1	ALL	Enabled	Disabled	0x8100
GE3	Trunk	1	ALL	Enabled	Disabled	0x8100
GE4	Trunk	1	ALL	Enabled	Disabled	0x8100
GE5	Trunk	1	ALL	Enabled	Disabled	0x8100
GE6	Trunk	1	ALL	Enabled	Disabled	0x8100
GE7	Trunk	1	ALL	Enabled	Disabled	0x8100
GE8	Trunk	1	ALL	Enabled	Disabled	0x8100
GE9	Trunk	1	ALL	Enabled	Disabled	0x8100
GE10	Trunk	1	ALL	Enabled	Disabled	0x8100
GE11	Trunk	1	ALL	Enabled	Disabled	0x8100
GE12	Trunk	1	ALL	Enabled	Disabled	0x8100
GE13	Trunk	1	ALL	Enabled	Disabled	0x8100
GE14	Trunk	1	ALL	Enabled	Disabled	0x8100
GE15	Trunk	1	ALL	Enabled	Disabled	0x8100
GE16	Trunk	1	ALL	Enabled	Disabled	0x8100
GE17	Trunk	1	ALL	Enabled	Disabled	0x8100
GE18	Trunk	1	ALL	Enabled	Disabled	0x8100
GE19	Trunk	1	ALL	Enabled	Disabled	0x8100
GE20	Trunk	1	ALL	Enabled	Disabled	0x8100
GE21	Trunk	1	ALL	Enabled	Disabled	0x8100
GE22	Trunk	1	ALL	Enabled	Disabled	0x8100
GE23	Trunk	1	ALL	Enabled	Disabled	0x8100
GE24	Trunk	1	ALL	Enabled	Disabled	0x8100
GE25	Trunk	1	ALL	Enabled	Disabled	0x8100
GE26	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG1	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG2	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG3	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG4	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG5	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG6	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG7	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG8	Trunk	1	ALL	Enabled	Disabled	0x8100

Figure 4-5-4: Edit Interface Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Interface VLAN Mode**	Display the current interface VLAN mode.
• **PVID**	Display the current PVID.
• **Accepted Frame Type**	Display the current access frame type.
• **Ingress Filtering**	Display the current ingress filtering.
• **Uplink**	Display the current uplink mode.
• **TPID**	Display the current TPID.

4.5.5 Port to VLAN

Use the VLAN Static Table to configure port members for the selected VLAN index. This Page allows for adding and deleting port members of each VLAN. The screen in Figure 4-5-5 appears.

Figure 4-5-5: Port to VLAN Setting Page Screenshot

106

The page includes the following fields:

Object	Description
• **VLAN ID**	Select VLAN ID for this drop down list to assign VLAN membership.
• **Port**	The switch port number of the logical port.
• **Interface VLAN Mode**	Display the current interface VLAN mode.
• **Membership**	Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
	Forbidden: Interface is forbidden from automatically joining the VLAN via GVRP.
	Excluded: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
	Tagged: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
	Untagged: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
• **PVID**	Display the current PVID

Button

Apply : Click to apply changes.

4.5.6 Port VLAN Membership

This Page provides an overview of membership status for VLAN users. The VLAN Membership Status screen in Figure 4-5-6 appears.

Figure 4-5-6: Port VLAN Membership Table Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Mode**	Display the current VLAN mode.
• **Administrative VLANs**	Display the current administrative VLANs.
• **Operational VLANs**	Display the current operational VLANs.
• **Modify**	Click **Edit** to modify VLAN membership.

4.5.7 Protocol VLAN Group Setting

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 PoE Managed Switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Command Usage

To configure protocol-based VLANs, follow these steps:

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

This Page allows for configures protocol-based VLAN Group Setting. The portocol-based VLAN screens in Figure 4-5-7 & Figure 4-5-8 appear.

Figure 4-5-7: Add Protocol VLAN Group Page Screenshot

The page includes the following fields:

Object	Description
• **Group ID**	Protocol Group ID assigned to the Special Protocol VLAN Group.
• **Frame Type**	Frame Type can have one of the following values: ■ **Ethernet II** ■ **IEEE802.3_LLC_Other** ■ **RFC_1042** Note: On changing the Frame type field, valid value of the following text field will

	vary depending on the new frame type you selected.
• **Protocol Value (0x0600-0xFFFE)**	Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu. Valid values for frame type ranges from 0x0600-0xfffe

Button

Apply : Click to apply changes.
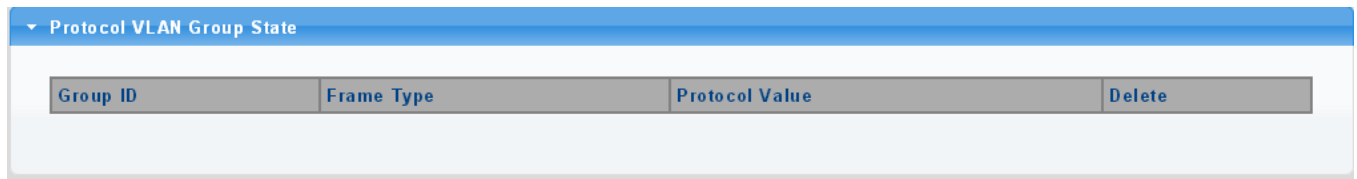
Figure 4-5-8: Protocol VLAN Group State Page Screenshot

The page includes the following fields:

Object	Description
• **Group ID**	Display the current group ID
• **Frame Type**	Display the current frame type
• **Protocol Value**	Display the current protocol value
• **Delete**	Click **Delete** to delete the group ID entry.

4.5.8 Protocol VLAN Port Setting

This Page allows you to map a already configured Group Name to a VLAN/port for the switch. The Protocol VLAN Port Setting/State screens in Figure 4-5-9 & Figure 4-5-10 appear.
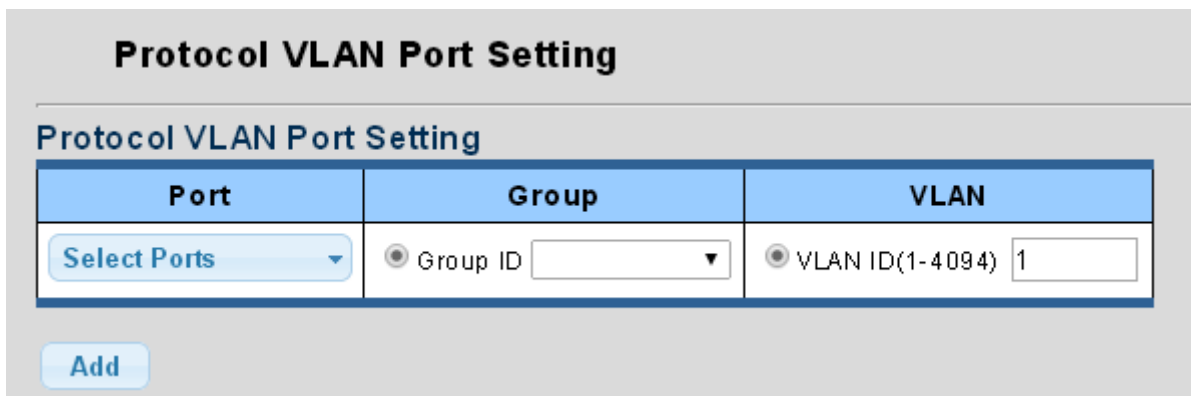
Figure 4-5-9: Protocol VLAN Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list to assign protocol VLAN port.
• **Group**	Select group ID for this drop down list to protocol VLAN group.
• **VLAN**	VLAN ID assigned to the Special Protocol VLAN Group.

Button

Add : Click to add protocol VLAN port entry.
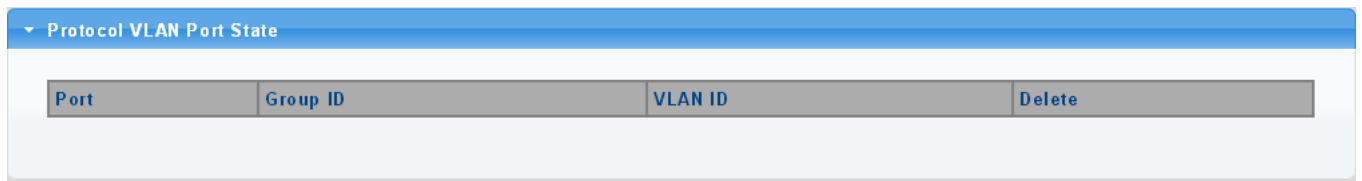
Figure 4-5-10: Protocol VLAN Port State Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Display the current port
• **Group ID**	Display the current group ID
• **VLAN ID**	Display the current VLAN ID

4.5.9 VLAN setting example:

- Separate VLANs

- 802.1Q VLAN Trunk

4.5.9.1 Two separate 802.1Q VLANs

The diagram shows how the PoE Managed Switch handle Tagged and Untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separated VLANs. Each VLAN isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. The screen in Figure 4-5-11 appears and Table 4-5-2 describes the port configuration of the PoE Managed Switches.
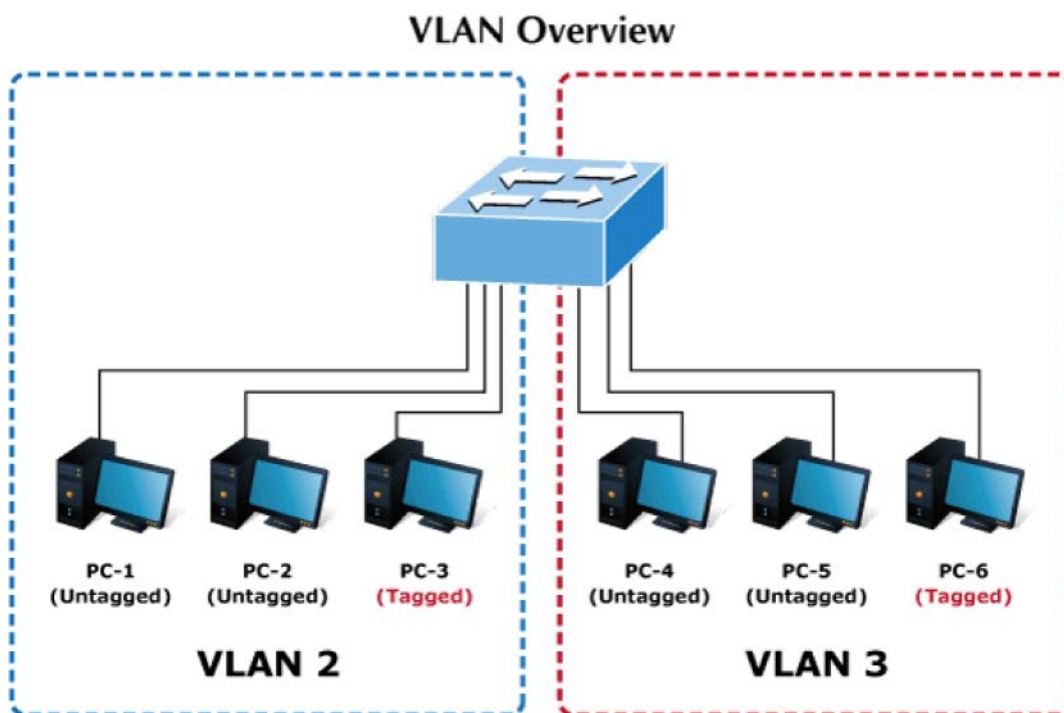
Figure 4-5-11: Two Separate VLAN Diagrams

VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 1	1	Port-7~Port-8	N/A
VLAN Group 2	2	Port-1,Port-2	Port-3
VLAN Group 3	3	Port-4,Port-5	Port-6

Table 4-5-2: VLAN and Port Configuration

The scenario described as follows:

■ **Untagged packet entering VLAN 2**

1. While **[PC-1]** transmit an **untagged** packet enters **Port-1**, the PoE Managed Switch will tag it with a **VLAN Tag=2**. **[PC-2]** and **[PC-3]** will received the packet through **Port-2** and **Port-3**.

2. [PC-4],[PC-5] and [PC-6] received no packet.

3. While the packet leaves **Port-2**, it will be stripped away it tag becoming an **untagged** packet.

4. While the packet leaves **Port-3**, it will keep as a **tagged** packet with **VLAN Tag=2**.

■ **Tagged packet entering VLAN 2**

1. While **[PC-3]** transmit a **tagged** packet with **VLAN Tag=2** enters **Port-3**, **[PC-1]** and **[PC-2]** will received the packet through **Port-1** and **Port-2**.

2. While the packet leaves **Port-1** and **Port-2**, it will be stripped away it tag becoming an **untagged** packet.

■ **Untagged packet entering VLAN 3**

1. While **[PC-4]** transmit an **untagged** packet enters **Port-4**, the PoE Managed Switch will tag it with a **VLAN Tag=3**. **[PC-5]** and **[PC-6]** will received the packet through **Port-5** and **Port-6**.

2. While the packet leaves **Port-5**, it will be stripped away it tag becoming an **untagged** packet.

3. While the packet leaves **Port-6**, it will keep as a **tagged** packet with **VLAN Tag=3**.

In this example, VLAN Group 1 is set as default VLAN, but only focuses on VLAN 2 and VLAN 3 traffic flow.

Setup steps

1. Create VLAN Group 2 and 3

Add VLAN group 2 and group 3

VLAN ID	VLAN Name	VLAN Type
1	default	Default
2	20002	Static
3	30003	Static

2. Assign VLAN mode and PVID for each port:

Port-1,Port-2 and Port-3 : VLAN Mode = Hybrid, PVID=*2*

Port-4,Port-5 and Port-6 : VLAN Mode = Hybrid, PVID=*3*

Port VLAN Status

Port	Interface VLAN Mode	PVID	Accept Frame Type
GE1	Hybrid	2	ALL
GE2	Hybrid	2	ALL
GE3	Hybrid	2	ALL
GE4	Hybrid	3	ALL
GE5	Hybrid	3	ALL
GE6	Hybrid	3	ALL

3. Assign Tagged/Untagged for each port:

VLAN ID = 2:

Port-1 & 2 = Untagged,

Port-3 = Tagged,

Port -4~6 = Excluded.

Port to VLAN Settings

VLAN ID : 2

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☑
GE2	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☑
GE3	Hybrid	○ Forbidden ○ Excluded ⦿ Tagged ○ Untagged	☑
GE4	Hybrid	○ Forbidden ⦿ Excluded ○ Tagged ○ Untagged	☐
GE5	Hybrid	○ Forbidden ⦿ Excluded ○ Tagged ○ Untagged	☐
GE6	Hybrid	○ Forbidden ⦿ Excluded ○ Tagged ○ Untagged	☐

VLAN ID = 3:

Port-4 & 5 = Untagged,

Port -6 = Tagged,

Port-1~3 = Excluded.

Port to VLAN Settings			
VLAN ID : 3			
Port	**Interface VLAN Mode**	**Membership**	**PVID**
GE1	Hybrid	○ Forbidden ⊙ Excluded ○ Tagged ○ Untagged	☐
GE2	Hybrid	○ Forbidden ⊙ Excluded ○ Tagged ○ Untagged	☐
GE3	Hybrid	○ Forbidden ⊙ Excluded ○ Tagged ○ Untagged	☐
GE4	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⊙ Untagged	☑
GE5	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⊙ Untagged	☑
GE6	Hybrid	○ Forbidden ○ Excluded ⊙ Tagged ○ Untagged	☑

4.5.9.2 VLAN Trunking between two 802.1Q aware switch

The most cases are used for "**Uplink**" to other switches. VLANs are separated at different switches, but they need to access with other switches within the same VLAN group. The screen in Figure 4-5-12 appears.
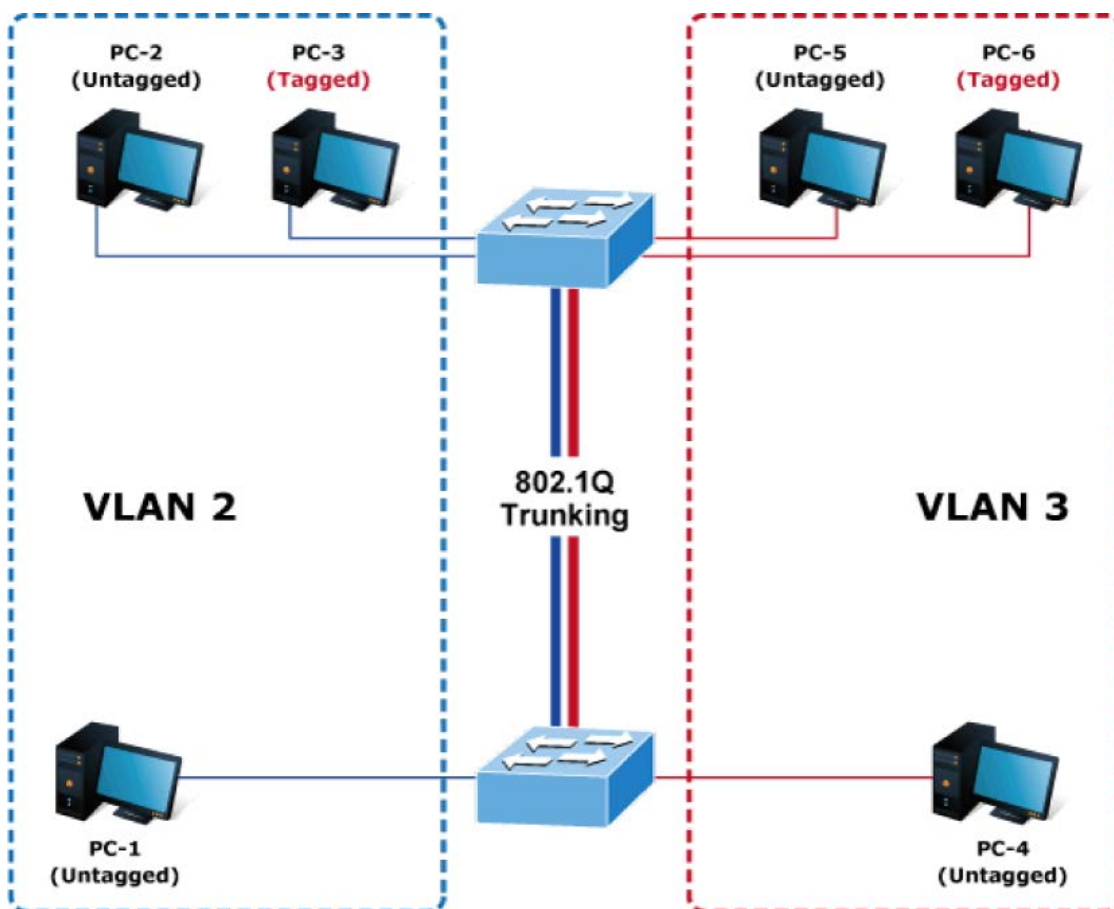
Setup steps

1.   Create VLAN Group 2 and 3

Add VLAN group 2 and group 3

VLAN ID	VLAN Name	VLAN Type
1	default	Default
2	20002	Static
3	30003	Static

2.   Assign VLAN mode and PVID for each port:

Port-1,Port-2 and Port-3 : VLAN Mode = Hybrid, PVID=*2*

Port-4,Port-5 and Port-6 : VLAN Mode = Hybrid, PVID=*3*

Port-7 : VLAN Mode = Hybrid, PVID=1

Port VLAN Status

Port	Interface VLAN Mode	PVID	Accept Frame Type
GE1	Hybrid	2	ALL
GE2	Hybrid	2	ALL
GE3	Hybrid	2	ALL
GE4	Hybrid	3	ALL
GE5	Hybrid	3	ALL
GE6	Hybrid	3	ALL
GE7	Hybrid	1	ALL

3.   Assign Tagged/Untagged for each port:

VLAN ID = 1:

Port-1~6 = Untagged,

Port -7 = Excluded.

Port to VLAN Settings

VLAN ID : 1

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☐
GE2	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☐
GE3	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☐
GE4	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☐
GE5	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☐
GE6	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☐
GE7	Hybrid	○ Forbidden ○ Excluded ⦿ Tagged ○ Untagged	☑

VLAN ID = 2:

Port-1 & 2 = Untagged,

Port-3 & 7 = Tagged,

Port -4~6 = Excluded.

Port to VLAN Settings

VLAN ID : 2

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☑
GE2	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☑
GE3	Hybrid	○ Forbidden ○ Excluded ⦿ Tagged ○ Untagged	☑
GE4	Hybrid	○ Forbidden ⦿ Excluded ○ Tagged ○ Untagged	☐
GE5	Hybrid	○ Forbidden ⦿ Excluded ○ Tagged ○ Untagged	☐
GE6	Hybrid	○ Forbidden ⦿ Excluded ○ Tagged ○ Untagged	☐
GE7	Hybrid	○ Forbidden ○ Excluded ⦿ Tagged ○ Untagged	☐

VLAN ID = 3:

Port-4 & 5 = Untagged,

Port -6 & 7= Tagged,

Port-1~3 = Excluded.

Port to VLAN Settings

VLAN ID : 3

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	○ Forbidden ⦿ Excluded ○ Tagged ○ Untagged	☐
GE2	Hybrid	○ Forbidden ⦿ Excluded ○ Tagged ○ Untagged	☐
GE3	Hybrid	○ Forbidden ⦿ Excluded ○ Tagged ○ Untagged	☐
GE4	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☑
GE5	Hybrid	○ Forbidden ○ Excluded ○ Tagged ⦿ Untagged	☑
GE6	Hybrid	○ Forbidden ○ Excluded ⦿ Tagged ○ Untagged	☑
GE7	Hybrid	○ Forbidden ○ Excluded ⦿ Tagged ○ Untagged	☐

4.6 Spanning Tree Protocol

4.6.1 Theory

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

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

The **IEEE 802.1D Spanning Tree** Protocol and **IEEE 802.1w Rapid Spanning Tree** Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port

■   The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission. The communication between switches via BPDUs results in the following:

■   One switch is elected as the root switch

■   The shortest distance to the root switch is calculated for each switch

■   A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.

■   A port for each switch is selected. This is the port providing the best path from the switch to the root switch.

■   Ports included in the STP are selected.

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

■   **Blocking** – the port is blocked from forwarding or receiving packets

■   **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state

■   **Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets

■   **Forwarding** – the port is forwarding packets

■   **Disabled** – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

■   From initialization (switch boot) to blocking

■   From blocking to listening or to disabled

■   From listening to learning or to disabled

■   From learning to forwarding or to disabled

■   From forwarding to disabled

■ From disabled to blocking
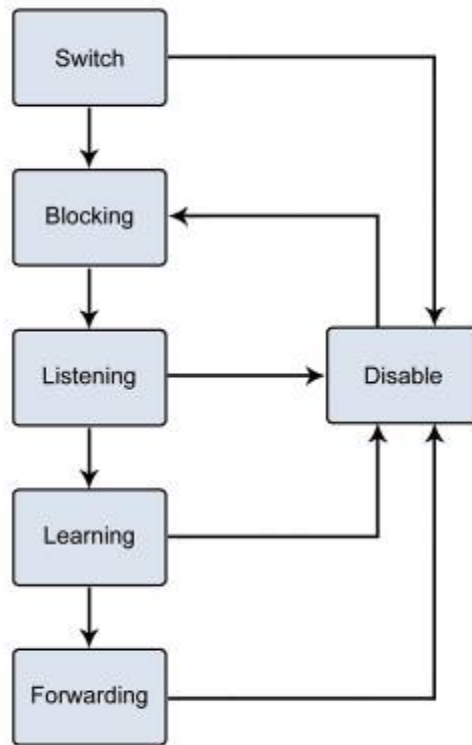
Figure 4-6-1: STP Port State Transitions

You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

2. STP Parameters

STP Operation Levels

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Note	On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges. On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier(Not user configurable	A combination of the User-set priority and the switch's MAC address.	32768 + MAC

except by setting priority below)	The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port –lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-Changeable STA Parameters

The Switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

Hello Time – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

> The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the

Switch spends in the listening state while moving from the blocking state to the forwarding state.

> Observe the following formulas when setting the above parameters:
>
> **Max. Age _ 2 x (Forward Delay - 1 second)**
>
> **Max. Age _ 2 x (Hello Time + 1 second)**

Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.

Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

3. Illustration of STP

A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.

If switch A broadcasts a packet to switch B, switch B will broadcast it to switch C, and switch C will broadcast it to back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings.

Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.
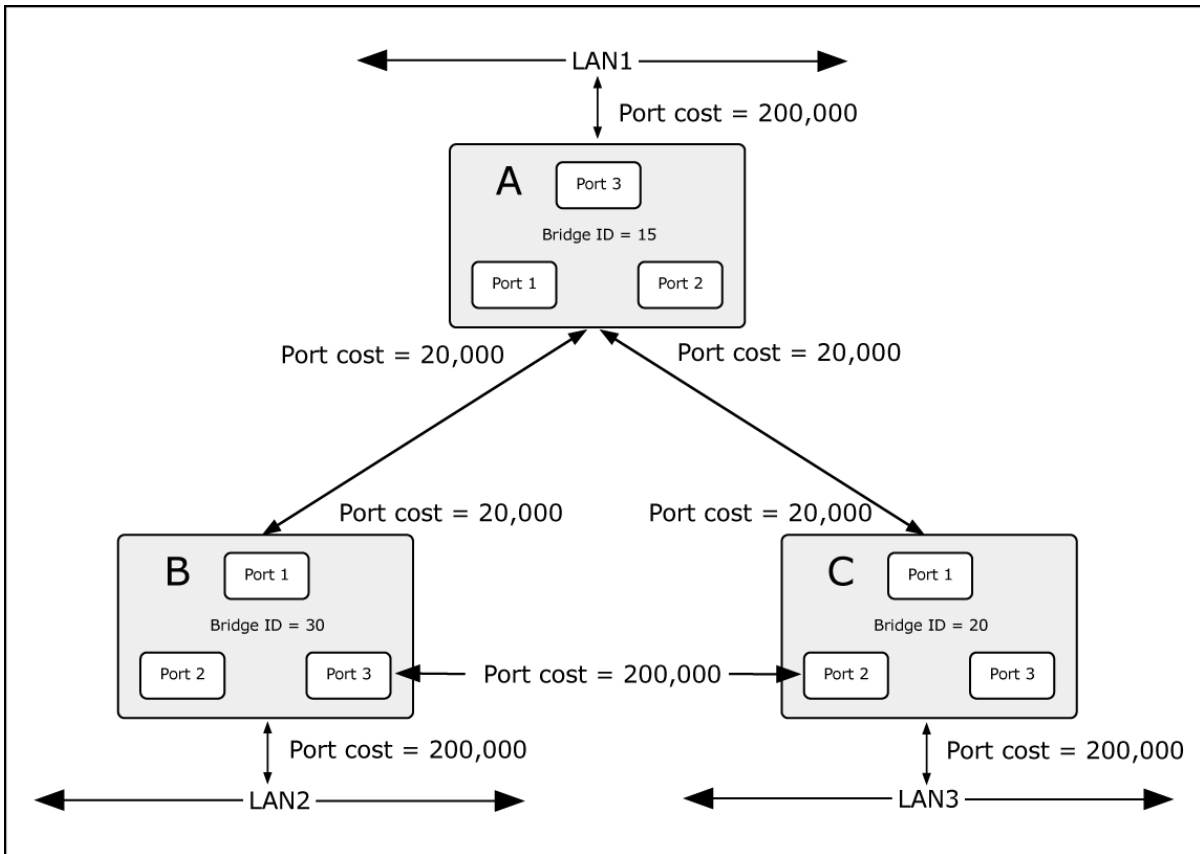
Figure 4-6-2: Before Applying the STA Rules

In this example, only the default STP values are used.
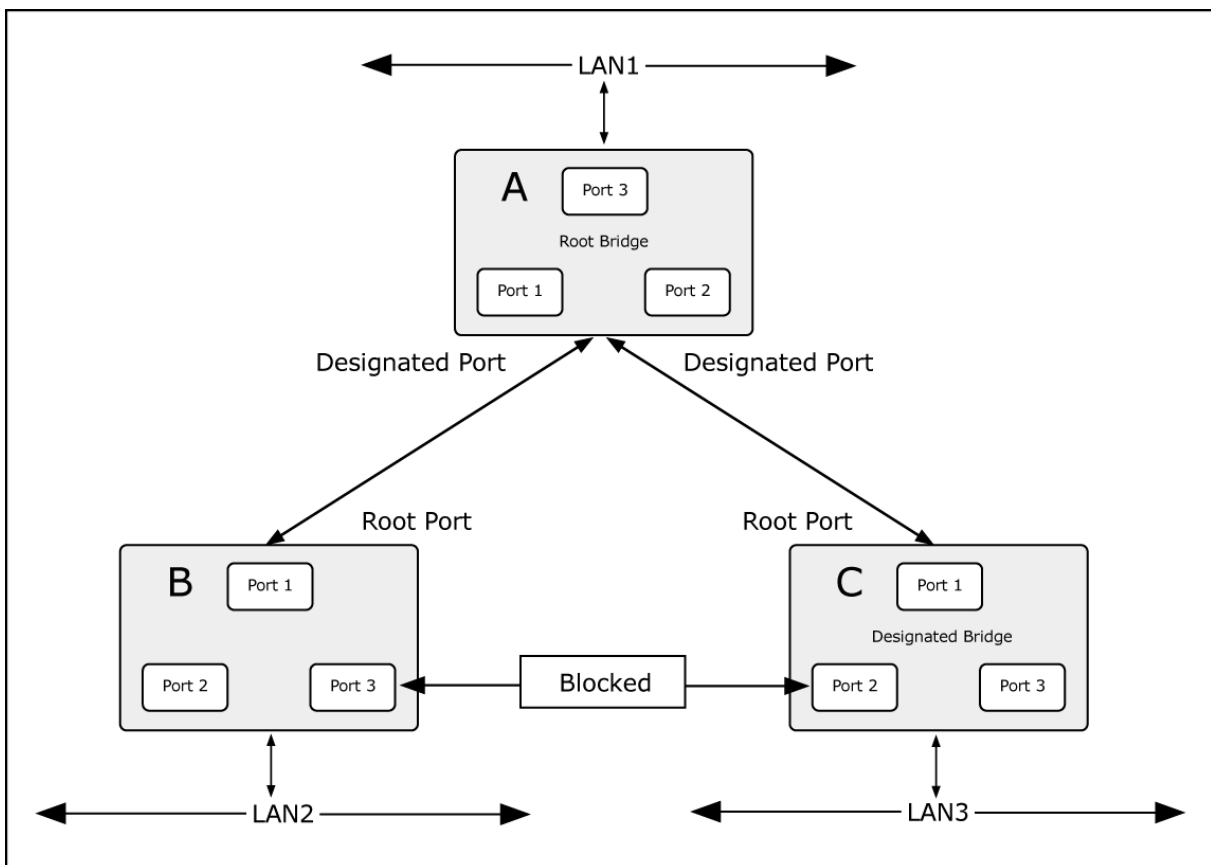
Figure 4-6-3: After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

This section has the following items:

■	**STP Global Setting**	Configures STP system settings
■	**STP Port Setting**	Configuration per port STP settings
■	**CIST Instance Setting**	Configure system configuration
■	**CIST Port Setting**	Configure CIST port setting
■	**MST Instance Setting**	Configuration each MST instance settings
■	**MST Port Setting**	Configuration per port MST setting
■	**STP Statistics**	Display the STP statistics

4.6.2 STP Global Settings

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch. The PoE Managed Switch support the following Spanning Tree protocols:

· **Compatiable -- Spanning Tree Protocol (STP):**Provides a single path between end stations, avoiding and eliminating loops.

· **Normal -- Rapid Spanning Tree Protocol (RSTP):** Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.

· **Extension – Multiple Spanning Tree Protocol (MSTP):** Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

The STP Global Settings screens in Figure 4-6-4 & Figure 4-6-5 appear.

Figure 4-6-4: Global Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Enable**	Enable or disable the STP function. The default value is "Disabled".
• **BPDU Forward**	Set the BPDU forward method.
• **PathCost Method**	The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
• **Force Version**	The STP protocol version setting. Valid values are **STP-Compatible**, **RSTP-Operation** and **MSTP-Operation**.
• **Configuration Name**	Identifier used to identify the configuration currently being used.
• **Configuration Revision**	Identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is **0**.

Button

Apply : Click to apply changes.

Figure 4-6-5: STP Information Page Screenshot

The page includes the following fields:

Object	Description
• **STP**	Display the current STP state.
• **BPDU Forward**	Display the current BPDU forward mode.
• **Cost Method**	Display the current cost method.
• **Force Version**	Display the current force version.
• **Configuration Name**	Display the current configuration name.
• **Configuration Revision**	Display the current configuration revision.

4.6.3 STP Port Setting

This page allows you to configure per port STP settings. The STP Port Setting screens in Figure 4-6-6 & Figure 4-6-7 appear.

Figure 4-6-6 : STP Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number for this drop down list.
• **External Cost (0 = Auto)**	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
• **Edge Port**	Controls whether the operEdge flag should start as beeing set or cleared. (The initial operEdge state when a port is initialized).
• **BPDU Filter**	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
• **BPDU Guard**	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
• **P2P MAC**	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media. (This applies to physical ports only. Aggregations are always *forced Point2Point*).
• **Migrate**	If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: **Disabled**)

Button

Apply : Click to apply changes.

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

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

Table 4-6-1: Recommended STP Path Cost Range

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

Table 4-6-2: Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

Table 4-6-3: Default STP Path Costs

▾ CIST Port Status

Port	Admin Enable	External Cost	Edge Port	BPDU Filter	BPDU Guard	P2P MAC
GE1	Enable	0	No	No	No	Yes
GE2	Enable	0	No	No	No	Yes
GE3	Enable	0	No	No	No	Yes
GE4	Enable	0	No	No	No	Yes
GE5	Enable	0	No	No	No	Yes
GE6	Enable	0	No	No	No	Yes
GE7	Enable	0	No	No	No	Yes
GE8	Enable	0	No	No	No	Yes
GE9	Enable	0	No	No	No	Yes
GE10	Enable	0	No	No	No	Yes
GE11	Enable	0	No	No	No	Yes
GE12	Enable	0	No	No	No	Yes
GE13	Enable	0	No	No	No	Yes
GE14	Enable	0	No	No	No	Yes
GE15	Enable	0	No	No	No	Yes
GE16	Enable	0	No	No	No	Yes
GE17	Enable	0	No	No	No	Yes
GE18	Enable	0	No	No	No	Yes
GE19	Enable	0	No	No	No	Yes
GE20	Enable	0	No	No	No	Yes
GE21	Enable	0	No	No	No	Yes
GE22	Enable	0	No	No	No	Yes
GE23	Enable	0	No	No	No	Yes
GE24	Enable	0	No	No	No	Yes
GE25	Enable	0	No	No	No	Yes
GE26	Enable	0	No	No	No	Yes
LAG1	Enable	0	No	No	No	Yes
LAG2	Enable	0	No	No	No	Yes
LAG3	Enable	0	No	No	No	Yes
LAG4	Enable	0	No	No	No	Yes
LAG5	Enable	0	No	No	No	Yes
LAG6	Enable	0	No	No	No	Yes
LAG7	Enable	0	No	No	No	Yes
LAG8	Enable	0	No	No	No	Yes

Figure 4-6-7: STP Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **Admin Enable**	Display the current STP port mode status
• **External Cost**	Display the current external cost.
• **Edge Port**	Display the current edge port status.
• **BPDU Filter**	Display the current BPDU filter configuration.
• **BPDU Guard**	Display the current BPDU guard configuration.
• **P2P MAC**	Display the current P2P MAC status.

4.6.4 CIST Instance Setting

This Page allows you to configure CIST instance settings. The CIST Instance Setting and Information screens in Figure 4-6-8 & Figure 4-6-9 & Figure 4-6-10 appear.

Figure 4-6-8: CIST Instance Setting Page Screenshot

The Page includes the following fields:

Object	Description
• **Priority**	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
• **Max Hops**	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 1 to 40 hops.
• **Forward Delay**	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds -Default: 15 -Minimum: The higher of 4 or [(Max. Message Age / 2) + 1] -Maximum: 30
• **Max Age**	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds.

	-Default: 20
	-Minimum: The higher of 6 or [2 x (Hello Time + 1)].
	-Maximum: The lower of 40 or [2 x (Forward Delay -1)]
• **Tx Hold Count**	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
• **Hello Time**	The time that controls the switch to send out the BPDU packet to check STP current status. Enter a value between 1 through 10.

Button

Apply : Click to apply changes.

▼ CIST Instance Information	
Information Name	**Information Value**
Priority	32768
Max Hops	20
Forward Delay	15
Max Age	20
Tx Hold Count	6
Hello Time	2

Figure 4-6-9: CIST Instance Information Page Screenshot

The page includes the following fields:

Object	Description
• **Priority**	Display the current CIST priority.
• **Max Hop**	Display the current Max. hops.
• **Forward Delay**	Display the current forward delay.
• **Max Age**	Display the current Max. age.
• **Tx Hold Count**	Display the current Tx hold count.
• **Hello Time**	Display the current hello time.

Figure 4-6-10: CIST Instance Information Page Screenshot

The page includes the following fields:

Object	Description
• **Bridge Identifier**	Display the bridge identifier information.
• **Designated Root Bridge**	Display the designed root bridge information.
• **External Root Path Cost**	Display the external root path cost informaiton.
• **Regional Root Bridge**	Display the regional root bridge information.
• **Internal Root Path Cost**	Display the internal root path cost information.
• **Designated Bridge**	Display the designated bridge information.
• **Root Port**	Display the root port information.
• **Remainging Hops**	Display the remaining hops information.
• **Last Topology Change**	Disaply the last topology change information.

4.6.5 CIST Port Setting

This page allows you to configure per port CIST priority and cost. The CIST Port Setting and Status screens in Figure 4-6-11 & Figure 4-6-12 appear.
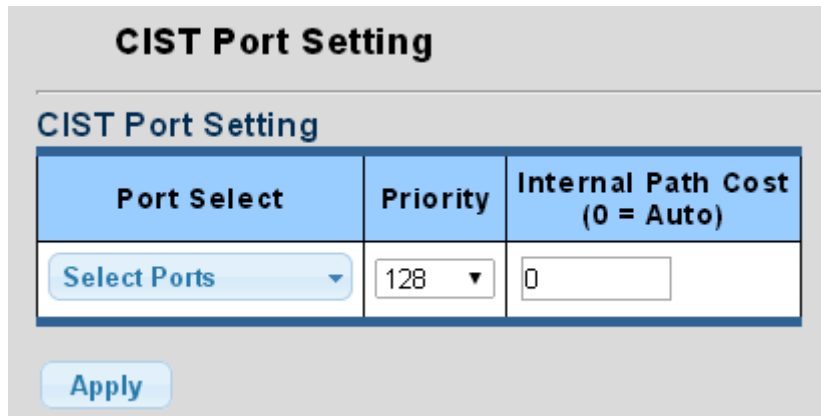
Figure 4-6-11: CIST Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number for this drop down list.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Default: **128** Range: 0-240, in steps of 16
• **Internal Path Cost (0 = Auto)**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Button

Apply : Click to apply changes.

▾ CIST Port Status

Port	Indentifier (Priority / Port ID)	External Path Cost Conf./Oper	Internal Path Cost Conf./Oper	Designated Root Bridge	External Root Cost	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Port Path Cost	Edge Port Conf./Oper	P2P MAC Conf./Oper	Port Role	Port State
GE1	128 / 1	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE2	128 / 2	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE3	128 / 3	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE4	128 / 4	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE5	128 / 5	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE6	128 / 6	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE7	128 / 7	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE8	128 / 8	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE9	128 / 9	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE10	128 / 10	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE11	128 / 11	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE12	128 / 12	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE13	128 / 13	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE14	128 / 14	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE15	128 / 15	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE16	128 / 16	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE17	128 / 17	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE18	128 / 18	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE19	128 / 19	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE20	128 / 20	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE21	128 / 21	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE22	128 / 22	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE23	128 / 23	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE24	128 / 24	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / Yes	Disabed	Forwarding
GE25	128 / 25	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
GE26	128 / 26	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
LAG1	128 / 27	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
LAG2	128 / 28	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
LAG3	128 / 29	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
LAG4	128 / 30	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
LAG5	128 / 31	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
LAG6	128 / 32	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
LAG7	128 / 33	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled
LAG8	128 / 34	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabed	Disabled

Figure 4-6-12: CIST Port Status Page Screenshot

133

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **Indentifier (Priority / Port ID)**	Display the current indentifier (Priority / Port ID).
• **External Path Cost Conf/Oper**	Display the current external path cost conf/oper.
• **Internal Path Cost Conf/Oper**	Display the current internal path cost/oper.
• **Designated Root Bridge**	Display the current designated root bridge.
• **External Root Cost**	Display the current external root cost
• **Regional Root Bridge**	Display the current regional root bridge
• **Internal Root Cost**	Display the current internal root cost
• **Designated Bridge**	Display the current designated bridge
• **Internal Port Path Cost**	Display the current internal port path cost
• **Edge Port Conf/Oper**	Display the current edge port conf/oper
• **P2P MAC Conf/Oper**	Display the current P2P MAC conf/oper
• **Port Role**	Display the current prot role
• **Port State**	Display the current port state

4.6.6 MST Instance Configuration

This page allows the user to configure MST Instance Configuration. The MST Instance Setting, Information and Status screens in Figure 4-6-13, Figure 4-6-14 & Figure 4-6-15 appear.
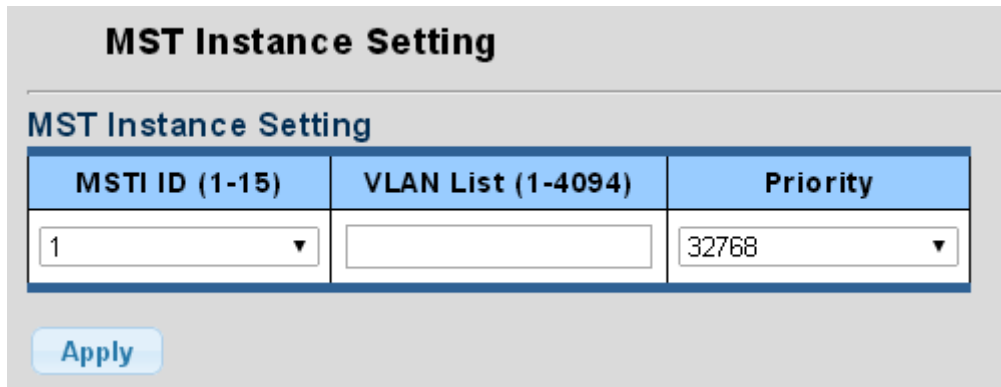
Figure 4-6-13: MST Instance Setting Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI ID**	Allow assign MSTI ID. The range for the MSTI ID is 1-15.
• **VLAN List (1-4094)**	Allow assign VLAN list for special MSTI ID. The range for the VLAN list is 1-4094.
• **Priority**	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Button

Apply : Click to apply changes.
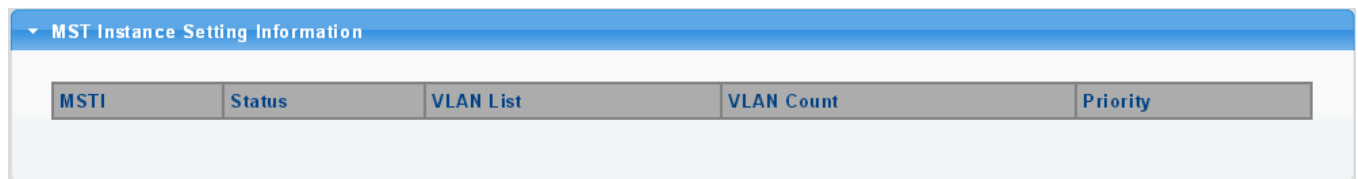
Figure 4-6-14: MSTI Instance Setting Information Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI**	Display the current MSTI entry.
• **Status**	Display the current MSTI status
• **VLAN List**	Display the current VLAN list.
• **VLAN Count**	Display the current VLAN count.
• **Priority**	Display the current MSTI priority

Figure 4-6-15: MST Instance Status Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI ID**	Display the MSTI ID.
• **Regional Root Bridge**	Display the current designated root bridge.
• **Internal Root Cost**	Display the current internal root cost.
• **Designated Bridge**	Display the current designated bridge.
• **Root Port**	Display the current root port.
• **Max Age**	Display the current max. age.
• **Forward Delay**	Display the current forward delay.
• **Remaining Hops**	Display the current remaininging hops.
• **Last Topology Change**	Display the current last topology change.

4.6.7 MST Port Setting

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

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

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are global. The MSTI Ports Setting screens in Figure 4-6-16 & Figure 4-6-17 appear.

Figure 4-6-16: MST Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **MST ID**	Enter the special MST ID to configure path cost & priority.
• **Port Select**	Select port number for this drop down list.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost.
• **Internal Path Cost (0 = Auto)**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Button

Apply : Click to apply changes.

▾ MST Port Status

MSTI ID	Port	Indentifier (Priority / Port ID)	Internal Path Cost Conf/Oper	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Path Cost	Port Role	Port State
1	GE1	128/1	0/--	--/--	--	--/--	--	--	--
1	GE2	128/2	0/--	--/--	--	--/--	--	--	--
1	GE3	128/3	0/--	--/--	--	--/--	--	--	--
1	GE4	128/4	0/--	--/--	--	--/--	--	--	--
1	GE5	128/5	0/--	--/--	--	--/--	--	--	--
1	GE6	128/6	0/--	--/--	--	--/--	--	--	--
1	GE7	128/7	0/--	--/--	--	--/--	--	--	--
1	GE8	128/8	0/--	--/--	--	--/--	--	--	--
1	GE9	128/9	0/--	--/--	--	--/--	--	--	--
1	GE10	128/10	0/--	--/--	--	--/--	--	--	--
1	GE11	128/11	0/--	--/--	--	--/--	--	--	--
1	GE12	128/12	0/--	--/--	--	--/--	--	--	--
1	GE13	128/13	0/--	--/--	--	--/--	--	--	--
1	GE14	128/14	0/--	--/--	--	--/--	--	--	--
1	GE15	128/15	0/--	--/--	--	--/--	--	--	--
1	GE16	128/16	0/--	--/--	--	--/--	--	--	--
1	GE17	128/17	0/--	--/--	--	--/--	--	--	--
1	GE18	128/18	0/--	--/--	--	--/--	--	--	--
1	GE19	128/19	0/--	--/--	--	--/--	--	--	--
1	GE20	128/20	0/--	--/--	--	--/--	--	--	--
1	GE21	128/21	0/--	--/--	--	--/--	--	--	--
1	GE22	128/22	0/--	--/--	--	--/--	--	--	--
1	GE23	128/23	0/--	--/--	--	--/--	--	--	--
1	GE24	128/24	0/--	--/--	--	--/--	--	--	--
1	GE25	128/25	0/--	--/--	--	--/--	--	--	--
1	GE26	128/26	0/--	--/--	--	--/--	--	--	--
1	LAG1	128/27	0/--	--/--	--	--/--	--	--	--
1	LAG2	128/28	0/--	--/--	--	--/--	--	--	--
1	LAG3	128/29	0/--	--/--	--	--/--	--	--	--
1	LAG4	128/30	0/--	--/--	--	--/--	--	--	--
1	LAG5	128/31	0/--	--/--	--	--/--	--	--	--
1	LAG6	128/32	0/--	--/--	--	--/--	--	--	--
1	LAG7	128/33	0/--	--/--	--	--/--	--	--	--
1	LAG8	128/34	0/--	--/--	--	--/--	--	--	--

Figure 4-6-17: MST Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI ID**	Display the current MSTI ID.
• **Port**	The switch port number of the logical STP port.
• **Indentifier (Priority / Port ID)**	Display the current indentifier (priority / port ID)
• **Internal Path Cost Conf/Oper**	Display the current internal path cost configuration / operation
• **Regional Root Bridge**	Display the current regional root bridget.
• **Internal Root Cost**	Display the current internal root cost.

• **Designated Bridge**	Display the current designated bridge.
• **Internal Path Cost**	Display the current internal path cost.
• **Port Role**	Display the current port role.
• **Port State**	Display the current port state.

• **Designated Bridge**	Display the current designated bridge.
• **Internal Path Cost**	Display the current internal path cost.

4.6.8 STP Statistics

This page displays STP statistics. The STP statistics screen in Figure 4-6-18 appears.

STP Statistics

▾ STP Statistics

Port	Configuration BDPUs Received	TCN BDPUs Received	MSTP BDPUs Received	Configuration BDPUs Transmitted	TCN BDPUs Transmitted	MSTP BDPUs Transmitted
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0
GE4	0	0	0	0	0	0
GE5	0	0	0	0	0	0
GE6	0	0	0	0	0	0
GE7	0	0	0	0	0	0
GE8	0	0	0	0	0	0
GE9	0	0	0	0	0	0
GE10	0	0	0	0	0	0
GE11	0	0	0	0	0	0
GE12	0	0	0	0	0	0
GE13	0	0	0	0	0	0
GE14	0	0	0	0	0	0
GE15	0	0	0	0	0	0
GE16	0	0	0	0	0	0
GE17	0	0	0	0	0	0
GE18	0	0	0	0	0	0
GE19	0	0	0	0	0	0
GE20	0	0	0	0	0	0
GE21	0	0	0	0	0	0
GE22	0	0	0	0	0	0
GE23	0	0	0	0	0	0
GE24	0	0	0	0	0	0
GE25	0	0	0	0	0	0
GE26	0	0	0	0	0	0
LAG1	0	0	0	0	0	0
LAG2	0	0	0	0	0	0
LAG3	0	0	0	0	0	0
LAG4	0	0	0	0	0	0
LAG5	0	0	0	0	0	0
LAG6	0	0	0	0	0	0
LAG7	0	0	0	0	0	0
LAG8	0	0	0	0	0	0

Figure 4-6-18: STP Statistics Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **Configuration BPDUs Received**	Display the current configuration BPDUs received.
• **TCN BPDUs Received**	Display the current TCN BPDUs received
• **MSTP BPDUs Received**	Display the current MSTP BPDUs received

• **Configuration BPDUs Transmitted**	Display the configuration BPDUs transmitted
• **TCN BPDUs Transmitted**	Display the current TCN BPDUs transmitted
• **MSTP BPDUs Transmitted**	Display the current BPDUs transmitted

• **Configuration BPDUs**

   Transmitted

• **TCN BPDUs**

4.7 Multicast

This section has the following items:

- **Properties**   Configures multicast properties.
- **IGMP Snooping**   Configures IGMP snooping settings.
- **IGMP Snooping Statistics** Display the IGMP snooping statistics.
- **Multicast Throttling Setting**   Configures multicast throttling setting
- **Multicast Filter**   Configures multicast filter

4.7.1 Properties

This page provides multicast properties related configuration.

The multicast Properties and Information screen in Figure 4-7-1 & Figure 4-7-2 appear.

Figure 4-7-1: Properties Setting Page Screenshot

The page includes the following fields:

Object	Description
• **L2 Unknow Multicast Action**	Action for L2 unknown multicast traffic: Options are: **Drop** or **flood.**
• **IP Unknown Multicast Action**	Action for IP unknown multicast traffic: **Drop**, **flood** or send to **router port**.
• **IPv4 Forward Method**	Configure the IPv4 multicast fordward method. Options are: **MAC** or **Src-Dst-Ip.**

Button

Apply : Click to apply changes.

Figure 4-7-2: Properties Information Page Screenshot

The page includes the following fields:

Object	Description
• **L2 Unknow Multicast Action**	Display the current L2 unknown multicast action status.
• **IP Uknown Multicast Action**	Display the current IP unknown multicast action status.
• **Forward Method For IPv4**	Display the current IPv4 multicast forward method.

4.7.2 IGMP Snooping

The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.
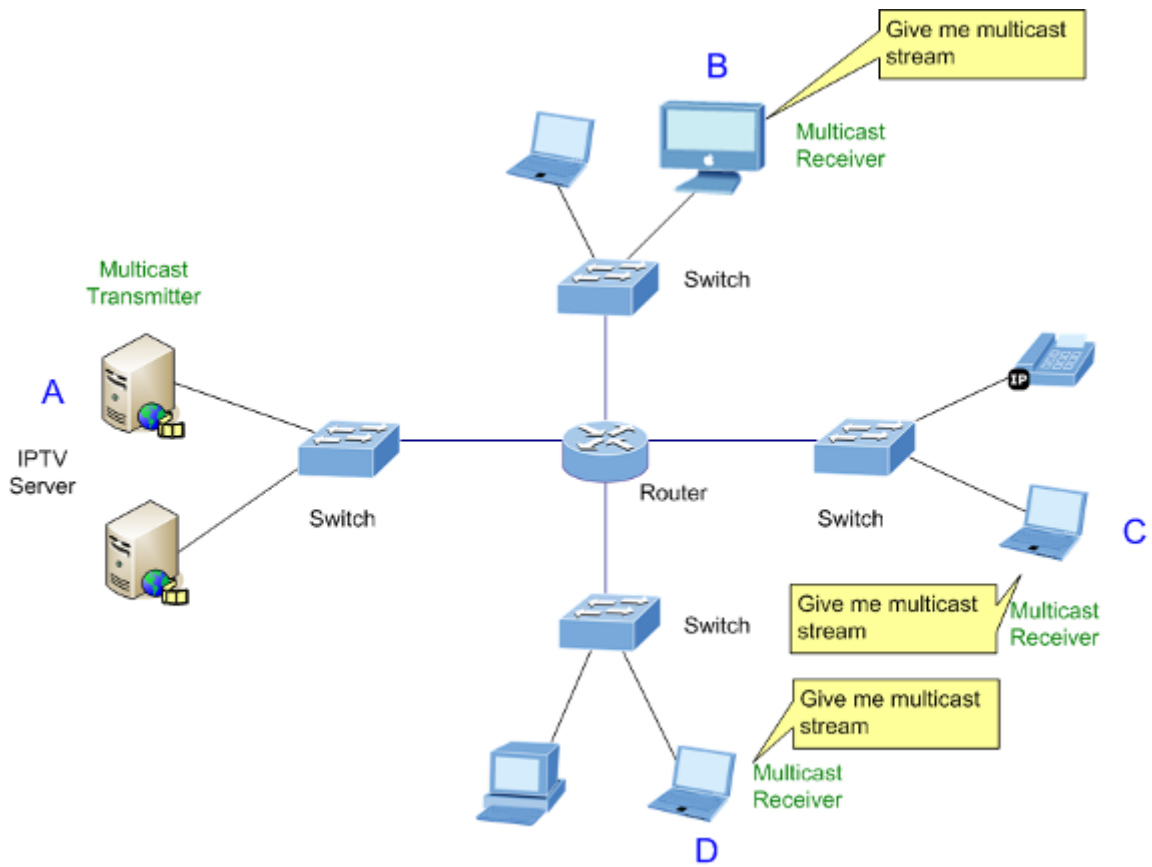
Figure 4-7-3: Multicast Service
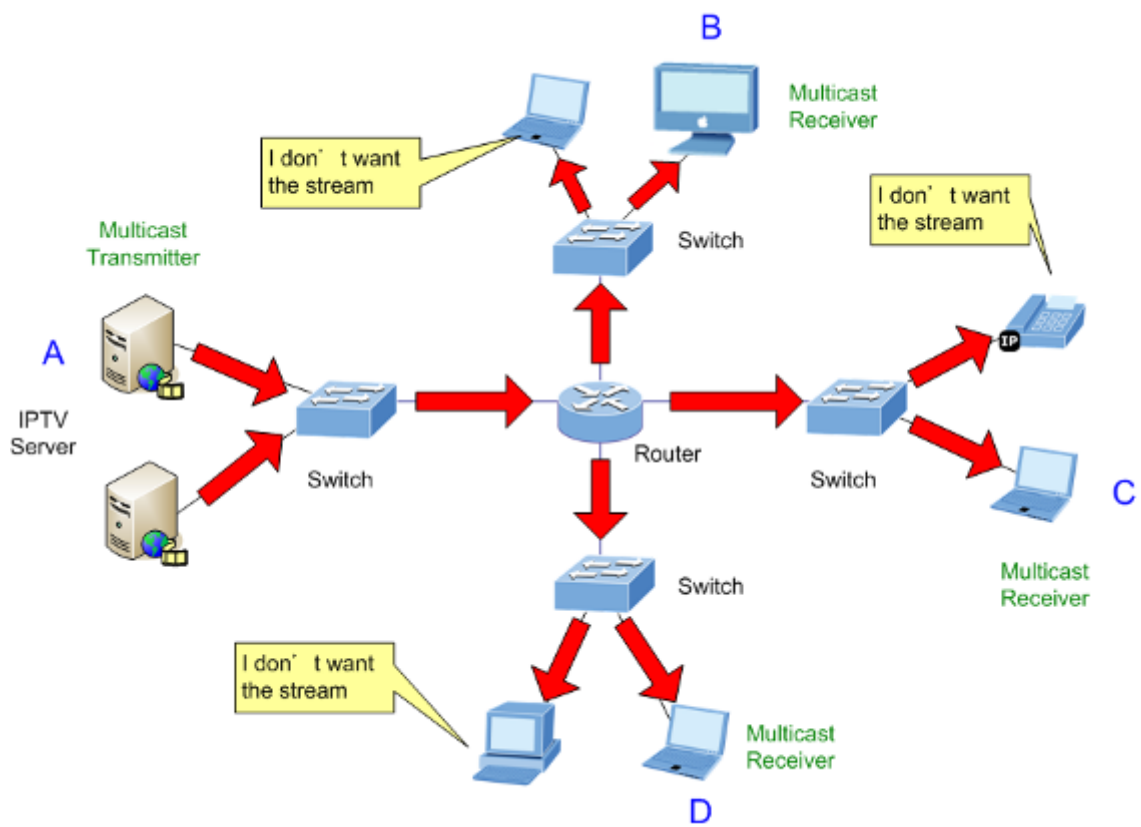
Figure 4-7-4: Multicast Flooding
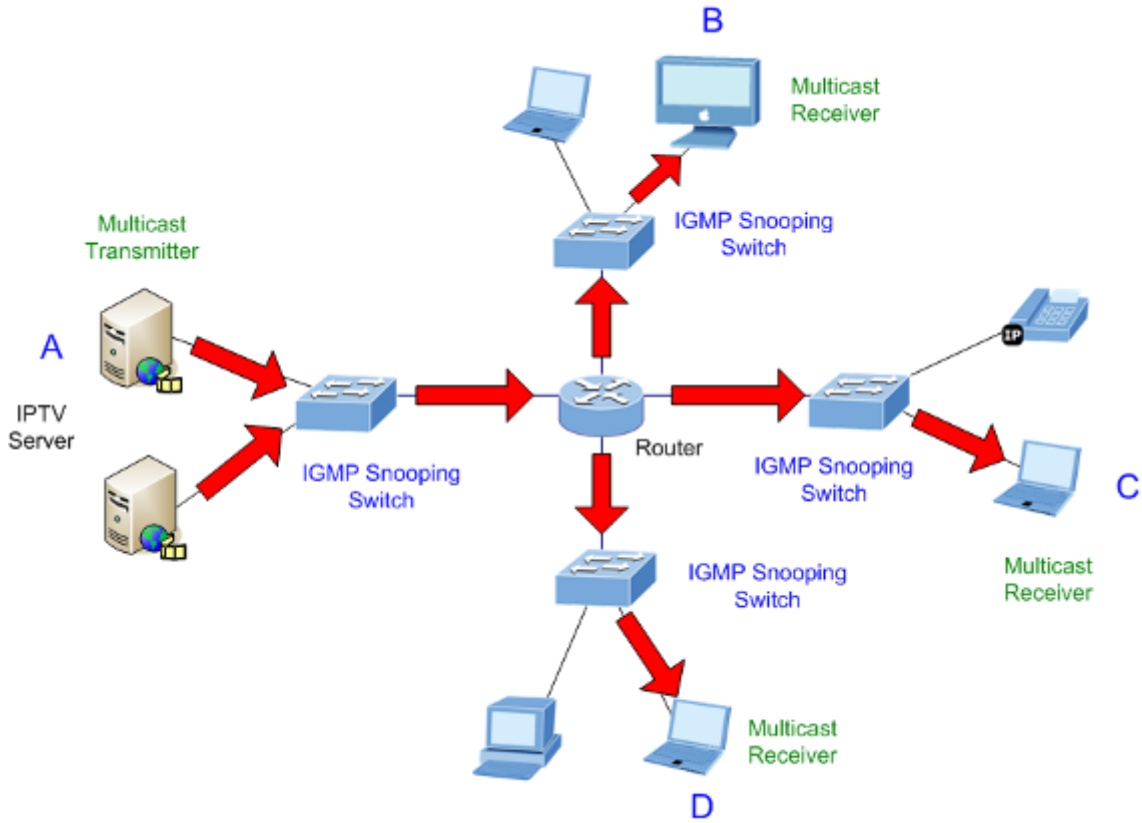
Figure 4-7-5: IGMP Snooping Multicast Stream Control

IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0	8	16	31

Type	Response Time	Checksum

Group Address (all zeros if this is a query)
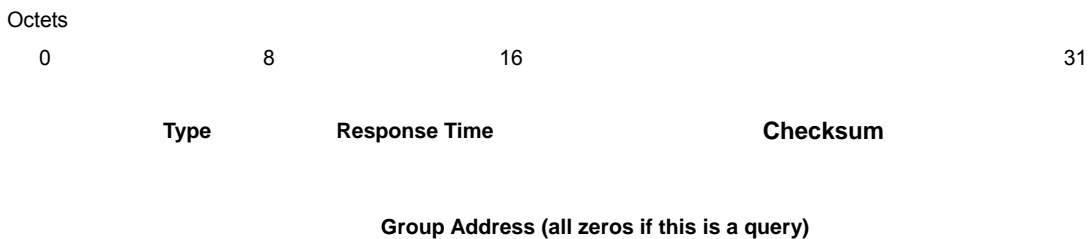
The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)

145

0x11	Specific Group Membership Query (if Group Address is Present)
0x16	**Membership Report (version 2)**
0x17	**Leave a Group (version 2)**
0x12	**Membership Report (version 1)**

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.
A host sends an IGMP **"report"** to join a group

A host will never send a report when it wants to leave a group (for version 1).

A host will send a **"leave"** report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:
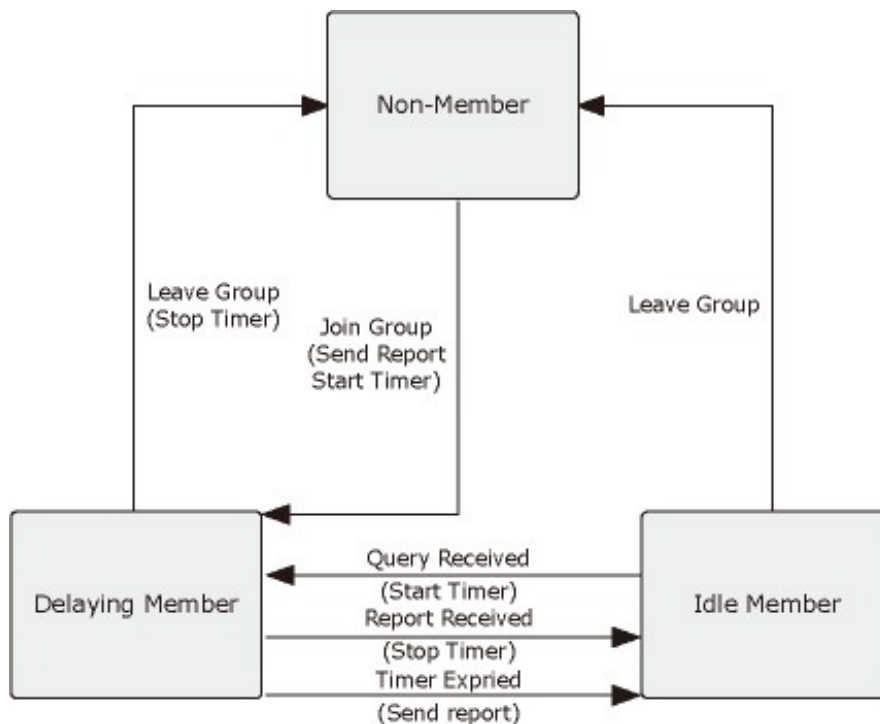
Figure 4-7-6: IGMP State Transitions

■ **IGMP Querier –**

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "**querier**" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note	Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

4.7.2.1 IGMP Setting

This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header. The IGMP Snooping Setting and Information screens in Figure 4-7-7, Figure 4-7-8 & Figure 4-7-9 appear.
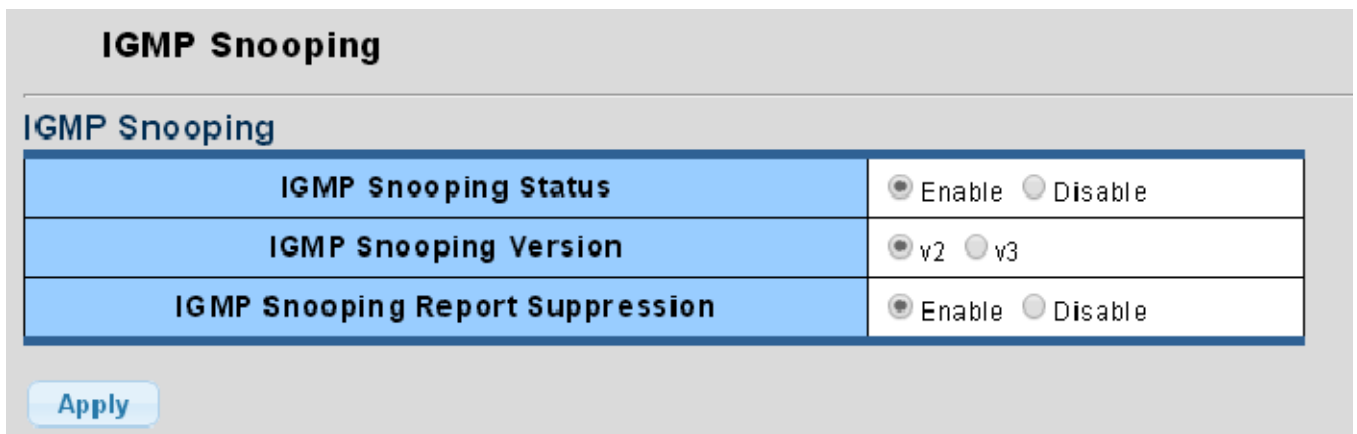
Figure 4-7-7: IGMP Snooping Page Screenshot

The page includes the following fields:

Object	Description
• **IGMP Snooping Status**	Enable or disable the IGMP snooping. The default value is "Disabled".
• **IGMP Snooping Version**	Sets the IGMP Snooping operation version. Possible versions are: ■ **v2**: Set IGMP Snooping supported IGMP version 2. ■ **v3**: Set IGMP Snooping supported IGMP version 3.
• **IGMP Snooping Report Suppression**	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers. The default is enabled.

Button

Apply : Click to apply changes.

IGMP Snooping Information

Information Name	Information Value
IGMP Snooping Status	Enable
IGMP Snooping Version	v2
IGMP Snooping V2 Report Suppression	Enable

Figure 4-7-8: IGMP Snooping Information Page Screenshot

The page includes the following fields:

Object	Description
• **IGMP Snooping Status**	Dipaly the current IGMP snooping status.
• **IGMP Snooping Version**	Display the current IGMP snooping version.
• **IGMP Snooping V2 Report Suppression**	Display the current IGMP snooping v2 report suppression.

IGMP Snooping Table

Entry No.	VLAN ID	IGMP Snooping Operation Status	Router Ports Auto Learn	Query Robustness	Query Interval(sec.)	Query Max Response Interval(sec.)	Last Member Query count	Last Member Query Interval(sec)	Immediate Leave	Modify
1	1	Disabled	Enabled	2	125	10	2	1	Disabled	Edit

Figure 4-7-9: IGMP Snooping Information Page Screenshot

The page includes the following fields:

Object	Description
• **Entry No.**	Display the current entry number.
• **VLAN ID**	Display the current VLAN ID.
• **IGMP Snooping Operation Status**	Display the current IGMP snooping operation status.
• **Router Ports Auto Learn**	Display the current router ports auto learning.
• **Query Robustness**	Display the current query robustness.
• **Query Interval (sec.)**	Display the current query interval.
• **Query Max Response Interval (sec.)**	Display the current query max response interval.
• **Last Member Query conut**	Display the current last member query count.
• **Last Member Query Interval (sec)**	Display the current last member query interval.
• **Immediate Leave**	Display the current immediate leave.
• **Modify**	Click **Edit** to edit parameter.

4.7.2.2 IGMP Querier Setting

This page provides IGMP Querier Setting. The IGMP Querier Setting screens in Figure 4-7-10 & Figure 4-7-11 appear.
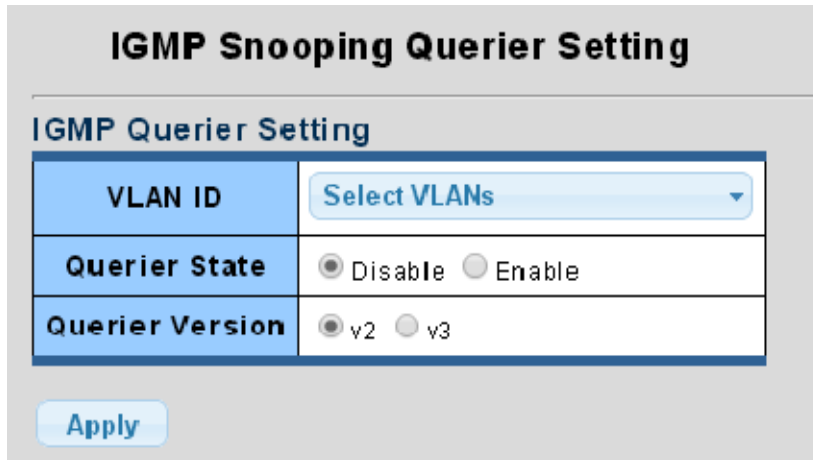
Figure 4-7-10: IGMP VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Select VLAN ID for this drop down list.
• **Querier State**	Enable or disable the querier state. The default value is "Disabled".
• **Querier Version**	Sets the querier version for compatibility with other devices on the network. Version: 2 or 3; Default: **v2**

Button

Apply : Click to apply changes.
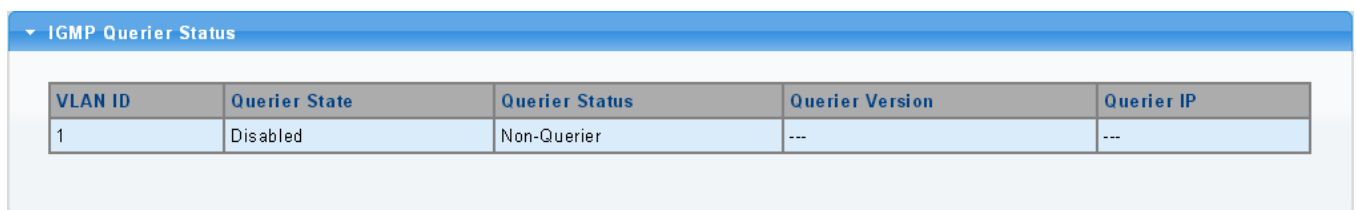
Figure 4-7-11: IGMP Querier Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID.
• **Querier State**	Display the current querier state.
• **Querier Status**	Display the current querier stauts.
• **Querier Version**	Display the current querier version.
• **Querier IP**	Display the current querier IP.

4.7.2.3 IGMP Static Group

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in above sections. For certain applications that require tighter control, you may need to statically configure a multicast service on the PoE Managed Switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

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

The IGMP Static Group configuration screens in Figure 4-7-12 & Figure 4-7-13 appear.

Figure 4-7-12: Add IGMP Static Group Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Select VLAN ID for this drop down list.
• **Group IP Address**	The IP address for a specific multicast service.
• **Member Ports**	Select port number for this drop down list.

Button

Add : Click to add IGMP router port entry.
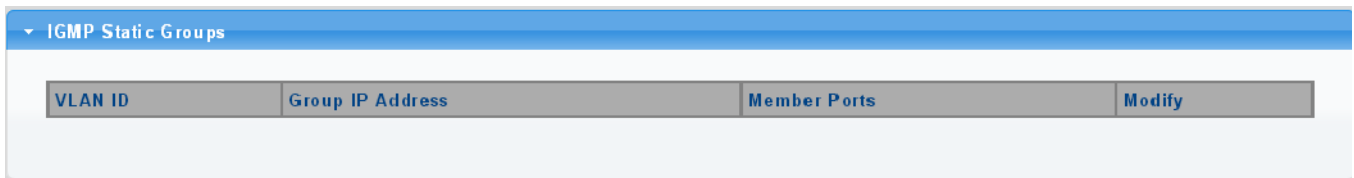
Figure 4-7-13: IGMP Static Groups Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID
• **Group IP Address**	Display the current group IP address
• **Member Ports**	Display the current member ports
• **Modify**	Click [Edit] to edit parameter.

4.7.2.4 IGMP Group Table

This page provides Multicast Database. The IGMP Group Table screen in Figure 4-7-14 appears.
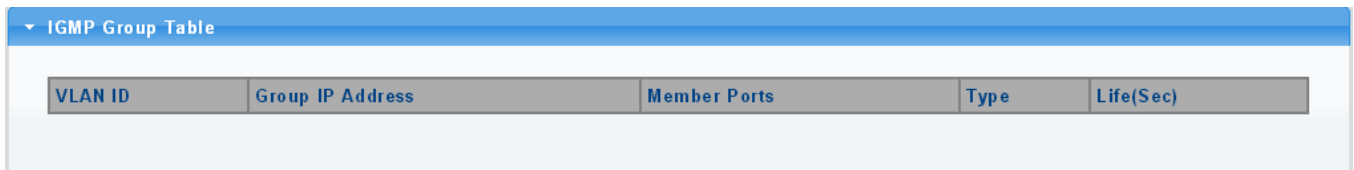
Figure 4-7-14: IGMP Group Table Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VID.
• **Group IP Address**	Display multicast IP address for a specific multicast service.
• **Member Ports**	Display the current member port.
• **Type**	Member types displayed include Static or Dynamic, depending on selected options.
• **Life(Sec)**	Display the current life.

4.7.2.5 IGMP Router Setting

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your PoE Managed Switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the PoE Managed Switch. The IGMP Router Setting and Status screens in Figure 4-7-15 & Figure 4-7-16 appear.

Figure 4-7-15: Add Router Port Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
• **Type**	Sets the Router port type. The types of Router port as below: ■ Static ■ Forbid
• **Static Ports Select**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
• **Forbid Port Select**	Specify which ports un-act as router ports.

Button

 : Click to add IGMP router port entry.

Figure 4-7-16: Router Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID.
• **Static Ports**	Display the current static ports
• **Forbidden Ports**	Display the current forbidden ports
• **Modify**	Click **Edit** to edit parameter. Click **Delete** to delete the group ID entry.

4.7.2.6 IGMP Router Table

This page provides Router Table. The Dynamic, Static and Forbidden Router Table screens in Figure 4-7-17, Figure 4-7-18 & Figure 4-7-19 appear.

IGMP Router Table

▾ Dynamic Router Table

VLAN ID	Port	Expiry Time (Sec)
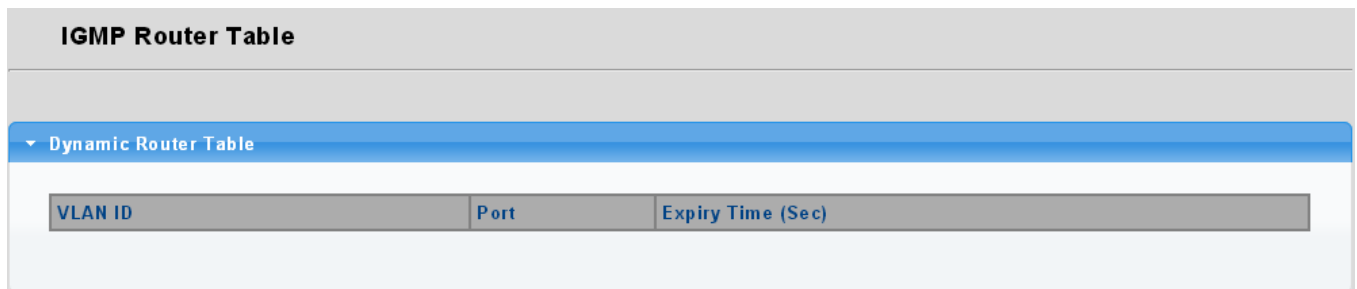
Figure 4-7-17: Dynamic Router Table Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID.
• **Port**	Display the current dynamic router ports
• **Expiry Time (Sec)**	Display the current expiry time
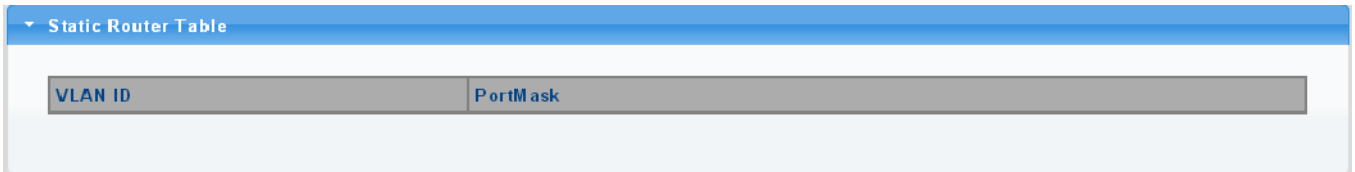
Figure 4-7-18: Static Router Table Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID.
• **Port Mask**	Display the current port mask.
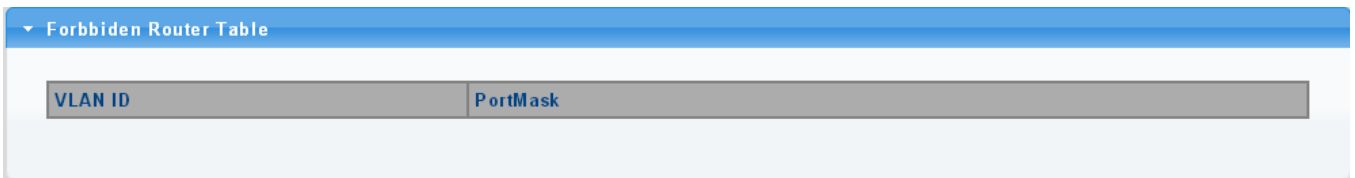
Figure 4-7-19: Forbidden Router Table Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID.
• **Port Mask**	Display the current port mask.

4.7.2.7 IGMP Forward All

This page provides IGMP Forward All. The Forward All screen in Figure 4-7-20 appears.

Figure 4-7-20: Forward All Setting Page Screenshot

The page includes the following fields:
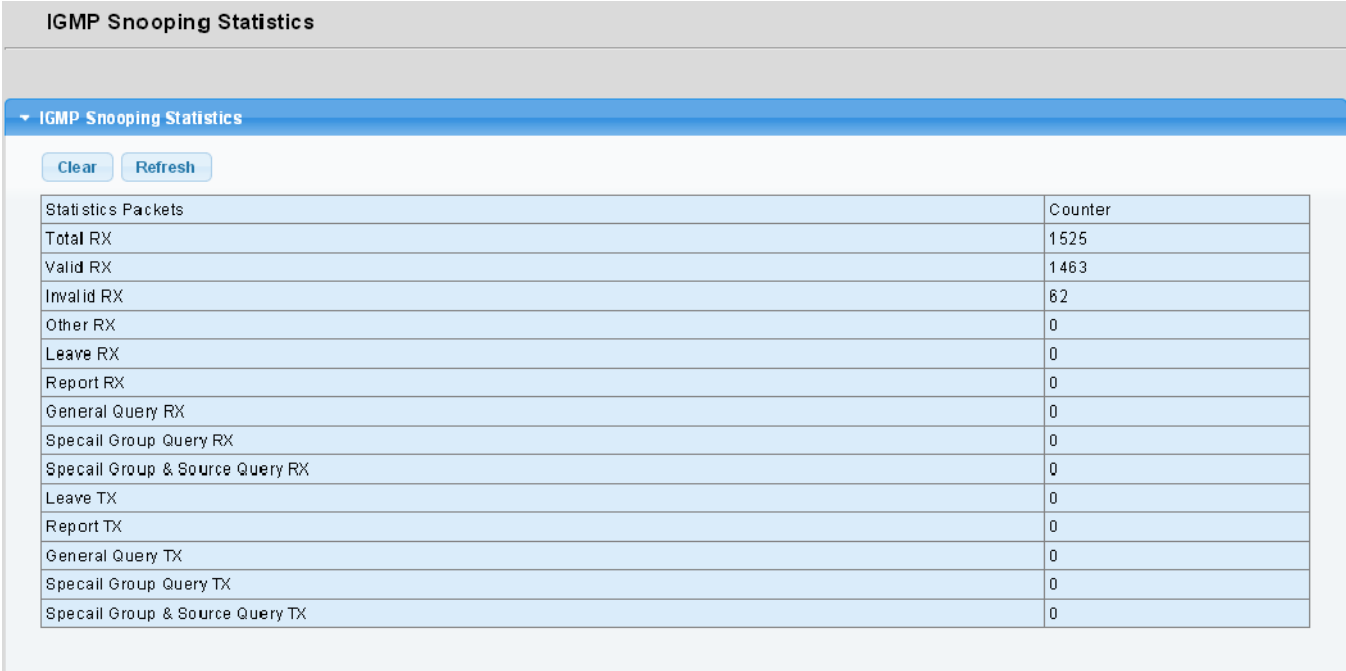
Object	Description	
• **VLAN ID**	Select VLAN ID for this drop down list to assign IGMP membership.	
• **Port**	The switch port number of the logical port.	
• **Membership**	Select IGMP membership for each interface:	
	Static:	Interface is a member of the IGMP.
	Forbidden:	Interface is forbidden from automatically joining the IGMP via MVR.
	None:	Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.

Button

Apply : Click to apply changes.

4.7.3 IGMP Snooping Statics

This page provides IGMP Snooping Statics. The IGMP Snooping Statics screen in Figure 4-7-21 appears.

IGMP Snooping Statistics

IGMP Snooping Statistics

Clear   Refresh
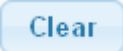
Statistics Packets	Counter
Total RX	1525
Valid RX	1463
Invalid RX	62
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Specail Group Query RX	0
Specail Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Specail Group Query TX	0
Specail Group & Source Query TX	0

Figure 4-7-21: Forward All Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Total RX**	Display current total RX
• **Valid RX**	Display current valid RX
• **Invalid RX**	Display current invalid RX
• **Other RX**	Display current other RX
• **Leave RX**	Display current leave RX
• **Report RX**	Display current report RX
• **General Query RX**	Display current general query RX
• **Special Group Query RX**	Display current special group query RX
• **Special Group & Source Query RX**	Display current special group & source query RX
• **Leave TX**	Display current leave TX
• **Report TX**	Display current report TX
• **General Query TX**	Display current general query TX
• **Special Group Query TX**	Display current special group query TX
• **Special Group & Source Query TX**	Display current special group & source query TX

Buttons

Clear : Click to clear the IGMP Snooping Statistics.

Refresh : Click to refresh the IGMP Snooping Statistics.

4.7.4 Multicast Throttling Setting

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

Once you have configured multicast profiles, you can assign them to interfaces on the PoE Managed Switch. Also you can set the multicast throttling number to limit the number of multicast groups an interface can join at the same time. The MAX Group and Information screens in Figure 4-7-22 & Figure 4-7-23 appear.
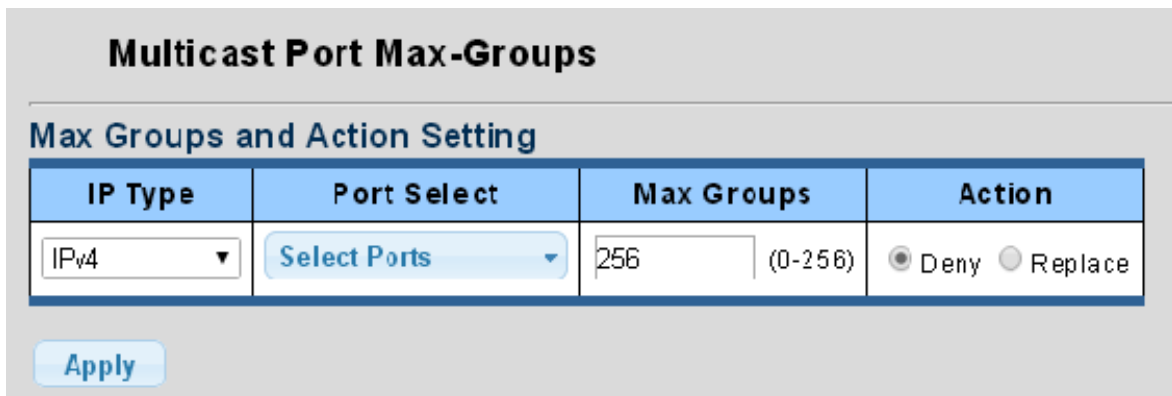
Figure 4-7-22: Max Groups and Action Setting Page Screenshot

The page includes the following fields:

Object	Description
• **IP Type**	Select IPv4 for this drop down list.
• **Port Select**	Select port number for this drop down list.
• **Max Groups**	Sets the maximum number of multicast groups an interface can join at the same time. Range: 0-256; Default: **256**
• **Action**	Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny) -**Deny** - The new multicast group join report is dropped. -**Replace** - The new multicast group replaces an existing group.

Button

Apply : Click to apply changes.

▾ IGMP Port Max Groups Information		
Port	**Max Groups**	**Action**
GE1	256	Deny
GE2	256	Deny
GE3	256	Deny
GE4	256	Deny
GE5	256	Deny
GE6	256	Deny
GE7	256	Deny
GE8	256	Deny
GE9	256	Deny
GE10	256	Deny
GE11	256	Deny
GE12	256	Deny
GE13	256	Deny
GE14	256	Deny
GE15	256	Deny
GE16	256	Deny
GE17	256	Deny
GE18	256	Deny
GE19	256	Deny
GE20	256	Deny
GE21	256	Deny
GE22	256	Deny
GE23	256	Deny
GE24	256	Deny
GE25	256	Deny
GE26	256	Deny
LAG1	256	Deny
LAG2	256	Deny
LAG3	256	Deny
LAG4	256	Deny
LAG5	256	Deny
LAG6	256	Deny
LAG7	256	Deny
LAG8	256	Deny

Figure 4-7-23: IGMP Port Max Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Max Groups**	Display the current Max groups.
• **Action**	Display the current action.

4.7.5 Multicast Filter

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service is based on a specific subscription plan. The multicast filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port.

Multicast filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A multicast filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, multicast join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the multicast join report is forwarded as normal. If a requested multicast group is denied, the multicast join report is dropped.

When you have created a Multicast profile number, you can then configure the multicast groups to filter and set the access mode.

Command Usage

- Each profile has only one access mode; either **permit** or **deny**.
- When the access mode is set to **permit**, multicast join reports are processed when a multicast group falls within the controlled range.
- When the access mode is set to **deny**, multicast join reports are only processed when the multicast group is not in the controlled range.

4.7.5.1 Multicast Profile Setting

The Add Profile and Profile Status screens in Figure 4-7-24 & Figure 4-7-25 appear.

Figure 4-7-24: Add Profile Setting Page Screenshot

The page includes the following fields:

Object	Description	
• **IP Type**	Select IPv4 for this drop down list.	
• **Profile Index**	Indicates the ID of this particular profile, the available range is 1 to 128.	
• **Group from**	Specifies multicast groups to include in the profile. Specify a multicast group range by entering a start IP address.	
• **Group to**	Specifies multicast groups to include in the profile. Specify a multicast group range by entering an end IP address.	
• **Action**	Sets the access mode of the profile; either **permit** or **deny**.	
	- Permit	Multicast join reports are processed when a multicast group falls within the controlled range.
	- Deny	When the access mode is set to, multicast join reports are only processed when the multicast group is not in the controlled range.

Button

Add : Click to add multicast profile entry.
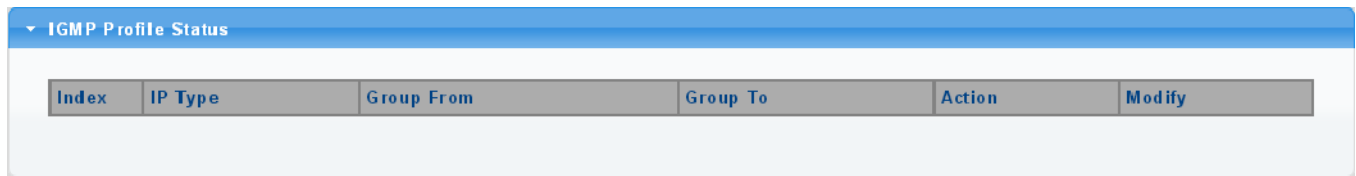
Figure 4-7-25: IGMP/MLD Profile Status Page Screenshot

The page includes the following fields:

Object	Description
• **Index**	Display the current index.
• **IP Type**	Display the current IP Type.
• **Group From**	Display the current group from.
• **Group To**	Display the current group to.
• **Action**	Display the current action.
• **Modify**	Click Edit to edit parameter. Click Delete to delete the IGMP profile entry.

4.7.5.2 IGMP Filter Setting

The Filter Setting and Status screens in Figure 4-7-26 & Figure 4-7-27 appear.
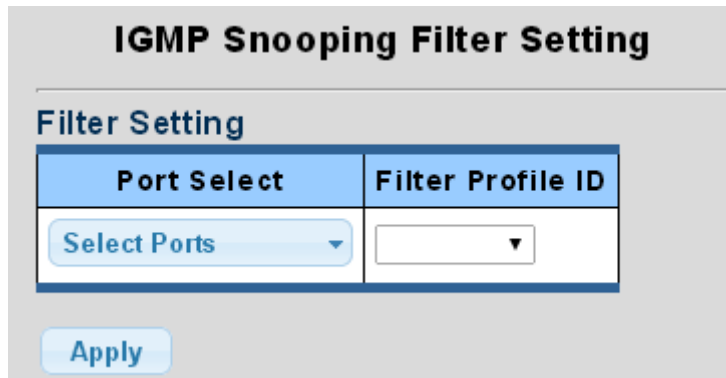
Figure 4-7-26: Filter Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number for this drop down list.
• **Filter Profile ID**	Select filter profile ID for this drop down list.

Button

Apply : Click to apply changes.
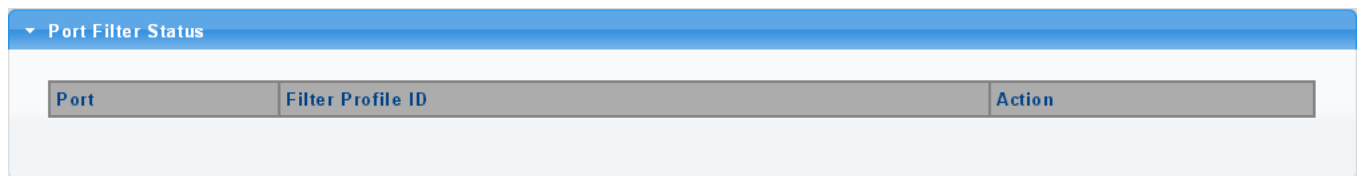
Figure 4-7-27: Port Filter Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Display the current port
• **Filter Profile ID**	Display the current filter profile ID
• **Action**	Click **Show** to display detail profile parameter. Click **Delete** to delete the IGMP filter profile entry.

4.8 Quality of Service

4.8.1 Understand QoS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. 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.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic.

You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

To implement QoS on your network, you need to carry out the following actions:

1.   Define a service level to determine the priority that will be applied to traffic.

2.   Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Switch.

3.   Create a QoS profile which associates a service level and a classifier.

4.   Apply a QoS profile to a port(s).

The **QoS** page of the PoE Managed Switch contains three types of QoS mode - the **802.1p** mode, **DSCP** mode or **Port-base** mode can be selected. Both the three mode rely on predefined fields within the packet to determine the output queue.

- **802.1p Tag Priority** Mode –The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.

- **IP DSCP** Mode - The output queue assignment is determined by the TOS or DSCP field in the IP packets.

- **Port-Base Priority** Mode – Any packet received from the specify high priority port will treated as a high priority packet.

The PoE Managed Switch supports **eight priority level** queue, the queue service rate is based on the **WRR**(**Weight Round Robin**) and **WFQ (Weighted Fair Queuing)** alorithm. The WRR ratio of high-priority and low-priority can be set to "**4:1** and **8:1.**

4.8.2 General

4.8.2.1 QoS Properties

The QoS Global Setting and Information screen in Figure 4-8-1 & Figure 4-8-2 appear.

Figure 4-8-1: QoS Global Setting Page Screenshot

The page includes the following fields:

Object	Description
• **QoS Mode**	Enable or disable QoS mode

Button

 : Click to apply changes.

Figure 4-8-2: QoS Information Page Screenshot

The page includes the following fields:

Object	Description
• **QoS Mode**	Display the current QoS mode.

4.8.2.2 QoS Port Settings

The QoS Port Settings and Status screen in Figure 4-8-3 & Figure 4-8-4 appear.

Figure 4-8-3: QoS Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number for this drop down list.
• **CoS Value**	Select CoS value for this drop down list, the available options are 0 to 7.
• **Remark CoS**	Disable or enable remark CoS
• **Remark DSCP**	Disable or enable remark DSCP
• **Remark IP Precedence**	Disable or enable remark IP Precedence

Button

Apply : Click to apply changes.

▼ QoS Port Status

Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
GE1	0	Disabled	Disabled	Disabled
GE2	0	Disabled	Disabled	Disabled
GE3	0	Disabled	Disabled	Disabled
GE4	0	Disabled	Disabled	Disabled
GE5	0	Disabled	Disabled	Disabled
GE6	0	Disabled	Disabled	Disabled
GE7	0	Disabled	Disabled	Disabled
GE8	0	Disabled	Disabled	Disabled
GE9	0	Disabled	Disabled	Disabled
GE10	0	Disabled	Disabled	Disabled
GE11	0	Disabled	Disabled	Disabled
GE12	0	Disabled	Disabled	Disabled
GE13	0	Disabled	Disabled	Disabled
GE14	0	Disabled	Disabled	Disabled
GE15	0	Disabled	Disabled	Disabled
GE16	0	Disabled	Disabled	Disabled
GE17	0	Disabled	Disabled	Disabled
GE18	0	Disabled	Disabled	Disabled
GE19	0	Disabled	Disabled	Disabled
GE20	0	Disabled	Disabled	Disabled
GE21	0	Disabled	Disabled	Disabled
GE22	0	Disabled	Disabled	Disabled
GE23	0	Disabled	Disabled	Disabled
GE24	0	Disabled	Disabled	Disabled
GE25	0	Disabled	Disabled	Disabled
GE26	0	Disabled	Disabled	Disabled
LAG1	0	Disabled	Disabled	Disabled
LAG2	0	Disabled	Disabled	Disabled
LAG3	0	Disabled	Disabled	Disabled
LAG4	0	Disabled	Disabled	Disabled
LAG5	0	Disabled	Disabled	Disabled
LAG6	0	Disabled	Disabled	Disabled
LAG7	0	Disabled	Disabled	Disabled
LAG8	0	Disabled	Disabled	Disabled

Figure 4-8-4: QoS Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **CoS Value**	Display the current CoS value.
• **Remark CoS**	Display the current remark CoS.
• **Remark DSCP**	Display the current remark DSCP.
• **Remark IP Precedence**	Display the current remark IP precedence.

4.8.2.3 Queue Settings

The Queue Table and Information screens in Figure 4-8-5 & Figure 4-8-6 appear.

Figure 4-8-5: Queue Table Page Screenshot

The page includes the following fields:

Object	Description
• **Queue**	Display the current queue ID.
• **Strict Priority**	Controls whether the scheduler mode is "Strict Priority" on this switch port.
• **WRR**	Controls whether the scheduler mode is "Weighted" on this switch port.
• **Weight**	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
• **% of WRR Bandwidth**	Display the current bandwith for each queue.

Button

Apply : Click to apply changes.

167
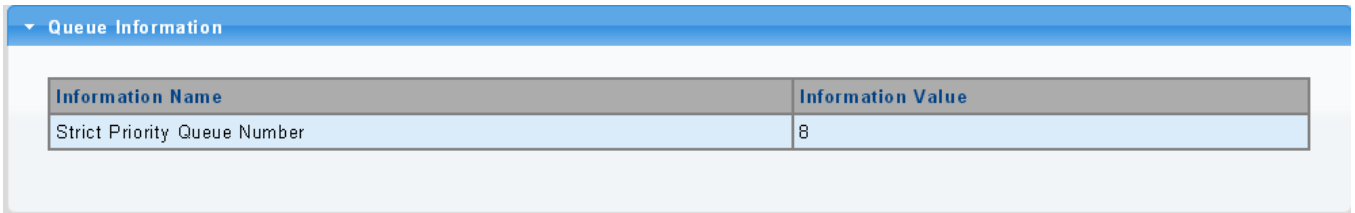
Figure 4-8-6: Queue Information Page Screenshot

The page includes the following fields:

Object	Description
• **Information Name**	Display the current queue method information
• **Information Value**	Display the current queue vlaue information

4.8.2.4 CoS Mapping

The CoS to Queue and Queue to CoS Mapping screens in Figure 4-8-7 & Figure 4-8-8 appear.
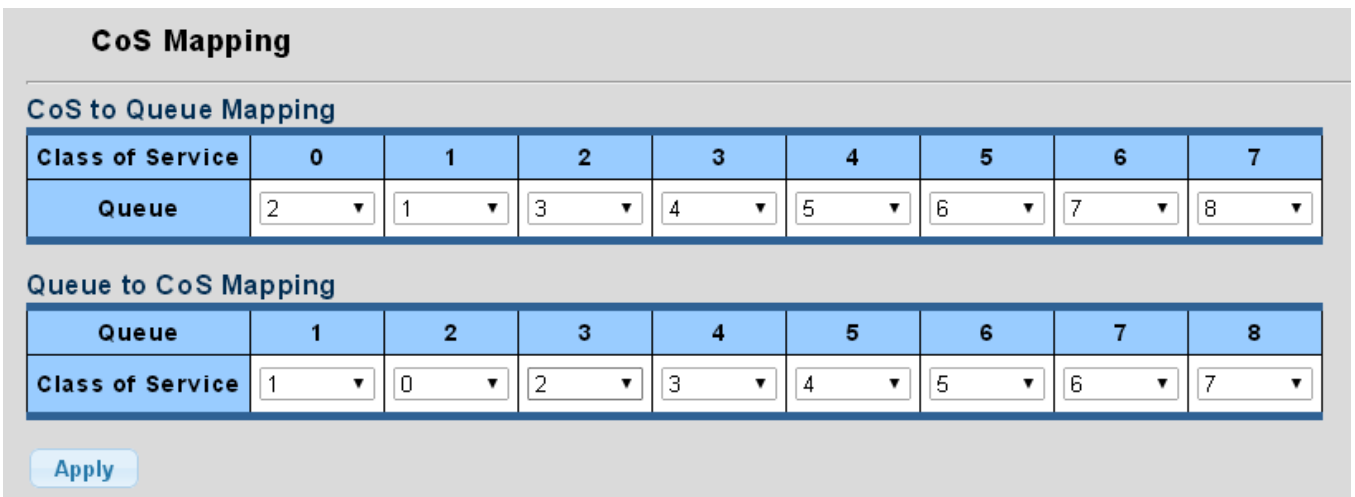
Figure 4-8-7: CoS to Queue and Queue to CoS Mapping Page Screenshot

The page includes the following fields:

Object	Description
• **Queue**	Select Queue value for this drop down list.
• **Class of Service**	Select CoS value for this drop down list.

Button

Apply : Click to apply changes.

Figure 4-8-8: CoS Mapping Page Screenshot

The page includes the following fields:

Object	Description
• **CoS**	Display the current CoS value.
• **Mapping to Queue**	Display the current mapping to queue.
• **Queue**	Display the current queue value.
• **Mapping to CoS**	Display the current mapping to CoS.

4.8.2.5 DSCP Mapping

The DSCP to Queue and Queue to DSCP Mapping screens in Figure 4-8-9 & Figure 4-8-10 appear.

Figure 4-8-9: DSCP to Queue and Queue to DSCP Mapping Page Screenshot

The page includes the following fields:

Object	Description
• **Queue**	Select Queue value for this drop down list.
• **DSCP**	Select DSCP value for this drop down list.

Button

Apply : Click to apply changes.

▼ DSCP Mapping

DSCP	Mapping to Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	2
9	2
10	2
11	2
12	2
13	2
14	2
15	2
16	3
17	3
18	3
19	3
20	3
21	3
22	3
23	3
24	4
25	4
26	4
27	4
28	4
29	4
30	4
31	4
32	5
33	5
34	5
35	5
36	5
37	5
38	5
39	5
40	6
41	6
42	6
43	6
44	6
45	6
46	6
47	6
48	7
49	7
50	7
51	7
52	7
53	7
54	7
55	7
56	8
57	8
58	8
59	8
60	8
61	8
62	8
63	8

Queue	Mapping to DSCP
1	0
2	8
3	16
4	24
5	32
6	40
7	48
8	56

Figure 4-8-10: DSCP Mapping Page Screenshot

171

The page includes the following fields:

Object	Description
• **DSCP**	Display the current CoS value.
• **Mapping to Queue**	Display the current mapping to queue.
• **Queue**	Display the current queue value.
• **Mapping to DSCP**	Display the current mapping to DSCP.

4.8.2.6 IP Precedence Mapping

The IP Precedence to Queue and Queue to IP Precedence Mapping screens in Figure 4-8-11 & Figure 4-8-12 appear.

Figure 4-8-11: IP Precedence to Queue and Queue to IP Precedence Mapping Page Screenshot

The page includes the following fields:

Object	Description
• **Queue**	Select Queue value for this drop down list.
• **IP Precedence**	Select IP Precedence value for this drop down list.

Button

Apply : Click to apply changes.

IP Precedence Mapping

IP Precedence	Mapping to Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Queue	Mapping to IP Precedence
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

Figure 4-8-12: IP Precedence Mapping Page Screenshot

The page includes the following fields:

Object	Description
• **IP Precedence**	Display the current CoS value.
• **Mapping to Queue**	Display the current mapping to queue.
• **Queue**	Display the current queue value.
• **Mapping to IP Precedence**	Display the current mapping to IP Precedence.

4.8.3 QoS Basic Mode

4.8.3.1 Global Settings

The Basic Mode Global Settings and QoS Information screen in Figure 4-8-13 & Figure 4-8-14 appear.
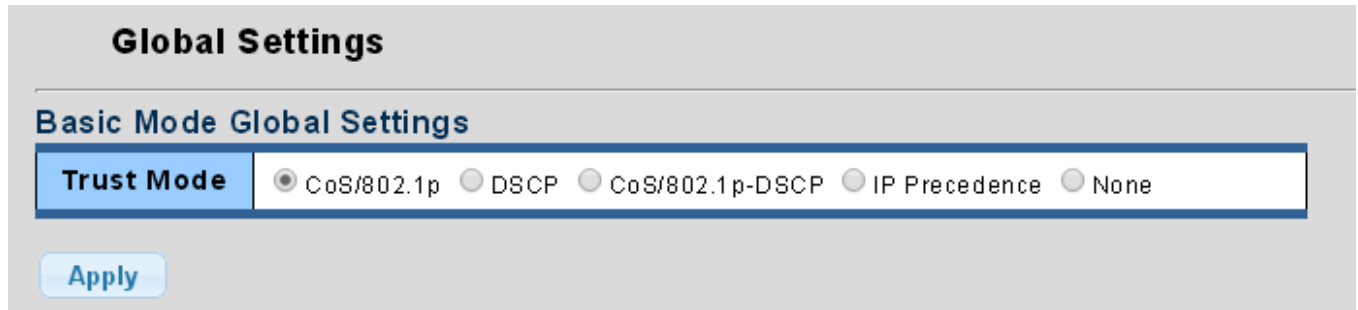
Figure 4-8-13: Basic Mode Global Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Trust Mode**	Set the QoS mode, the optios are shown as below: **Cos/802.1p (Default)** **DSCP** **CoS/802.1p-DSCP** **IP Precedence** **None**

Button

: Click to apply changes.
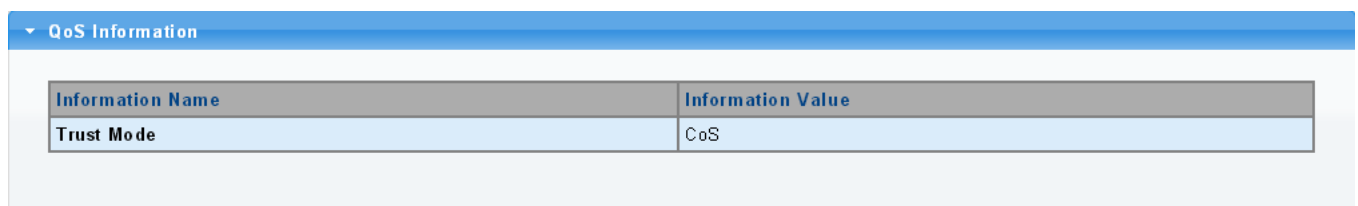
Figure 4-8-14: QoS Information Page Screenshot

The page includes the following fields:

Object	Description
• **Trust Mode**	Display the current QoS mode

4.8.3.2 Port Settings

The QoS Port Setting and Status screen in Figure 4-8-15 & Figure 4-8-16 appear.

Figure 4-8-15: Basic Mode Global Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number for this drop down list.
• **Trust Mode**	Enable or disable the trust mode.

Button

Apply : Click to apply changes.

▾ QoS Port Status

Port	Trust Type
GE1	Enabled
GE2	Enabled
GE3	Enabled
GE4	Enabled
GE5	Enabled
GE6	Enabled
GE7	Enabled
GE8	Enabled
GE9	Enabled
GE10	Enabled
GE11	Enabled
GE12	Enabled
GE13	Enabled
GE14	Enabled
GE15	Enabled
GE16	Enabled
GE17	Enabled
GE18	Enabled
GE19	Enabled
GE20	Enabled
GE21	Enabled
GE22	Enabled
GE23	Enabled
GE24	Enabled
GE25	Enabled
GE26	Enabled
LAG1	Enabled
LAG2	Enabled
LAG3	Enabled
LAG4	Enabled
LAG5	Enabled
LAG6	Enabled
LAG7	Enabled
LAG8	Enabled

Figure 4-8-16: QoS Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Trust Mode**	Display the current trust type.

4.8.4 QoS Advanced Mode

4.8.4.1 Global Settings

The Advanced Mode Global Settings and QoS Information screen in Figure 4-8-17 & Figure 4-8-18 appear.

Figure 4-8-17: Advanced Mode Global Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Trust Mode**	Set the QoS mode, the optios are shown as below: **Cos/802.1p (Default)** **DSCP** **CoS/802.1p-DSCP** **IP Precedence**
• **Default Mode Status**	Set the default mode as "Trusted" or "Not Trusted" (Default).

Button

Apply : Click to apply changes.

Figure 4-8-18: QoS Information Page Screenshot

The page includes the following fields:

Object	Description
• **Trust Mode**	Display the current QoS mode.
• **Default Mode Status**	Disaply the current default mode status.

4.8.4.2 Class Mapping

The QoS Class Mapping and Class Mapping status screen in Figure 4-8-19 & Figure 4-8-20 appear.

Class Configuration

Class Configuration

Class Name	
Match ACL Type	○ IP ○ MAC ○ IP or MAC
IP	☐ IPv4 [▼] or ☐ IPv6 [▼]
MAC	[▼]
Preferred ACL	◉ IP ○ MAC

Add

Figure 4-8-19: QoS Class Mapping Page Screenshot

The page includes the following fields:

Object	Description
• **Class Name**	Input the class name and 32 characters allowed.
• **Match ACL Type**	Choose "IP", "MAC" or "IP or MAC" as match ACL type.
• **IP**	Choose "IPv4" or "IPv6".
• **MAC**	Choose specific MAC adrress.
• **Preferred ACL**	Choose "IP" or "MAC" for preferred ACL.

Button

Add : Click to add Class Mapping profile entry.

Class Table

Class Name	Match	Action

Figure 4-8-20: QoS Class Mapping Table Page Screenshot

The page includes the following fields:

Object	Description
• **Class Name**	Display the current class name.
• **Match**	Disaply the current match information.
• **Action**	Disaply the current action information.

4.8.4.3 Aggregate Police

The QoS Aggregate Police and Aggregate Police status screen in Figure 4-8-21 & Figure 4-8-22 appear.

Figure 4-8-21: QoS Aggregate Police Page Screenshot

The page includes the following fields:

Object	Description
• **Aggregate Police Name**	Input the aggregate police name and 32 characters allowed.
• **Ingress Committed Information Rate (CIR)**	Allow input a number as ingress committed information rate.
• **Ingress Committed Burst Size (CBS)**	Allow input a number as ingress committed burst size.
• **Exceed Action**	Choose "Forward" or "Drop" when the exceed action situation appears.

Button

Add : Click to add aggregate police profile entry.

Figure 4-8-22: QoS Aggregate Police Table Page Screenshot

The page includes the following fields:

Object	Description
• **Police Name**	Display the current policer name.
• **Ingress CIR**	Disaply the current Ingress CIR information.
• **Ingress CBS**	Disaply the current Ingress CBS information.
• **Exceed Action**	Disaply the current exceed action information.
• **Action**	Disaply the current action information.

4.8.4.4 Policy Table

The QoS Policy table and Policy table status screen in Figure 4-8-23 & Figure 4-8-24 appear.

Figure 4-8-23: QoS Policy Table Page Screenshot

The page includes the following fields:

Object	Description
• **Policy Name**	Input the policy name and 31 characters allowed.

Button

Add : Click to add policy profile entry.
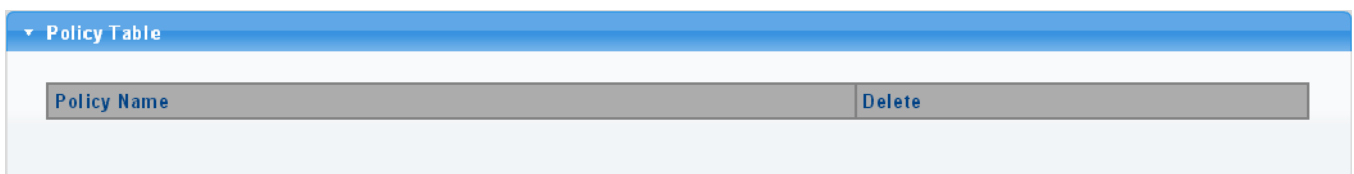
Figure 4-8-24: QoS Policy Table Page Screenshot

The page includes the following fields:

Object	Description
• **Policy Name**	Display the current policy name.
• **Delete**	Click **Delete** to delete the policy name profile entry.

4.8.4.5 Policy Class Maps

The QoS policy class maps and policy class maps status screen in Figure 4-8-25 & Figure 4-8-26 appear.

Figure 4-8-25: QoS Policy Class Maps Table Page Screenshot

The page includes the following fields:

Object	Description
• **Policy Name**	Allow choose one specific policy name.
• **Class Name**	Allow choose one specific class name.
• **Action Type**	Provide "Trust None", Always Trust" and "Set Queue" oprtions.
• **Police Type**	Provide "None", "Single" and "Aggregate" options.
• **Aggregate Police**	Allow choose one specific aggregate police profile.
• **Ingress Committed**	Allow input a number as ingress committed information rate.

Information Rate (CIR)	
• **Ingress Committed Burst Size (CBS)**	Allow input a number as ingress committed burst size.
• **Exceed Action**	Choose "Forward" or "Drop" when the exceed action situation appears.

Button

Add : Click to add policy class maps profile entry.
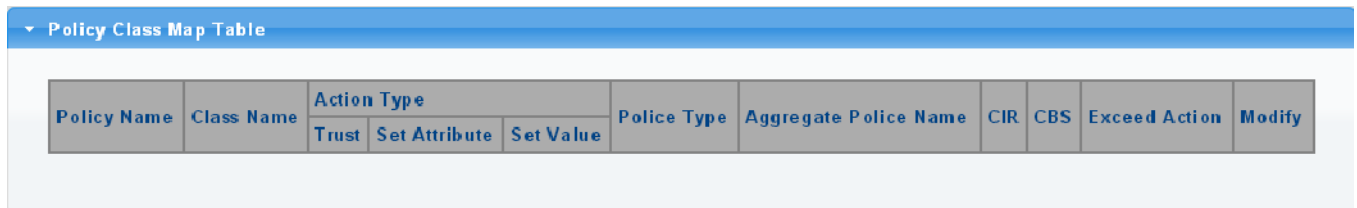
Figure 4-8-26: QoS Policy Class Map Table Page Screenshot

The page includes the following fields:

Object	Description
• **Policy Name**	Display the current policy name information.
• **Class Name**	Disaply the current class name information.
• **Action Type**	Disaply current "Trust", "Set Attribute" and "Set Value" information.
• **Police Type**	Display current policy type information.
• **Aggregate Police Name**	Display current Aggregate Police Name information.
• **CIR**	Display current CIR information.
• **CBS**	Display current CBS information.
• **Exceed Action**	Display current exceed action information.
• **Modify**	Click **Edit** to edit parameter. Click **Delete** to delete the policy class maps profile entry.

4.8.4.6 Policy Binding

The QoS policy binding and policy bidning table screen in Figure 4-8-27 & Figure 4-8-28 appear.

Figure 4-8-27: QoS Policy Binding Table Page Screenshot

The page includes the following fields:

Object	Description
• **Policy Select**	Select policy from this drop down list.
• **Binding Port**	Select one specific port from this drop down list.

Button

Apply : Click to apply changes.

▼ **Policy Binding Table**

Port	Policy Name
GE1	
GE2	
GE3	
GE4	
GE5	
GE6	
GE7	
GE8	
GE9	
GE10	
GE11	
GE12	
GE13	
GE14	
GE15	
GE16	
GE17	
GE18	
GE19	
GE20	
GE21	
GE22	
GE23	
GE24	
GE25	
GE26	
LAG1	
LAG2	
LAG3	
LAG4	
LAG5	
LAG6	
LAG7	
LAG8	

Figure 4-8-28: QoS Policy Binding Table Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Disaply per port information.
• **Policy Name**	Display the current policy name information.

4.8.5 Rate Limit

Configure the switch port rate limit for the switch port on this page.

4.8.5.1 Ingress Bandwidth Control

This page provides to select the ingress bandwidth preamble. The Ingress Bandwidth Control Setting and Status screens in Figure 4-8-29 & Figure 4-8-30 & Figure 4-8-31 appear.

Figure 4-8-29: Ingress Bandwidth Control Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Burst Size**	Allow assigning burst size and the options are 1 to 65535. Unit: Bytes.
• **Port**	Select port number for this drop down list.
• **State**	Enable or disable the port rate policer. The default value is "Disabled".
• **Rate (Kbps)**	Configure the rate for the port policer. The default value is "unlimited". Valid values are in the range 0 to 1000000, must a multiple of 16.

Button

Apply : Click to apply changes.

Figure 4-8-30: Ingress Port Burst Size Configuration Page Screenshot

185

The page includes the following fields:

Object	Description
• **Burst Size**	Display current burst size information.

Figure 4-8-31: Ingress Bandwidth Control Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Ingress Rate Limit (Kbps)**	Display the current ingress rate limit.

186

4.8.5.2 Ingress VLAN Settings

This page provides to select the VLAN ingress bandwidth preamble. The VLAN Ingress Bandwidth Control Setting and Status screens in Figure 4-8-32 & Figure 4-8-33 appear.

Figure 4-8-32: VLAN Ingress Bandwidth Control Settings Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN**	Select VLAN number for this drop down list.
• **Port**	Select port number for this drop down list.
• **State**	Enable or disable the port rate policer. The default value is "Disabled".
• **Rate (Kbps)**	Configure the rate for the VLAN ingress bandwidth. The default value is "unlimited". Valid values are in the range 0 to 1000000, must a multiple of 16.

Button

Apply : Click to apply changes.

Figure 4-8-33: VLAN Ingress Bandwidth Control Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN**	Display the VLAN group information.
• **Port**	The switch port number of the logical port.
• **Rate (Kbps)**	Display the current ingress rate limit.

4.8.5.3 Egress Bandwidth Control

This page provides to select the egress bandwidth preamble. The Egress Bandwidth Control Setting and Status screens in Figure 4-8-34 & Figure 4-8-35 & Figure 4-8-36 appear.

Figure 4-8-34: Egress Bandwidth Control Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Burst Size**	Allow assigning burst size and the options are 1 to 65535. Unit: Bytes.
• **Port**	Select port number for this drop down list.
• **State**	Enable or disable the port rate policer. The default value is "Disabled".
• **Rate (Kbps)**	Configure the rate for the port policer. The default value is "unlimited". Valid values are in the range 0 to 1000000, must a multiple of 16.

Button

Apply : Click to apply changes.

Figure 4-8-35: Egress Port Burst Size Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Burst Size**	Display current burst size information.

Figure 4-8-36: Egress Bandwidth Control Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Egress Rate Limit (Kbps)**	Display the current egress rate limit.

4.8.5.4 Egress Queue Settings

The Egress Queue Badwidth Control Settings and Status screens in Figure 4-8-37 & Figure 4-8-38 & Figure 4-8-39 appear.

Figure 4-8-37: Egress Queue BandwidthSettings Page Screenshot

The page includes the following fields:

Object	Description
• **Burst Size**	Allow assigning burst size and the options are 1 to 65535. Unit: Bytes.
• **Port**	Select port number for this drop down list.
• **Queue**	Select queue numbers for this drop down list, options are 1 to 8.
• **State**	Enable or disable the port rate policer. The default value is "Disabled".
• **CIR (Kbps)**	Configure the CIR for the port policer. The default value is "unlimited". Valid values are in the range 0 to 1000000, must a multiple of 16.

Button

Apply : Click to apply changes.

Figure 4-8-38: Egress Port Burst Size Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Burst Size**	Display current burst size information.

Figure 4-8-39: Egress Queue Status Page Screenshot

The page includes the following fields:

Object	Description
• **Queue ID**	Display the current queue ID
• **Rate Limit (Kbps)**	Display the current rate limit.

191

4.9 Security

This section is to control the access of the PoE Managed Switch, including the user access and management control.

The Security Page contains links to the following main topics:

- ■ **Strom Control**
- ■ **802.1x**
- ■ **DHCP Snooping**
- ■ **Port Security**
- ■ **AAA**
- ■ **TACACS+ Server**
- ■ **Radius Server**
- ■ **Access**

4.9.1 Storm Control

Storm control for the switch is configured on this Page.

There is an unknown unicast storm rate control, unknown multicast storm rate control, and a broadcast storm rate control.

These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

4.9.1.1 Global Setting

The Storm Control Global Setting and Information screens in Figure 4-9-1 & Figure 4-9-2 appear.

Figure 4-9-1: Storm Control Global Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Unit**	Controls the unit of measure for the storm control rate as "pps" or "bps". The default value is "bps".
• **Preamble & IFG**	Set the excluded or included interframe gap

Button

Apply : Click to apply changes.

Figure 4-9-2: Storm Control Global Information Page Screenshot

The page includes the following fields:

Object	Description
• **Unit**	Display the current unit.
• **Preamble & IFG**	Display the current preamble & IFG.

4.9.1.2 Port Setting

Storm control for the switch is configured on this page. There are three types of storm rate control:

- **Broadcast** storm rate control
- **Unknown Unicast** storm rate control
- **Unknow Multicast** storm rate contro.l

The configuration indicates the permitted packet rate for unknown unicast, unknown multicast, or broadcast traffic across the switch. The Storm Control Configuration screens in Figure 4-9-3 & Figure 4-9-4 appear.

Figure 4-9-3: Storm Control Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.

• **Port State**	Enable or disable the storm control status for the given storm type.	
• **Action**	Configures the action performed when storm control is over rate on a port. Valid values are **Shutdown** or **Drop**.	
• **Type Enable**	The settings in a particular row apply to the frame type listed here: ■ **Broadcast** ■ **Unknown Multicast** ■ **Unknown Unicast**	
• **Rate (kbps/pps)**	Configure the rate for the storm control. The default value is "10,000" and unit is 16Kbps.	

Button

Apply : Click to apply changes.

Figure 4-9-4: Storm Control Information Page Screenshot

194

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Port State**	Display the current port state.
• **Broadcast (16Kbps)**	Display the current brocast storm control rate.
• **Unknown Multicast (16Kbps)**	Display the current unknown multicast storm control rate.
• **Unknown Unicast (16Kbps)**	Display the current unknown unicast storm control rate.
• **Action**	Display the current action.

4.9.2 802.1X

Overview of 802.1X (Port-based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as **EAPOL (EAP Over LANs)** frames. EAPOL frames encapsulate **EAP PDU**s (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like **MD5-Challenge**, **PEAP**, and **TLS**. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

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

Overview of User Authentication

It is allowed to configure the PoE Managed Switch to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This PoE Managed Switch provides secure network management access using the following options:

- **Remote Authentication Dial-in User Service (RADIUS)**
- **Terminal Access Controller Access Control System Plus   (TACACS+)**
- **Local user name and Priviledge Level control**

4.9.2.1 Understanding IEEE 802.1X Port-based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1X access control allows only **Extensible Authentication Protocol over LAN (EAPOL)** traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ **Device Roles**

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.
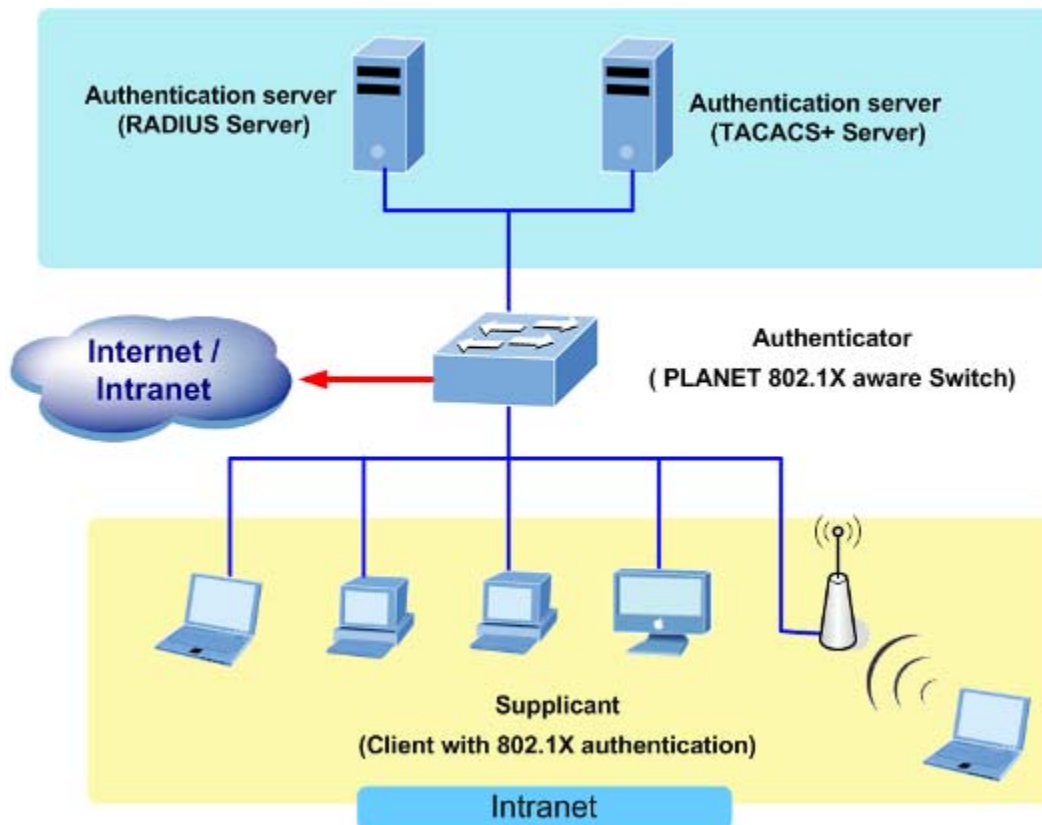
Figure 4-9-5

- *Client*—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the IEEE 802.1X specification.)

- *Authentication server*—performs the actual authentication of the client. The authentication server validates the

identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with **Extensible Authentication Protocol (EAP)** extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

● *Switch* **(802.1X device)**—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

■ **Authentication Initiation and Message Exchange**

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity

> If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. "Figure 4-9-6" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.
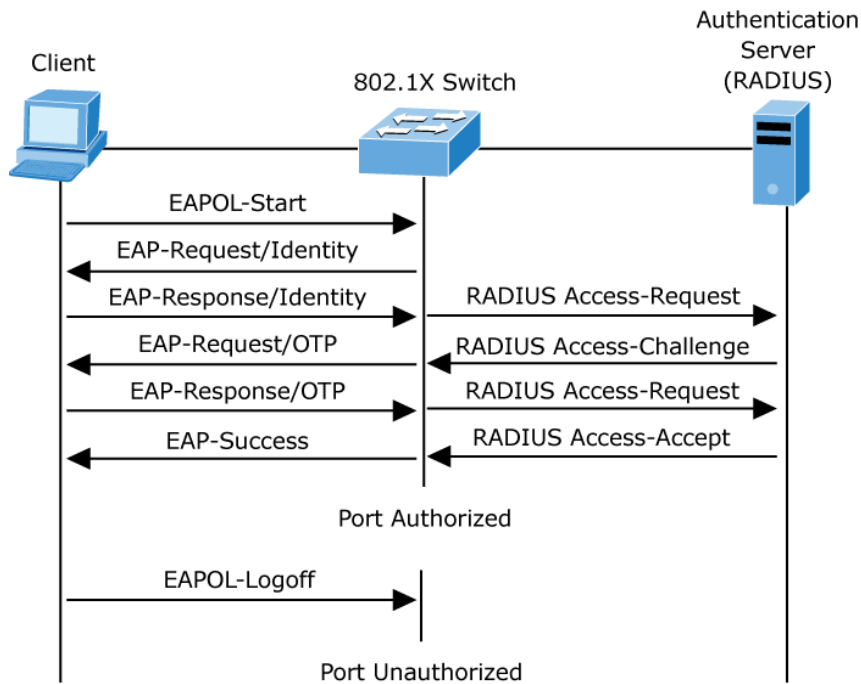
Figure 4-9-6: EAP Message Exchange

■ **Ports in Authorized and Unauthorized States**

The switch port state determines whether or not the client is granted access to the network. The port starts in the *unauthorized* state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the *authorized* state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

4.9.2.2 802.1X Setting

This page allows you to configure the IEEE 802.1X authentication system.

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

The 802.1X Setting and Information screens in Figure 4-9-7 & Figure 4-9-8 appear.
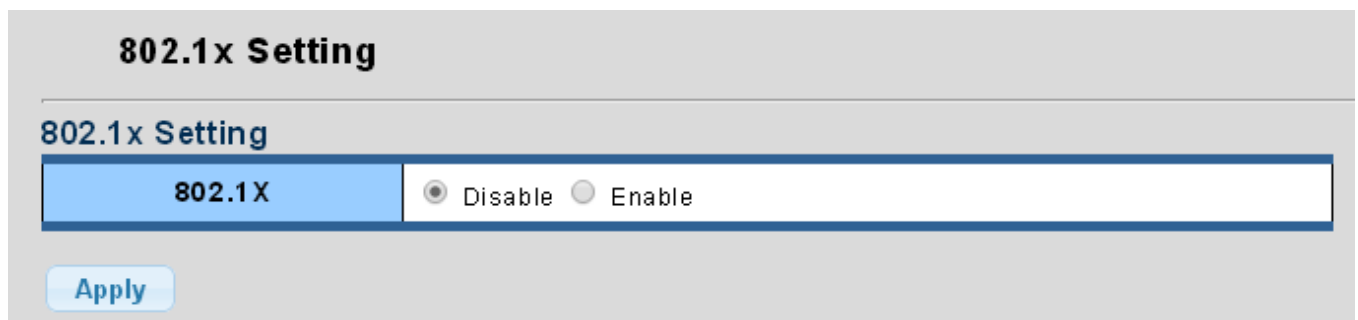
Figure 4-9-7: 802.1X Setting Page Screenshot

The page includes the following fields:

Object	Description
• **802.1X**	Enable or disable the 802.1x function and default is disable.

Button

 : Click to apply changes.
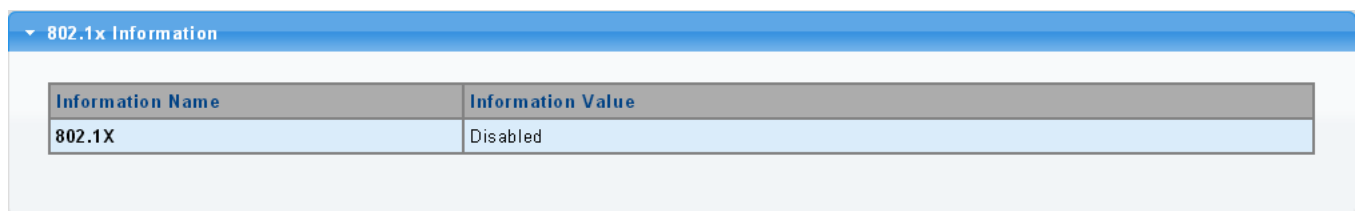
Figure 4-9-8: 802.1X Information Page Screenshot

The page includes the following fields:

Object	Description
• **802.1X**	Display the current 802.1X state.

4.9.2.3 802.1X Port Setting

This page allows you to configure the IEEE 802.1X Port Setting. The 802.1X Port Setting screens in Figure 4-9-9 & Figure 4-9-10 appear.

Figure 4-9-9: 802.1X Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **Mode**	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: ■ **No Authentication** ■ **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. ■ **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.
• **Reauthentication Enable**	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a

	switch port or if a supplicant is no longer attached.
• **Reauthentication Period**	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 30 to 65535 seconds.
• **Quiet Period**	Sets time to keep silent on supplicant authentication failure.
• **Supplicant Period**	Sets the interval for the supplicant to re-transmit EAP request/identify frame.
• **Maximun Request Retries**	The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.

Button

Apply : Click to apply changes.

▼ 802.1x Port Status

Port	Mode (pps)	Status (pps)	Periodic Reauthentication	Reauthentication Period	Quiet Period	Supplicant Timeout	Max. EAP Requests	Modify
GE1	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE2	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE3	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE4	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE5	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE6	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE7	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE8	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE9	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE10	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE11	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE12	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE13	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE14	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE15	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE16	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE17	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE18	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE19	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE20	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE21	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE22	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE23	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE24	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE25	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE26	802.1X Disabled	-	Enabled	3600	60	30	2	Edit

Figure 4-9-10 : 802.1X Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Mode (pps)**	Display the current mode.
• **Status (pps)**	Display the current status.
• **Periodic Reauthentication**	Display the current periodic reauthentication.
• **Reauthentication Period**	Display the current reauthentication period.
• **Quiet Period**	Display the current quiet period.
• **Supplicant Timeout**	Display the current supplicant timeout.
• **Max. EAP Requests**	Display the current Max. EAP requests.
• **Modify**	Click **Edit** to edit 802.1X port setting parameter.

4.9.2.4 Guest VLAN Setting

Overview

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meantime, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

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

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

The 802.1X Guest VLAN setting screens in Figure 4-9-11 & Figure 4-9-12 appear.
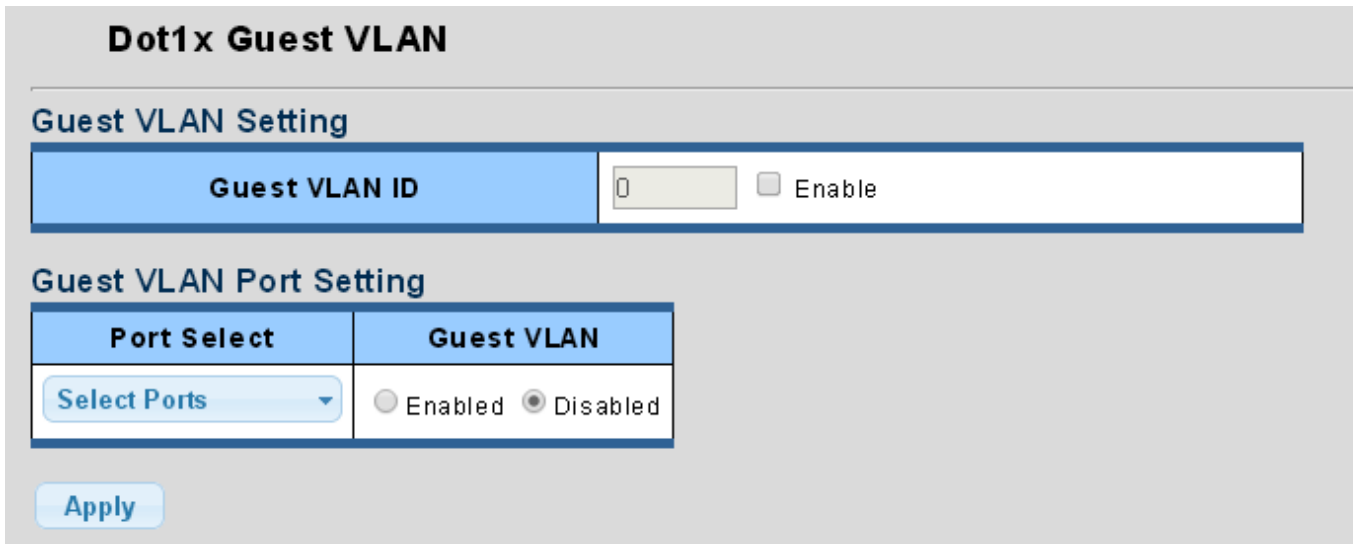
Figure 4-9-11: Guest VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Guest VLAN ID**	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1~4094].
• **Port**	Select port for this drop down list.
• **Guest VLAN Enabled**	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. ■ When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. ■ When unchecked, the ability to move to the Guest VLAN is disabled for all ports.

Button

Apply : Click to apply changes.

▼ Guest VLAN Status

Port Name	Enable State	In Guest VLAN
GE1	Disabled	NO
GE2	Disabled	NO
GE3	Disabled	NO
GE4	Disabled	NO
GE5	Disabled	NO
GE6	Disabled	NO
GE7	Disabled	NO
GE8	Disabled	NO
GE9	Disabled	NO
GE10	Disabled	NO
GE11	Disabled	NO
GE12	Disabled	NO
GE13	Disabled	NO
GE14	Disabled	NO
GE15	Disabled	NO
GE16	Disabled	NO
GE17	Disabled	NO
GE18	Disabled	NO
GE19	Disabled	NO
GE20	Disabled	NO
GE21	Disabled	NO
GE22	Disabled	NO
GE23	Disabled	NO
GE24	Disabled	NO
GE25	Disabled	NO
GE26	Disabled	NO

Figure 4-9-12: Guest VLAN Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port Name**	The switch port number of the logical port.
• **Enable State**	Display the current state.
• **In Guest VLAN**	Display the current guest VLAN.

4.9.2.5 Authenticed Host

The Authenticated Host Table screen in Figure 4-9-13 appears.

Authenticated Hosts

▼ Authenticated Host Table

User Name	Port	Session Time	Authentication Method	MAC Address
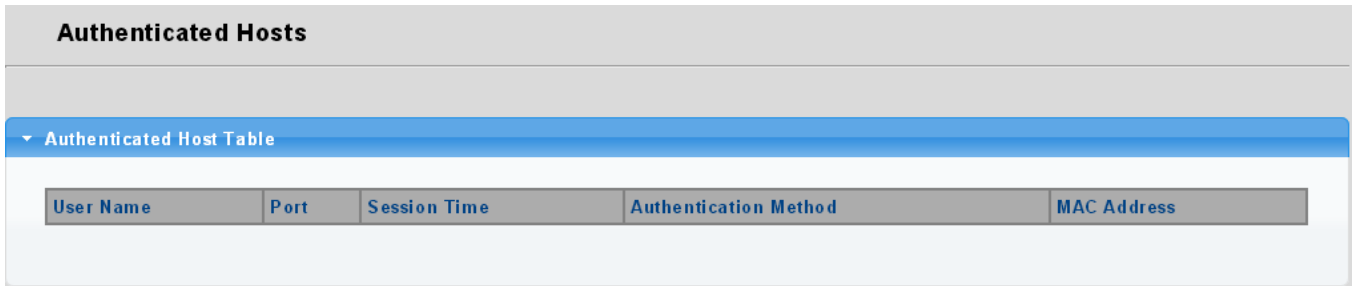
Figure 4-9-13: Authenticated Host Table Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	Display the current user name.
• **Port**	Display the current port number.
• **Session Time**	Display the current session time.
• **Authentication Method**	Display the current authentication method.
• **MAC Address**	Display the current MAC address.

4.9.3 DHCP Snooping

4.9.3.1 DHCP Snooping Overview

The addresses assigned to DHCP clients on unsecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.
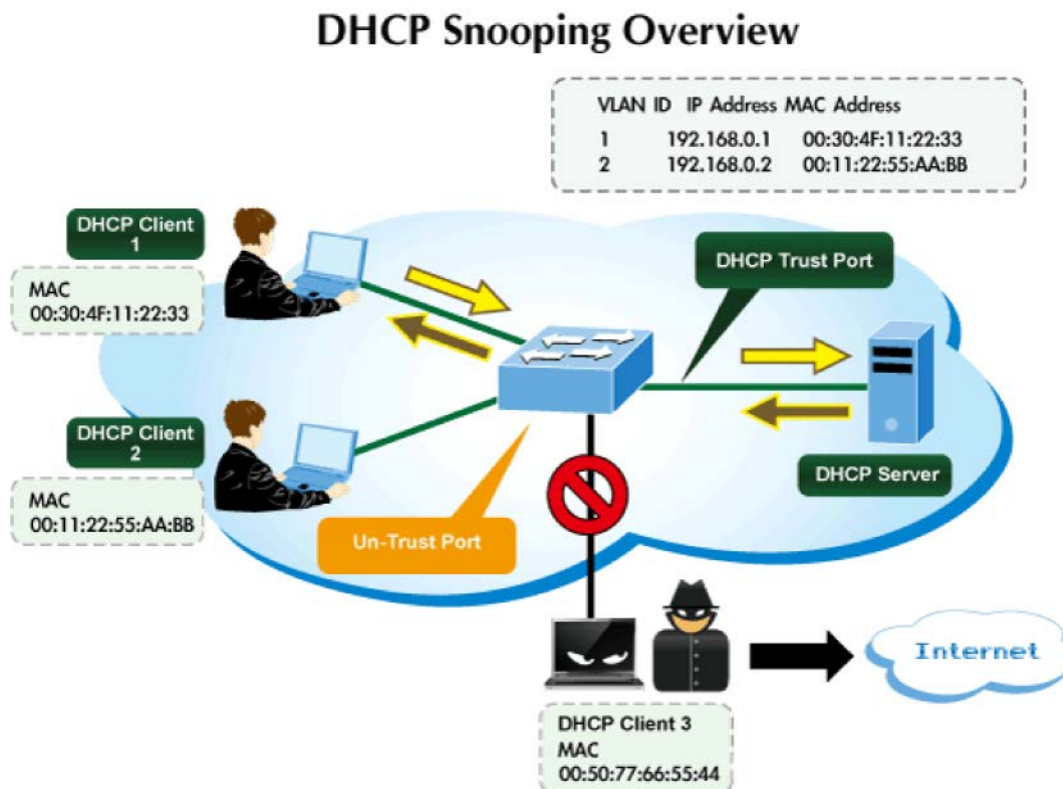
Command Usage

• Network traffic may be disrupted when malicious DHCP messages are received from an outside source. **DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall**. When DHCP snooping is enabled globally and enabled on a VLAN interface, **DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped**.

• Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

• When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

• Filtering rules are implemented as follows:
  ■ If the global DHCP snooping is disabled, all DHCP packets are forwarded.

- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:

  - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.

  - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.

  - If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.

  - If the DHCP packet is not a recognizable type, it is dropped.

- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

- Additional considerations when the switch itself is a DHCP client – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

4.9.3.2 Global Setting

DHCP Snooping is used to block intruder on the untrusted ports of switch when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server. Configure DHCP Snooping on this page. The DHCP Snooping Setting and Information screens in Figure 4-9-14 & Figure 4-9-15 appear.
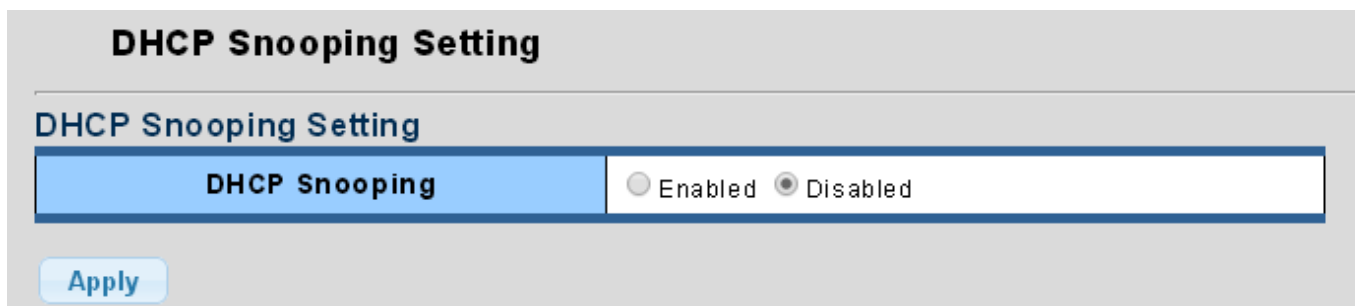
Figure 4-9-14: DHCP Snooping Setting Page Screenshot

The page includes the following fields:

Object	Description
• **DHCP Snooping**	Indicates the DHCP snooping mode operation. Default mode is Disabled and possible modes are: ■ **Enabled**: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. ■ **Disabled**: Disable DHCP snooping mode operation.

Button

Apply : Click to apply changes.

▾ **DHCP Snooping Information**

Information Name	Information Value
DHCP Snooping	Disabled
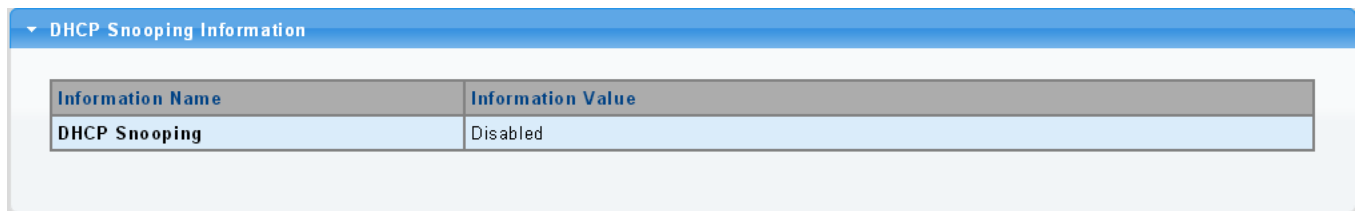
Figure 4-9-15: DHCP Snooping Information Page Screenshot

The page includes the following fields:

Object	Description
• **DHCP Snooping**	Display the current DHCP snooping status.

4.9.3.3 VLAN Setting

Command Usage

• When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.

• When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.

• When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

The DHCP Snooping VLAN Setting screens in Figure 4-9-16 & Figure 4-9-17 appear.
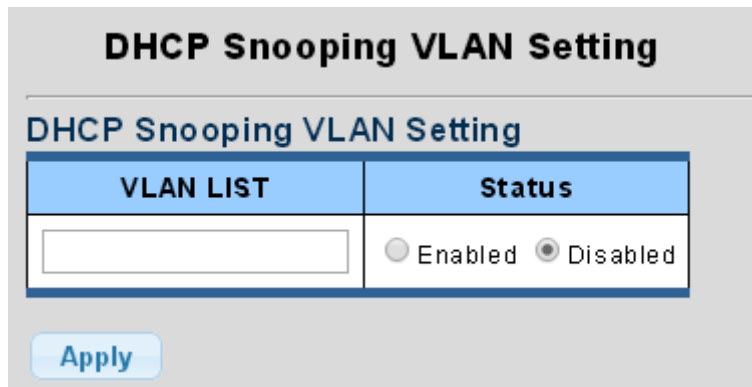
Figure 4-9-16: DHCP Snooping VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN List**	Indicates the ID of this particular VLAN.
• **Status**	Indicates the DHCP snooping VLAN mode operation. Default mode is Disabled and possible modes are: ■ **Enabled**: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. ■ **Disabled**: Disable DHCP snooping mode operation.

Button

Apply : Click to apply changes.
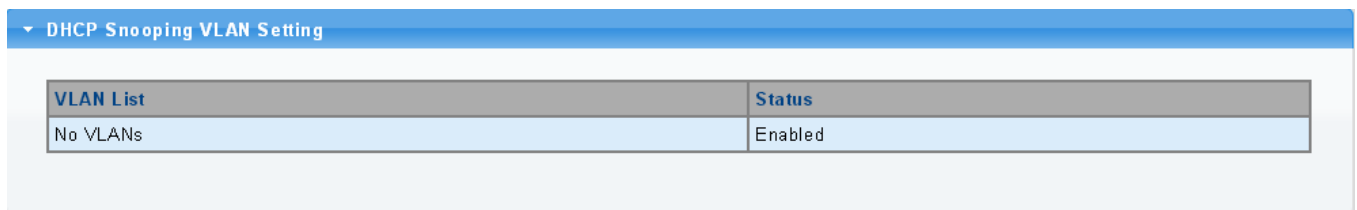
Figure 4-9-17: DHCP Snooping VLAN Setting Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN List**	Display the current VLAN list.
• **Status**	Display the current DHCP snooping status.

4.9.3.4 Port Setting

Configures switch ports as trusted or untrusted.

Command Usage

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.
- When DHCP snooping enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- Set all ports connected to DHCP servers within the local network or firewall to trusted state. Set all other ports outside the local network or firewall to untrusted state.

The DHCP Snooping Port Setting screen in Figure 4-9-18 & Figure 4-9-19 appears.
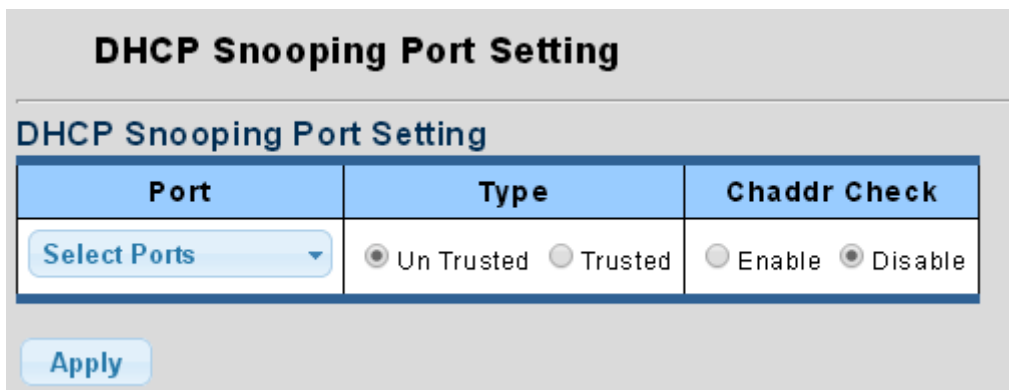
Figure 4-9-18: DHCP Snooping Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **Type**	Indicates the DHCP snooping port mode. Default mode is Untrusted and possible modes are: ■ **Trusted**: Configures the port as trusted sources of the DHCP message. ■ **Untrusted**: Configures the port as untrusted sources of the DHCP message.
• **Chaddr Check**	Indicates that the Chaddr check function is enabled on selected port. Chaddr: Client hardware address.

Button

Apply : Click to apply changes.

▾ **DHCP Snooping Port Setting**

Port	Type	Chaddr Check
GE1	Un Trusted	Disabled
GE2	Un Trusted	Disabled
GE3	Un Trusted	Disabled
GE4	Un Trusted	Disabled
GE5	Un Trusted	Disabled
GE6	Un Trusted	Disabled
GE7	Un Trusted	Disabled
GE8	Un Trusted	Disabled
GE9	Un Trusted	Disabled
GE10	Un Trusted	Disabled
GE11	Un Trusted	Disabled
GE12	Un Trusted	Disabled
GE13	Un Trusted	Disabled
GE14	Un Trusted	Disabled
GE15	Un Trusted	Disabled
GE16	Un Trusted	Disabled
GE17	Un Trusted	Disabled
GE18	Un Trusted	Disabled
GE19	Un Trusted	Disabled
GE20	Un Trusted	Disabled
GE21	Un Trusted	Disabled
GE22	Un Trusted	Disabled
GE23	Un Trusted	Disabled
GE24	Un Trusted	Disabled
GE25	Un Trusted	Disabled
GE26	Un Trusted	Disabled
LAG1	Un Trusted	Disabled
LAG2	Un Trusted	Disabled
LAG3	Un Trusted	Disabled
LAG4	Un Trusted	Disabled
LAG5	Un Trusted	Disabled
LAG6	Un Trusted	Disabled
LAG7	Un Trusted	Disabled
LAG8	Un Trusted	Disabled

Figure 4-9-19: DHCP Snooping Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Type**	Display the current type.
• **Chaddr Check**	Display the current chaddr check.

4.9.3.5 Statistics

The DHCP Snooping Statistics screen in Figure 4-9-20 appears.

Figure 4-9-20: DHCP Snooping Statistics Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Forwarded**	Display the current forwarded
• **Chaddr Check Dropped**	Display the chaddr check dropped
• **Untrust Port Dropped**	Display untrust port dropped

• **Untrust Port with Option82 Dropped**	Display untrust port with option82 dropped
• **Invaild Dropped**	Display invalid dropped

Buttons

Clear : Click to clear the statistics.

Refresh : Click to refresh the statistics.

4.9.3.6 Rate Limit

After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The DHCP Rate Limit Setting and Config screens in Figure 4-9-21 & Figure 4-9-22 appear.

DHCP Rate Limit

DHCP Rate Limit Setting

Port	State	Rate Limit (pps)
Select Ports ▼	⦿ Default ○ User-Define	Unlimited (1~50 pps)

Apply
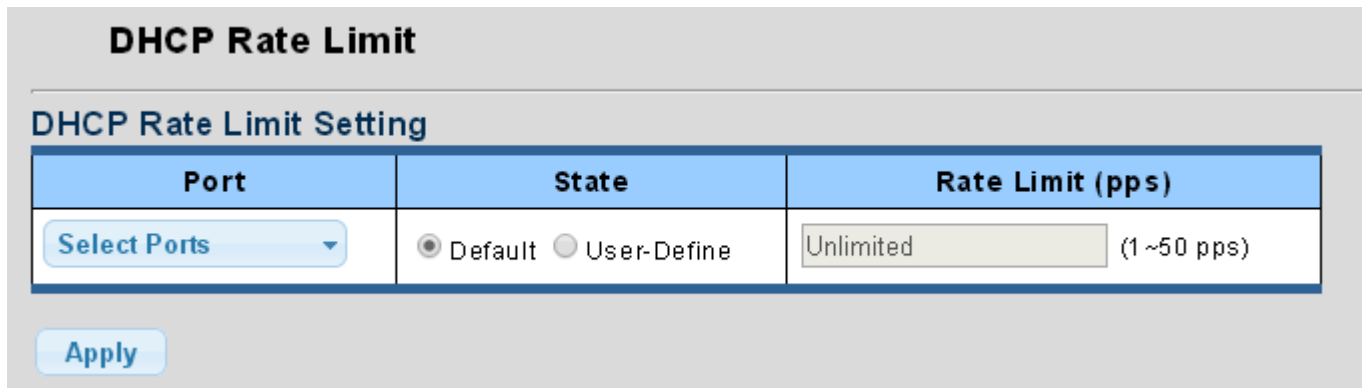
Figure 4-9-21: DHCP Rate Limit Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **State**	Set default or user-define.
• **Rate Limit (pps)**	Configure the rate limit for the port policer. The default value is "unlimited". Valid values are in the range 1 to 50 and unit is pps.

Button

Apply : Click to apply changes.

DHCP Rate Limit Config	
Port Name	**Rate Limit (pps)**
GE1	Unlimited
GE2	Unlimited
GE3	Unlimited
GE4	Unlimited
GE5	Unlimited
GE6	Unlimited
GE7	Unlimited
GE8	Unlimited
GE9	Unlimited
GE10	Unlimited
GE11	Unlimited
GE12	Unlimited
GE13	Unlimited
GE14	Unlimited
GE15	Unlimited
GE16	Unlimited
GE17	Unlimited
GE18	Unlimited
GE19	Unlimited
GE20	Unlimited
GE21	Unlimited
GE22	Unlimited
GE23	Unlimited
GE24	Unlimited
GE25	Unlimited
GE26	Unlimited
LAG1	Unlimited
LAG2	Unlimited
LAG3	Unlimited
LAG4	Unlimited
LAG5	Unlimited
LAG6	Unlimited
LAG7	Unlimited
LAG8	Unlimited

Figure 4-9-22: DHCP Rate Limit Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port Name**	The switch port number of the logical port.
• **Rate Limit (pps)**	Display the current rate limit.

4.9.3.7 Option82 Global Setting

DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to DHCP servers. Known as **DHCP Option 82**, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients. It is also an effective tool in preventing malicious network attacks from attached clients on DHCP services, such as IP Spoofing, Client Identifier Spoofing, MAC Address Spoofing, and Address Exhaustion.

The **DHCP option 82** enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options:

- Circuit ID (option 1)
- Remote ID (option2).

The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on.
The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The DHCP Rate Limit Setting and Config screens in Figure 4-9-23 & Figure 4-9-24 appear.
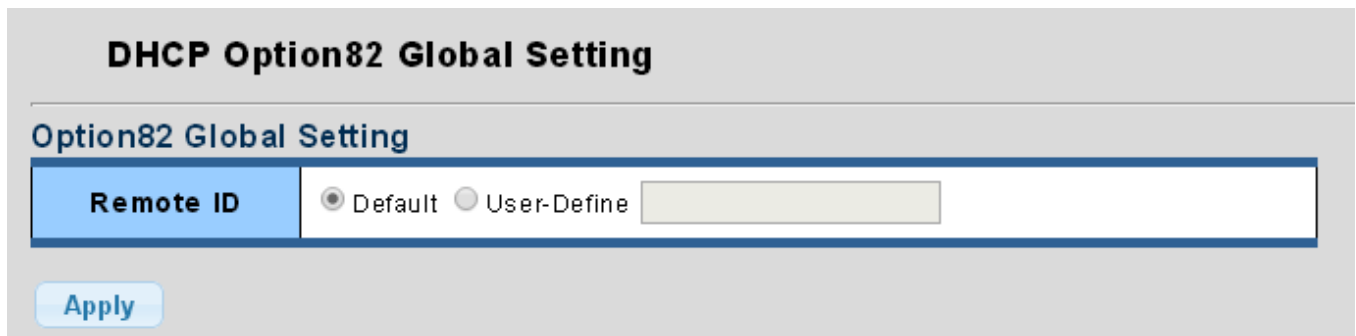
Figure 4-9-23: Option82 Global Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Remote ID**	Set the option2 (remote ID option) content of option 82 added by DHCP request packets. ■ **Default** means the default VLAN MAC format. ■ **User-Define** means the remote-id content of option 82 specified by users

Button

Apply : Click to apply changes.
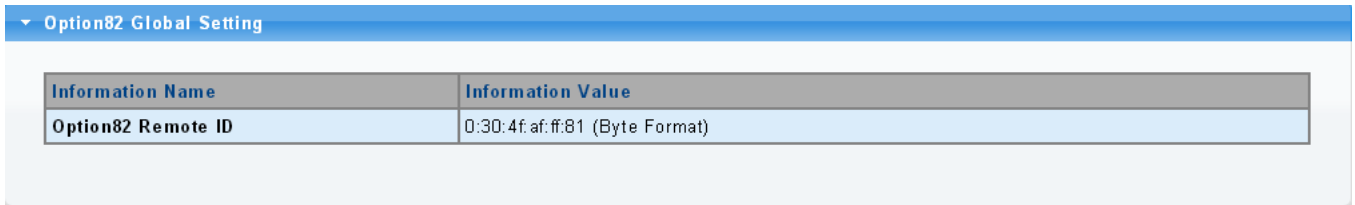
Figure 4-9-24: Option82 Global Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Option82 Remote ID**	Display the current option82 remite ID.

4.9.3.8 Option82 Port Setting

This function is used to set the retransmitting policy of the system for the received DHCP request message which contains option82. The **drop** mode means that if the message has option82, then the system will drop it without processing; **keep** mode means that the system will keep the original option82 segment in the message, and forward it to the server to process; **replace** mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process. Option82 Port Setting screens in Figure 4-9-25 & Figure 4-9-26 appear.
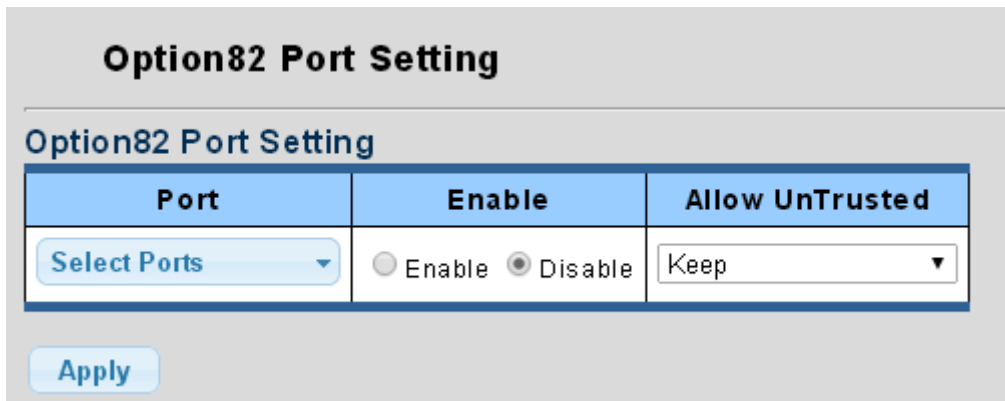
Figure 4-9-25: Option82 Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **Enable**	Enable or disable option82 function on port, default mode is Disable.
• **Allow UnTrusted**	Select modes for this drop down list. The following modes are available: ■ **Keep (Default mode)** ■ **Drop** ■ **Replace**

Button

Apply : Click to apply changes.

▾ **Option82 Port Setting**

Port	Enable	Allow UnTrusted
GE1	Disabled	Drop
GE2	Disabled	Drop
GE3	Disabled	Drop
GE4	Disabled	Drop
GE5	Disabled	Drop
GE6	Disabled	Drop
GE7	Disabled	Drop
GE8	Disabled	Drop
GE9	Disabled	Drop
GE10	Disabled	Drop
GE11	Disabled	Drop
GE12	Disabled	Drop
GE13	Disabled	Drop
GE14	Disabled	Drop
GE15	Disabled	Drop
GE16	Disabled	Drop
GE17	Disabled	Drop
GE18	Disabled	Drop
GE19	Disabled	Drop
GE20	Disabled	Drop
GE21	Disabled	Drop
GE22	Disabled	Drop
GE23	Disabled	Drop
GE24	Disabled	Drop
GE25	Disabled	Drop
GE26	Disabled	Drop
LAG1	Disabled	Drop
LAG2	Disabled	Drop
LAG3	Disabled	Drop
LAG4	Disabled	Drop
LAG5	Disabled	Drop
LAG6	Disabled	Drop
LAG7	Disabled	Drop
LAG8	Disabled	Drop

Figure 4-9-26: Option82 Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Enable**	Display the current status.
• **Allow UnTrusted**	Display the current untrusted mode.

4.9.3.9 Option82 Circuit-ID Setting

Set creation method for option82, users can define the parameters of circute-id suboption by themselves. Option82 Circuit-ID Setting screens in Figure 4-9-27 & Figure 4-9-28 appear.

Figure 4-9-27: Option82 Port Circuit-ID Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **VLAN**	Indicates the ID of this particular VLAN.
• **Circuit ID**	Set the option1 (Circuit ID) content of option 82 added by DHCP request packets.

Button

Apply : Click to apply changes.

Figure 4-9-28: Option82 Port Circuit-ID Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Display the current port.
• **VLAN**	Display the current VLAN.
• **Circuit ID**	Display the current circuit ID.

4.9.4 Port Security

This page allows you to configure the Port Security Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of four different as described below.

The Limit Control module is one of a range of modules that utilizes a lower-layer module, the Port Security module, which manages MAC addresses, learned on the port.

The Limit Control configuration consists of two sections, a system- and a port-wid. The IP Source Guard Static Binding Entry and Table Status screens in Figure 4-9-29 & Figure 4-9-30 appear.

Figure 4-9-29: Port Security Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **Security**	Enable or disable the port security.
• **Max L2 Entry**	The maximum number of MAC addresses that can be secured on this port. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
• **Action**	If Limit is reached, the switch can take one of the following actions: ■ **Forward**: Do not allow more than Limit MAC addresses on the port, but take no further action. ■ **Discard**: If Limit + 1 MAC addresses is seen on the port, it will trigger the action that do not learn the new MAC and drop the package. ■ **Discard/SNMP/Log**: If Limit + 1 MAC addresses is seen on the port, it will trigger the action that do not learn the new MAC and drop the package. Also appears under SNMP and System log.

■ **Discard/SNMP/Log/ 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 will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

1) Disable and re-enable Limit Control on the port or the switch,

2) Click the Reopen button.

Also appears under SNMP and System log.

• **Trap Frequency (sec.)**	Allow to input the seconds for trap frequency.

Button

Apply : Click to apply changes.

▼ **Port Security Status**

Port Name	Enable State	L2 Entry Num	Action	Trap Frequency
GE1	Disabled	16383	Forward	-
GE2	Disabled	16383	Forward	-
GE3	Disabled	16383	Forward	-
GE4	Disabled	16383	Forward	-
GE5	Disabled	16383	Forward	-
GE6	Disabled	16383	Forward	-
GE7	Disabled	16383	Forward	-
GE8	Disabled	16383	Forward	-
GE9	Disabled	16383	Forward	-
GE10	Disabled	16383	Forward	-
GE11	Disabled	16383	Forward	-
GE12	Disabled	16383	Forward	-
GE13	Disabled	16383	Forward	-
GE14	Disabled	16383	Forward	-
GE15	Disabled	16383	Forward	-
GE16	Disabled	16383	Forward	-
GE17	Disabled	16383	Forward	-
GE18	Disabled	16383	Forward	-
GE19	Disabled	16383	Forward	-
GE20	Disabled	16383	Forward	-
GE21	Disabled	16383	Forward	-
GE22	Disabled	16383	Forward	-
GE23	Disabled	16383	Forward	-
GE24	Disabled	16383	Forward	-
GE25	Disabled	16383	Forward	-
GE26	Disabled	16383	Forward	-
LAG1	Disabled	16383	Forward	-
LAG2	Disabled	16383	Forward	-
LAG3	Disabled	16383	Forward	-
LAG4	Disabled	16383	Forward	-
LAG5	Disabled	16383	Forward	-
LAG6	Disabled	16383	Forward	-
LAG7	Disabled	16383	Forward	-
LAG8	Disabled	16383	Forward	-

Figure 4-9-30: Port Security Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port Name**	The switch port number of the logical port.
• **Enable State**	Display the current per port security status.
• **L2 Entry Num**	Display the current L2 entry number.
• **Action**	Display the current aciotn.
• **Trap Frequency**	Display the current trap frequency.

Object	Description
• **Port Name**	The switch port number of the logical port.

4.9.5 AAA

Authentication, authorization, and accounting (AAA) provides a framework for configuring access control on the PoE Managed Switch. The three security functions can be summarized as follows:

- **Authentication** — Identifies users that request access to the network.
- **Authorization** — Determines if users can access specific services.
- **Accounting** — Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are then applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The PoE Managed Switch supports the following AAA features:

- Accounting for **IEEE 802.1X authenticated users** that access the network through the PoE Managed Switch.
- Accounting for users that access **management interfaces** on the PoE Managed Switch through the console and Telnet.
- Accounting for **commands** that users enter at specific CLI privilege levels. Authorization of users that access management interfaces on the PoE Managed Switch through the console and Telnet.

To configure AAA on the PoE Managed Switch, you need to follow this general process:

1.   Configure RADIUS and TACACS+ server access parameters. See "**Configuring Local/Remote Logon Authentication**".

2.   Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.

3.   Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use. Apply the method names to port or line interfaces.

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

4.9.5.1 Login List

This page is to login list parameters. The authentication list screen in Figure 4-9-31 & Figure 4-9-32 appears.

Login Authentication List

New Authentication List

List Name	Method 1	Method 2	Method 3	Method 4
	Empty ▼	Empty ▼	Empty ▼	Empty ▼

Add

Figure 4-9-31: New Authentication List Screenshot

The page includes the following fields:

Object	Description
• **List Name**	Defines a name for the authentication list, the available length is 31 characters.
• **Method 1-4**	Set the login authentication method: Empty / None / Local / TACACS+ / RADIUS / Enable Default mode is Empty.

Button

Add : Click to add authentication list.

Login Authentication Lists

List Name	Method List	Modify
Default	Local	Edit

Figure 4-9-32: Login Authentication List Screenshot

The page includes the following fields:

Object	Description
• **List Name**	Display the current list name.
• **Method List**	Display the current method list.
• **Modify**	Click Edit to edit login authentication list parameter. Click Delete to delete login authentication list entry.

223

4.9.5.2 Enable List

This page is to login list parameters. The authentication list screens in Figure 4-9-33 & Figure 4-9-34 appear.

Figure 4-9-33: New Authentication List Screenshot

The page includes the following fields:

Object	Description
• **List Name**	Defines a name for the authentication list, the available length is 31 characters.
• **Method 1-3**	Set the login authentication method: Empty / None / Enable / TACACS+ / RADIUS

Button

 : Click to add authentication list.

Figure 4-9-34: Login Authentication List Screenshot

The page includes the following fields:

Object	Description
• **List Name**	Display the current list name.
• **Method List**	Display the current method list.
• **Modify**	Click **Edit** to edit login authentication list parameter. Click **Delete** to delete login authentication list entry.

4.9.5.3 Accounting List

This page is to accounting list parameters. The authentication list screens in Figure 4-9-35 & Figure 4-9-36 appear.

Figure 4-9-35: New Accounting List Screenshot

The page includes the following fields:

Object	Description
• **List Name**	Defines a name for the accounting list, the available length is 31 characters.
• **Record Type**	Provide following record type: **Start-Stop (Default mode)** **Stop-Only**
• **Method 1-2**	Set the login accounting method: TACACS+ / RADIUS

Button

Add : Click to add accounting list.

Figure 4-9-36: Accounting List Screenshot

The page includes the following fields:

Object	Description
• **List Name**	Display the current list name.
• **Record Type**	Display the current record type.
• **Method List**	Display the current method list.

• **Modify**	Click **Edit** to edit login authentication list parameter. Click **Delete** to delete login authentication list entry.

4.9.5.4 Accounting Update

This page is to accounting update parameters. The authentication list screens in Figure 4-9-37 & Figure 4-9-38 appear.
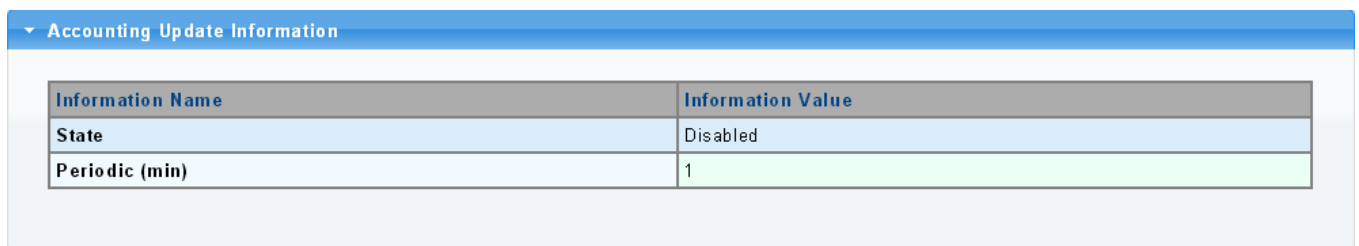
Figure 4-9-37: Accounting Update Screenshot

The page includes the following fields:

Object	Description
• **State**	Provide Disabled or Enabled this function.
• **Preamble & IFG**	Provide input the preamble & IFG value.

Button

Apply : Click to apply changes.

Figure 4-9-38: Accounting Update Screenshot

The page includes the following fields:

Object	Description
• **State**	Display the current state.
• **Periodic (mim)**	Display the current periodic value.

4.9.6 TACACS+ Server

This page is to configure the RADIUS server connection session parameters. The RADIUS Settings screens in Figure 4-9-39, Figure 4-9-40 & Figure 4-9-41 appear.

Figure 4-9-39: TACACS+ Server Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Key String**	The secret key - up to 128 characters long - shared between the TACACS+ server and the switch.
• **Timeout for Reply**	Retransmit is the number of times, in the range 1 to 30; a TACACS+ request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Button

Apply : Click to apply changes.

Figure 4-9-40: New TACACS+ Server Page Screenshot

The page includes the following fields:

Object	Description
• **Server Definition**	Set the server definition.
• **Server IP**	Address of the TACACS+ server IP/name.
• **Server Port**	Network (TCP) port of TACACS+ server used for authentication messages. (Range: 0-65535; Default: **49**)
• **Server Key**	The key- shared between the TACACS+ Authentication Server and the switch.
• **Server Timeout**	The number of seconds the switch waits for a reply from the server before it resends the request. (Range: 1-30 seconds)
• **Server Priority**	Set the server priority. (Range: 0-65535)

Button

[Add] : Click to add TACACS+ Server setting.
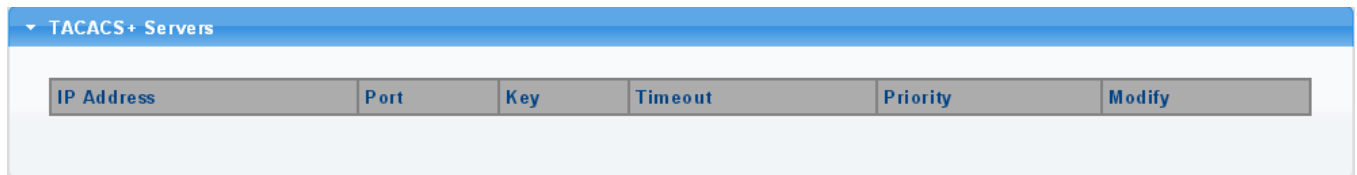
Figure 4-9-41: Login Authentication List Page Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	Display the current IP address.
• **Port**	Display the current port.
• **Key**	Display the current key.
• **Timeout**	Display the current timeout.
• **Priority**	Display the current priority
• **Modify**	Click [Edit] to edit login authentication list parameter. Click [Delete] to delete login authentication list entry.

4.9.7 RADIUS Server

This page is to configure the RADIUS server connection session parameters. The RADIUS Settings screens in Figure 4-9-42, Figure 4-9-43 & Figure 4-9-44 appears.

Radius Server Settings

Use Default Parameters

IP Version	Version 6 Version 4
Retries	3	(Range 1 - 10, Default: 3)
Timeout for Reply	3	sec. (Range 1 - 30, Default: 3)
Dead Time	0	min. (Range 0 - 2000, Default: 0)
Key String		(0/128 ASCII Alphanumeric Characters Used)

Apply

Figure 4-9-42: Radius Server Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Retries**	Timeout is the number of seconds, in the range 1 to 10, to wait for a reply from a RADIUS server before retransmitting the request. Default is 3.
• **Timeout for Reply**	Retransmit is the number of times, in the range 1 to 30, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead. Default is 3.
• **Dead Time**	The Dead Time, which can be set to a number between 0 and 2000 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. Default is 0.
• **Key String**	The secret key - up to 128 characters long - shared between the RADIUS server and the switch.

Button

Apply : Click to apply changes.

Figure 4-9-43: New Radius Server Page Screenshot

The page includes the following fields:

Object	Description
• **Server Definition**	Set the server definition.
• **Server IP**	Address of the Radius server IP/name.
• **Authetication Port**	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server. (Range: 0-65535)
• **Acct Port**	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server. (Range: 0-65535)
• **Key String**	The shared key - shared between the RADIUS Authentication Server and the switch.
• **Timeout for Reply**	The Timeout, which can be set to a number between 1 and 30 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to

	3 times before it is considered to be dead.
• **Retries**	Timeout is the number of seconds, in the range 1 to 10, to wait for a reply from a RADIUS server before retransmitting the request.
• **Server Priority**	Set the server priority. (Range: 0-65535)
• **Dead Time**	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. (Range: 0-2000)
• **Usage Type**	Set the usage type. The following modes are available: ■ **Login** ■ **802.1X** ■ **All**

Button

Add : Click to add Radius server setting.

Figure 4-9-44: Login Authentication List Page Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	Display the current IP address.
• **Auth Port**	Display the current auth port.
• **Acct Port**	Display the current acct port.
• **Key**	Display the current key.
• **Timeout**	Display the current timeout.
• **Retries**	Display the current retries times.
• **Priority**	Display the current priority.
• **Dead Time**	Display the current dead time
• **Usage Type**	Display the current usage type.
• **Modufy**	Click **Edit** to edit login authentication list parameter. Click **Delete** to delete login authentication list entry.

4.9.8 Access

This section is to control the access of the PoE Managed Switch, including the different access methods – Console, Telnet, HTTP and HTTPs.

4.9.8.1 Console

The Console Settings and Information screen in Figure 4-9-45 & Figure 4-9-46 appear.

Figure 4-9-45: Console Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Login Authentication List**	Select login authentication list for this drop down list.
• **Enable Authentication List**	Select enable authentication list for this drop down list.
• **EXEC Accounting List**	Select EXEC accounting list for this drop down list.
• **Session Timeout**	Set the session timeout value. Default is 10 and available range is 0-65535 minutes.
• **Password Retry Count**	Set the password retry count value. Default is 3 and available range is 0-120.
• **Silent Time**	Set the silent time value. Default is 0 and available range is 0-65535 seconds.

Button

Apply : Click to apply changes.

Console Information	
Information Name	**Information Value**
Login Authentication List	Default
Enable Authentication List	Default
EXEC Accounting List	Default
Session Timeout	10
Password Retry Count	3
Silent Time	0

Figure 4-9-46: Console Information Page Screenshot

The page includes the following fields:

Object	Description
• **Login Authentication List**	Display the current login authentication list information.
• **Enable Authentication List**	Display the current enable authentication list information.
• **EXEC Accounting List**	Display the EXEC accounting list information.
• **Session Timeout**	Display the current session timeout information.
• **Password Retry Count**	Displays the current password retry count information.
• **Silent Time**	Display the current silent time information.

4.9.8.2 Telnet

The Telnet Settings and Information screen in Figure 4-9-47 & Figure 4-9-48 appear.

Telnet Settings

Telnet Settings

Telnet Service	Disabled ▼
Login Authentication List	Default ▼
Enable Authentication List	Default ▼
EXEC Accounting List	Default ▼
Session Timeout	10 (0-65535) minutes
Password Retry Count	3 (0-120)
Silent Time	0 (0-65535) seconds

Apply   Disconnect

Figure 4-9-47: Telnet Settings Page Screenshot

The page includes the following fields:

Object	Description
• **Telnet Service**	Disable or enable telnet service.
• **Login Authentication List**	Select login authentication list for this drop down list.
• **Enable Authentication List**	Select enable authentication list for this drop down list.
• **EXEC Accounting List**	Select EXEC accounting list for this drop down list.
• **Session Timeout**	Set the session timeout value. Default is 10 and available range is 0-65535 minutes.
• **Password Retry Count**	Set the password retry count value. Default is 3 and available range is 0-120.
• **Silent Time**	Set the silent time value. Default is 0 and available range is 0-65535 seconds.

Button

Apply : Click to apply changes.

Disconnect : Click to disconnect telnet communication.

Information Name	Information Value
Telnet Service	Disabled
Login Authentication List	Default
Enable Authentication List	Default
EXEC Accounting List	Default
Session Timeout	10
Password Retry Count	3
Silent Time	0
Current Telnet Sessions Count	0

Figure 4-9-48: Telnet Information Page Screenshot

The page includes the following fields:

Object	Description
• **Telnet Service**	Display the current telent service information.
• **Login Authentication List**	Display the current login authentication list information.
• **Enable Authentication List**	Display the current enable authentication list information.
• **EXEC Accounting List**	Display the EXEC accounting list information.
• **Session Timeout**	Display the current session timeout information.
• **Password Retry Count**	Displays the current password retry count information.
• **Silent Time**	Display the current silent time information.
• **Current Telent Session Count**	Display the current telnet session count information.

4.9.8.3 HTTP

The HTTP Settings and Information screens in Figure 4-9-49 & Figure 4-9-50 appear.

Figure 4-9-49: HTTP Settings Page Screenshot

The page includes the following fields:

Object	Description
• **HTTP Service**	Disable or enable HTTP service. Default is Enabled.
• **Login Authentication List**	Select login authentication list for this drop down list.
• **Session Timeout**	Set the session timeout value. Default is 10 and available range is 0-86400 minutes.

Button

Apply : Click to apply changes.

Figure 4-9-50: HTTP Information Page Screenshot

The page includes the following fields:

Object	Description
• **HTTP Service**	Display the current HTTP service information.
• **Login Authentication List**	Display the current login authentication list information.
• **Session Timeout**	Display the current session timeout information.

4.9.8.4 HTTPs

The HTTPs Settings and Information screen in Figure 4-9-51 & Figure 4-9-52 appear.

Figure 4-9-51: HTTPs Settings Page Screenshot

The page includes the following fields:

Object	Description
• **HTTPs Service**	Disable or enable HTTPs service. Default is Disabled.
• **Login Authentication List**	Select login authentication list for this drop down list.
• **Session Timeout**	Set the session timeout value. Default is 10 and available range is 0-86400 minutes.

Button

 : Click to apply changes.

Figure 4-9-52: HTTPs Information Page Screenshot

The page includes the following fields:

Object	Description
• **HTTPs Service**	Display the current HTTPs service information.
• **Login Authentication List**	Display the current login authentication list information.
• **Session Timeout**	Display the current session timeout information.

4.10 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.

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.

The ACL page contains links to the following main topics:

■	**MAC-Based ACL**	Configuration MAC-based ACL setting
■	**MAC-Based ACE**	Add / Edit / Delete the MAC-based ACE (Access Control Entry) setting
■	**IPv4-Based ACL**	Configuration IPv4-based ACL setting
■	**IPv4-Based ACE**	Add / Edit / Delete the IPv4-based ACE (Access Control Entry) setting
■	**ACL Binding**	Configure the ACL parameters (ACE) of each switch port.

4.10.1 MAC-Based ACL

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. MAC-Based ACL screens in Figure 4-10-1 & Figure 4-10-2 appear.

Figure 4-10-1: MAC-Based ACL Page Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Create a named MAC-based ACL list.

Button

Add : Click to add MAC-Based ACL setting.
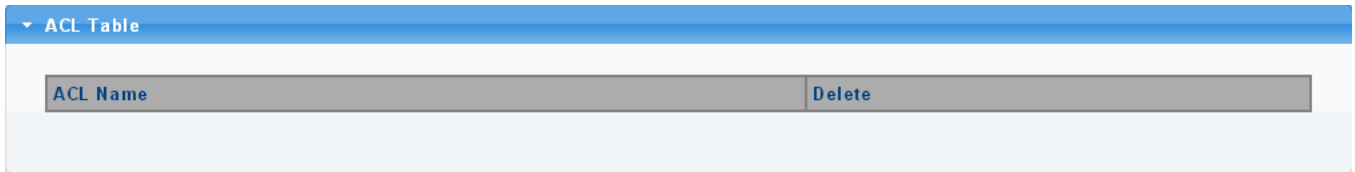
Figure 4-10-2: MAC-Based ACL Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Click **Delete** to delete ACL name entry.

4.10.2 MAC-Based ACE

An ACE consists of several parameters. Different parameter options are displayed depending on the frame type that you selected. The MAC-Based ACE screen in Figure 4-10-3 & Figure 4-10-4 appears.

Figure 4-10-3: MAC-Based ACE Page Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Select ACL name for this drop down list.
• **Sequence**	Set the ACL sequence.
• **Action**	Indicates the forwarding action of the ACE. ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped.
• **DA MAC**	Specify the destination MAC filter for this ACE. ■ **Any**: No DA MAC filter is specified. ■ **User Defined**: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DA MAC value appears.
• **DA MAC Value**	When "User Defined" is selected for the DA MAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DA MAC value.
• **DA MAC Mask**	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. ■ **0**: ARP frames where SHA is not equal to the DA MAC address. ■ **1**: ARP frames where SHA is equal to the DA MAC address.
• **SA MAC**	Specify the source MAC filter for this ACE. ■ **Any**: No SA MAC filter is specified. ■ **User Defined**: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering a SA MAC value appears.
• **SA MAC Value**	When "User Defined" is selected for the SA MAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SA MAC value.
• **SA MAC Mask**	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. ■ **0**: ARP frames where SHA is not equal to the SA MAC address. ■ **1**: ARP frames where SHA is equal to the SA MAC address.
• **VLAN ID**	Indicates the ID of this particular VLAN. The available range is 1-4094.
• **802.1p**	Include or exclude the 802.1p value.
• **802.1p Value**	Set the 802.1p value. The available range is 0-7.
• **802.1p Mask**	■ **0**: where frame is not equal to the 802.1p value. ■ **1**: where frame is equal to the 802.1p value.
• **Ethertype (Range:0x05DD – 0xFFFF)**	You can enter a specific EtherType value. The allowed range is **0x05DD** to **0xFFFF**. A frame that hits this ACE matches this EtherType value.

Button

Add : Click to add MAC-Based ACE setting.

Figure 4-10-4: MAC-Based ACE Table Page Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Display the current ACL name.
• **Sequence**	Display the current sequence.
• **Action**	Display the current action.
• **Destination MAC Address**	Display the current destination MAC address.
• **Destination Wildcard Mask**	Display the current destination wildcard mask.
• **Source MAC Address**	Display the current source MAC address.
• **Source Wildcard Mask**	Display the current source wildcard mask.
• **VLAN ID**	Display the current VLAN ID.
• **802.1p**	Display the current 802.1p value.
• **802.1p Mask**	Display the current 802.1p mask value.
• **Ethertype**	Display the current Ethernet type.
• **Modify**	Click Edit to edit MAC-Based ACE parameter. Click Delete to delete MAC-Based ACE entry.

4.10.3 IPv4-Based ACL

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. IPv4-Based ACL screens in Figure 4-10-5 & Figure 4-10-6 appear.

Figure 4-10-5: IPv4-Based ACL Page Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Create a named IPv4-based ACL list.

Button

Add : Click to add IPv4-Based ACL name list.
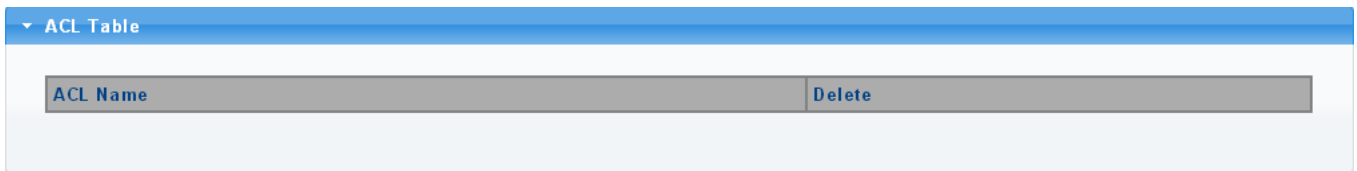
Figure 4-10-6: IPv4-Based ACL Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Click Delete to delete ACL name entry.

4.10.4 IPv4-Based ACE

An ACE consists of several parameters. Different parameter options are displayed depending on the frame type that you selected. The IPv4-Based ACE screens in Figure 4-10-7 & Figure 4-10-8 appear.

IPv4-Based ACE

IPv4-Based ACE	
ACL Name	▼
Sequence	____ (Range: 1 - 2147483647, 1 is first processed)
Action	● Permit ○ Deny
Protocol	● Any(IP) ○ Select from list icmp ▼ ○ Protocol ID to match 1
Source IP Address	● Any ○ User Defined
Source IP Address Value	____
Source IP Wildcard Mask	____ (0s for matching, 1s for no matching)
Destination IP Address	● Any ○ User Defined
Destination IP Address Value	____
Destination IP Wildcard Mask	____ (0s for matching, 1s for no matching)
Source Port	● Any ○ Single 0 (Range: 0 - 65535) ○ Range 0 - 65535 (Range: 0 - 65535)
Destination Port	● Any ○ Single(Range: 0 - 65535) 0 (Range: 0 - 65535) ○ Range(Range: 0 - 65535) 0 - 65535 (Range: 0 - 65535)
TCP Flags	Urg ● Set ○ Unset ○ Don't Care Ack ● Set ○ Unset ○ Don't Care Psh ● Set ○ Unset ○ Don't Care Rst ● Set ○ Unset ○ Don't Care Syn ● Set ○ Unset ○ Don't Care Fin ● Set ○ Unset ○ Don't Care
Type of Service	● Any ○ DSCP to match 0 (Range: 0 - 63) ○ IP Precedence to match 0 (Range: 0 - 7)
ICMP	● Any ○ Select from list Echo Re ▼ ○ Protocol ID to match 0 (Range: 0 - 255)
ICMP Code	● Any ○ User Defined 0 (Range: 0 - 255)

Add

Figure 4-10-7: IPv4-Based ACE Page Screenshot

243

The page includes the following fields:

Object	Description
• **ACL Name**	Select ACL name for this drop down list.
• **Sequence**	Set the ACL sequence.
• **Action**	Indicates the forwarding action of the ACE. ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped.
• **Protocol**	Specify the protocol filter for this ACE. ■ **Any(IP)**: No protocol filter is specified. ■ **Select from list**: If you want to filter a specific protocol with this ACE, choose this value and select protocol for this drop down list. ■ **Protocol ID to match**: I If you want to filter a specific protocol with this ACE, choose this value and set currect protocol ID.
• **Source IP Address**	Specify the Source IP address filter for this ACE. ■ **Any**: No source IP address filter is specified. ■ **User Defined**: If you want to filter a specific source IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• **Source IP Address Value**	When "User Defined" is selected for the source IP address filter, you can enter a specific source IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this source IP address value.
• **Source IP Wildcard Mask**	When "User Defined" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
• **Destination IP Address**	Specify the Destination IP address filter for this ACE. ■ **Any**: No destination IP address filter is specified. ■ **User Defined**: If you want to filter a specific destination IP address with this ACE, choose this value. A field for entering a source IP address value appears.
• **Destination IP Address Value**	When "User Defined" is selected for the destination IP address filter, you can enter a specific destination IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this destination IP address value.
• **Destination IP Wildcard Mask**	When "User Defined" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.
• **Source Port**	Specify the source port for this ACE. ■ **Any**: No specifc source port is specified (source port status is "don't-care"). ■ **Single**: If you want to filter a specific source port with this ACE, you can enter a specific source port value. A field for entering a source port value appears. The allowed range is `0` to `65535`. A frame that hits this ACE matches this source port value.

		■ **Range**: If you want to filter a specific source port range filter with this ACE, you can enter a specific source port range value. A field for entering a source port value appears. The allowed range is `0` to `65535`. A frame that hits this ACE matches this source port value.
• **Destination Port**		Specify the destination port for this ACE.
		■ **Any**: No specifc destination port is specified (destination port status is "don't-care").
		■ **Single**: If you want to filter a specific destination port with this ACE, you can enter a specific destiantino port value. A field for entering a destiantino port value appears. The allowed range is `0` to `65535`. A frame that hits this ACE matches this destination port value.
		■ **Range**: If you want to filter a specific destiantion port range filter with this ACE, you can enter a specific destiantion port range value. A field for entering a destination port value appears.
• **TCP Flags**	Urg	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.
		■ **Set**: TCP frames where the Urg field is set must be able to match this entry.
		■ **Unset**: TCP frames where the Urg field is set must not be able to match this entry.
		■ **Don't Care**: Any value is allowed ("don't-care").
	Ack	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.
		■ **Set**: TCP frames where the Ack field is set must be able to match this entry.
		■ **Unset**: TCP frames where the Ack field is set must not be able to match this entry.
		■ **Don't Care**: Any value is allowed ("don't-care").
	Psh	Specify the TCP "Push Function" (PSH) value for this ACE.
		■ **Set**: TCP frames where the Psh field is set must be able to match this entry.
		■ **Unset**: TCP frames where the Psh field is set must not be able to match this entry.
		■ **Don't Care**: Any value is allowed ("don't-care").
	Rst	■ Specify the TCP "Reset the connection" (RST) value for this ACE. **Set**: TCP frames where the Rst field is set must be able to match this entry.
		■ **Unset**: TCP frames where the Rst field is set must not be able to match this entry.
		■ **Don't Care**: Any value is allowed ("don't-care").

	Syn	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. ■ **Set**: TCP frames where the Syn field is set must be able to match this entry. ■ **Unset**: TCP frames where the Syn field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
	Fin	Specify the TCP "No more data from sender" (FIN) value for this ACE. ■ **Set**: TCP frames where the Fin field is set must be able to match this entry. ■ **Unset**: TCP frames where the Fin field is set must not be able to match this entry. ■ **Don't Care**: Any value is allowed ("don't-care").
● **Type of Service**		Specify the type pf service for this ACE. ■ **Any**: No specifc type of service is specified (destination port status is "don't-care"). ■ **DSCP to match**: If you want to filter a specific DSCP with this ACE, you can enter a specific DSCP value. A field for entering a DSCP value appears. The allowed range is `0` to `63`. A frame that hits this ACE matches this DSCP value. ■ **IP Recedence to match**: If you want to filter a specific IP recedence with this ACE, you can enter a specific IP recedence value. A field for entering an IP recedence value appears. The allowed range is `0` to `7`. A frame that hits this ACE matches this IP recedence value.
● **ICMP**		Specify the ICMP for this ACE. ■ **Any**: No specifc ICMP is specified (destination port status is "don't-care"). ■ **Select from List**: If you want to filter a specific list with this ACE, you can select a specific list value. ■ **Protocol ID to match**: If you want to filter a specific protocol ID filter with this ACE, you can enter a specific protocol ID value. A field for entering a protocol ID value appears. The allowed range is `0` to `255`. A frame that hits this ACE matches this protocol ID value.
● **ICMP Code**		Specify the ICMP code filter for this ACE. ■ **Any**: No ICMP code filter is specified (ICMP code filter status is "don't-care"). ■ **User Defined**: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. The allowed range is `0` to `255`. A frame that hits this ACE matches this ICMP code value.

Button

Add : Click to add IPv4-Based ACE list.
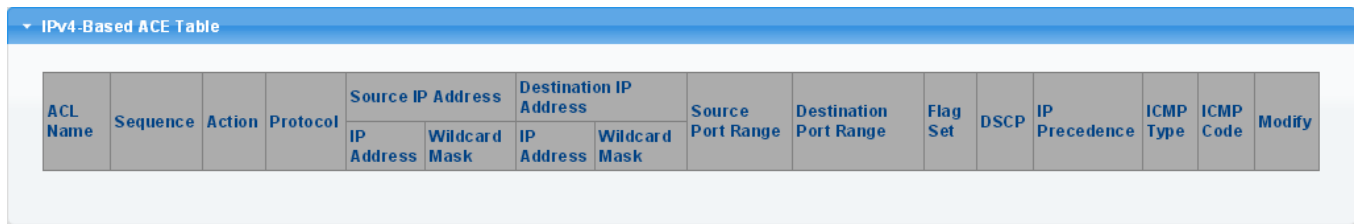
Figure 4-10-8: IPv4-Based ACE Table Page Screenshot

The page includes the following fields:

Object	Description
• **ACL Name**	Display the current ACL name.
• **Sequence**	Display the current sequence.
• **Action**	Display the current action.
• **Protocol**	Display the current protocol.
• **Source IP Address**	Display the current source IP address.
• **Source IP Address Wildcard Mask**	Display the current source IP address wildcard mask.
• **Destination IP Address**	Display the current destination IP address.
• **Destination IP Address Wildcard Mask**	Display the current destination IP address wildcard mask.
• **Source Port Range**	Display the current source port range.
• **Destiantion Port Range**	Display the current destination port range.
• **Flag Set**	Display the current flag set.
• **DSCP**	Display the current DSCP.
• **IP Precedence**	Display the current IP precedence.
• **ICMP Type**	Display the current ICMP Type.
• **ICMP Code**	Display the current ICMP code.
• **Modify**	Click **Edit** to edit IPv4-Based ACL parameter. Click **Delete** to delete IPv4-Based ACL entry.

4.10.5 ACL Binding

This page allows you to bind the Policy content to the appropriate ACLs. The ACL Policy screens in Figure 4-10-9 & Figure 4-10-10 appears.
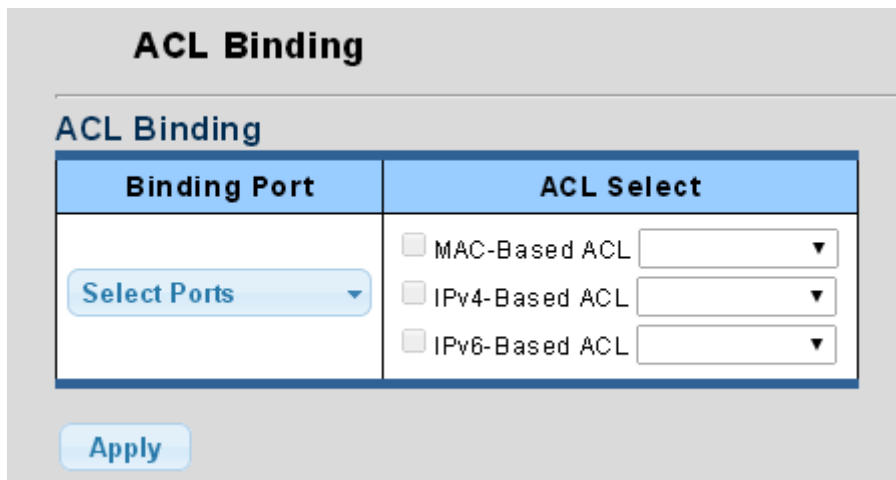
Figure 4-10-9: ACL Binding Page Screenshot

The page includes the following fields:

Object	Description
• **Binding Port**	Select port for this drop down list.
• **ACL Select**	Select ACL list for this drop down list.

Button

Apply : Click to apply changes.
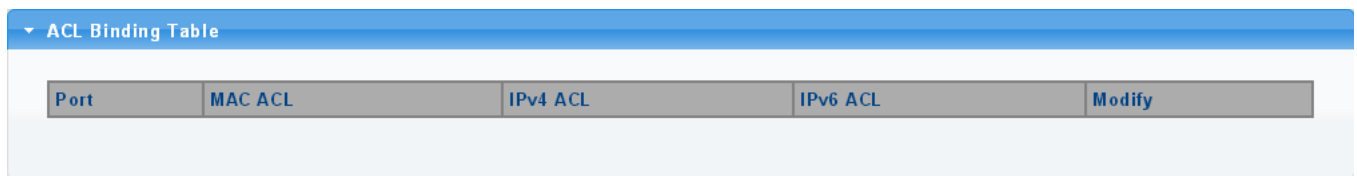
Figure 4-10-10: ACL Binding Table Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **MAC ACL**	Display the current MAC ACL
• **IPv4 ACL**	Display the current IPv4 ACL
• **IPv6 ACL**	Display the current IPv6 ACL
• **Modify**	Click Edit to edit ACL binding table parameter. Click Delete to delete ACL binding entry.

4.11 MAC Address Table

Switching of frames is based upon the DMAC address contained in the frame. The PoE Managed 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 frames with the corresponding SMAC address have been seen after a configurable age time.

4.11.1 Static MAC Setting

The static entries in the MAC table are shown in this table. The MAC table is sorted first by VLAN ID and then by MAC address. The Static MAC Setting screens in Figure 4-11-1 & Figure 4-11-2 appear.
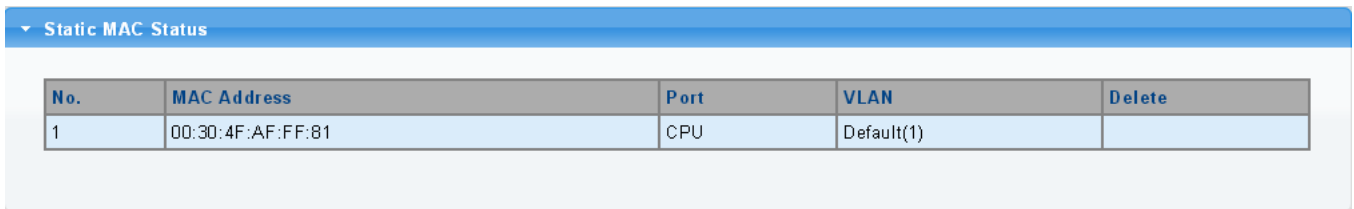
Figure 4-11-1: Static MAC Setting Page Screenshot

The page includes the following fields:

Object	Description
• **MAC Address**	Physical address associated with this interface.
• **Port**	Select port for this drop down list.
• **VLAN**	Select VLAN for this drop down list.

Button

 : Click to add new static MAC address.
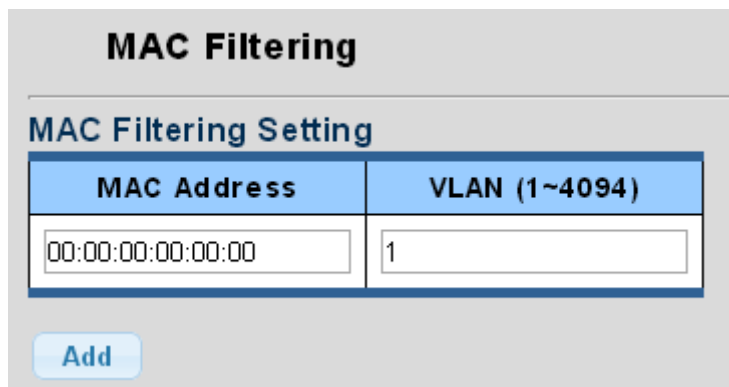
Figure 4-11-2: Static MAC Status Page Screenshot

The page includes the following fields:

Object	Description
• **No.**	This is the number for entries.
• **MAC Address**	The MAC address for the entry.
• **Port**	Display the current port.
• **VLAN**	The VLAN ID for the entry.
• **Delete**	Click **Delete** to delete static MAC status entry.

4.11.2 MAC Filtering

By filtering MAC address, the switch can easily filter the per-configured MAC address and reduce the un-safety. The Static MAC Setting screens in Figure 4-11-3 & Figure 4-11-4 appear.

Figure 4-11-3: MAC Filtering Setting Page Screenshot

The page includes the following fields:

Object	Description
• **MAC Address**	Physical address associated with this interface.
• **VLAN (1~4094)**	Indicates the ID of this particular VLAN.

Button

Add : Click to add new MAC filtering setting.
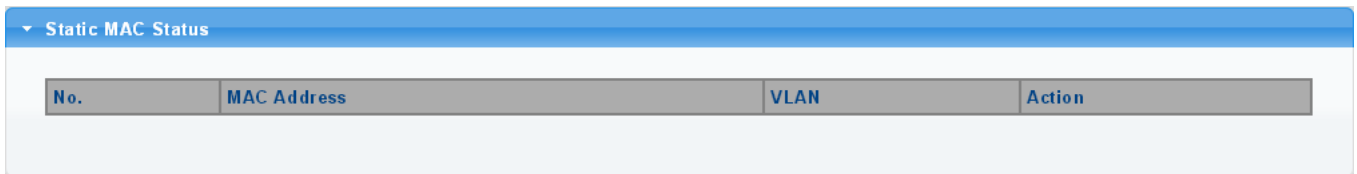
Figure 4-11-4: Statics MAC Status Page Screenshot

The page includes the following fields:

Object	Description
• **No.**	This is the number for entries
• **MAC Address**	The MAC address for the entry.
• **VLAN**	The VLAN ID for the entry.
• **Action**	Click **Delete** to delete static MAC status entry.

4.11.3 Dynamic Address Setting

By default, dynamic entries are removed from the MAC table after 300 seconds. The Dynamic Address Setting/Status screens in

Figure 4-11-5 & Figure 4-11-6 appear.
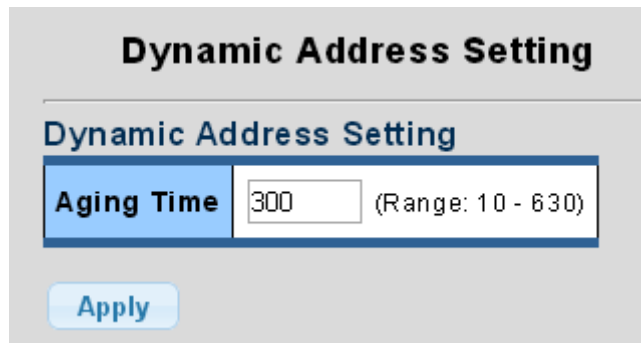
Figure 4-11-5: Dynamic Addresses Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Aging Time**	The time after which a learned entry is discarded.
	(Range: 10-630 seconds; Default: 300 seconds)

Button

Apply : Click to apply changes.

Figure 4-11-6: Dynamic Address Status Page Screenshot

The page includes the following fields:

Object	Description
• **Aging Time**	Display the current aging time setting information.

4.11.4 Dynamic Learned

Dynamic MAC Table

Dynamic Learned MAC Table are shown on this page. The MAC Table is sorted first by VLAN ID, then by MAC address. The Dynamic Learned screens in Figure 4-11-7 & Figure 4-11-8 appear.

Figure 4-11-7: Dynamic Learned Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **VLAN**	Select VLAN for this drop down list.
• **MAC Address**	Physical address associated with this interface.

Buttons

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

Clear : Flushes all dynamic entries.
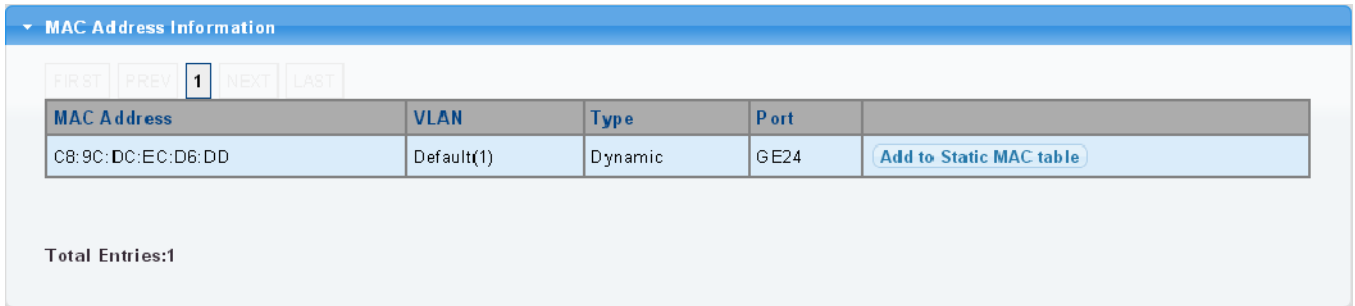
Figure 4-11-8: MAC Address Information Page Screenshot

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

Button

 : Click to add dynamic MAC address to static MAC address.

4.11.5 RMA Setting

Reserved MAC Addresses

Reserved MAC Addresses setting are shown on this page. This page provides **"Peer", "Bridge" and "Discard"** in Action mode for specific MAC address. The Reserved MAC Addresses setting screens in Figure 4-11-9 & Figure 4-11-10 appear.
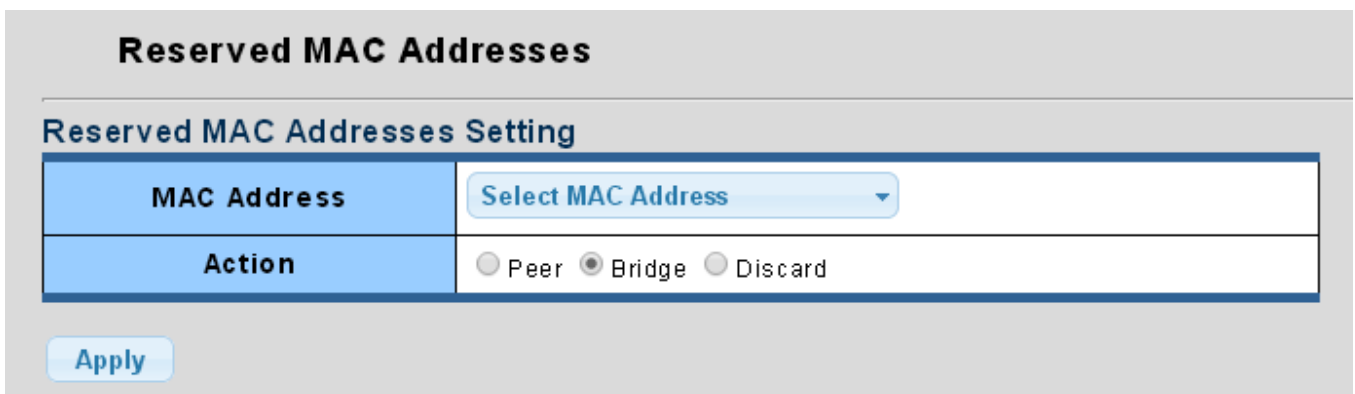
Figure 4-11-9: Reserved MAC Addresses Page Screenshot

The page includes the following fields:

Object	Description
• **MAC Address**	Select MAC Address from this drop down list.
• **Action**	Select **"Peer", "Bridge"** and **"Discard"** for specific MAC address.

Button

Apply : Click to apply changes.

Reserved MAC Addresses Config		
MAC Address	**Action**	**Delete**
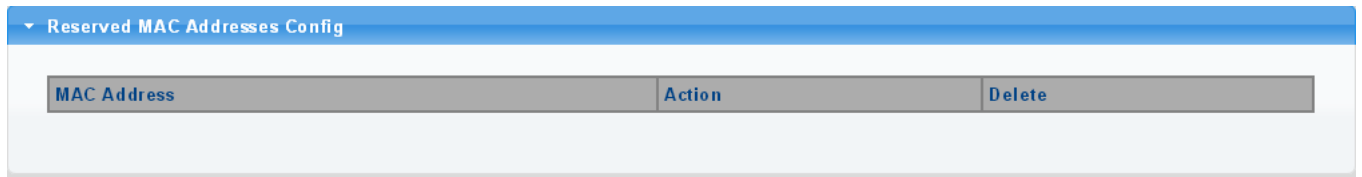
Figure 4-11-10: Reserved MAC Addresses StatusPage Screenshot

Object	Description
• **MAC Address**	The MAC address of the entry.
• **Action**	Display current Action mode.
• **Delete**	Click **Delete** to delete Reserved MAC Addresses status entry.

4.12 LLDP

4.12.1 Link Layer Discovery Protocol

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

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

4.12.2 LLDP Global Setting

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Global Setting and Config screens in Figure 4-12-1 & Figure 4-12-2 appear.

Figure 4-12-1: LLDP Global Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Enable**	Enable or disable LLDP globally function.
• **LLDP PDU Disable Action**	Set LLDP PDU disable action: include "Filtering", "Bridging" and "Flooding". ■ **Filtering**: discrad all LLDP PDU. ■ **Bridging**: transmit LLDP PDU in the same VLAN. ■ **Flooding**: transmit LLDP PDU for all port.
• **Transmission Interval**	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Transmission Interval** value. Valid values are restricted to 5 - 32768 seconds. Default: **30** seconds This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)
• **Holdtime Multiplier**	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Holdtime** multiplied by **Transmission Interval** seconds. Valid values are restricted to 2 - 10 times. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
• **Reinitialization Delay**	When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.
• **Transmit Delay**	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Transmit Delay** seconds. **Transmit Delay** cannot be larger than 1/4 of the **Transmission Interval** value. Valid values are restricted to 1 - 8192 seconds. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval
• **LLDP-MED Fast Start Repeat Count**	Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanisim. Range: 1-10 packets;

Default: **3** packets

The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

Button

Apply : Click to apply changes.

Config Name	Config Value
LLDP Enabled	Disabled
LLDP PDU Disable Action	Flooding
Transmission Interval	30 Secs
Holdtme Multiplier	4
Reinitialization Delay	2 Secs
Transmit Delay	2 Secs
LLDP-MED Fast Start Repeat Count	3 PDUs

Figure 4-12-2: LLDP Global Config Page Screenshot

The page includes the following fields:

Object	Description
• **LLDP Enable**	Display the current LLDP status.
• **LLDP PDU Disable Action**	Displays the current LLDP PDU disable action.
• **Transmission Interval**	Display the current transmission interval informaiton.
• **Holdtime Multiplier**	Display the current holdtime multiplier informaiton.
• **Reinitialization Delay**	Display the current reinitialization delay informaiton.
• **Transmit Delay**	Displays the current transmit delay informaiton.
• **LLDP-MED Fast Start Repeat Count**	Display the current LLDP-MED Fast Start Repeat Count informaiton.

4.12.3 LLDP Port Setting

Use the LLDP Port Setting to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received. The LLDP Port Configuration and Status screens in Figure 4-12-3 & Figure 4-12-4 appear.

Figure 4-12-3: LLDP Port Configuration and Optional TLVs Selection Page Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port for this drop down list.
• **State**	Enables LLDP messages transmit and receive modes for LLDP Protocol Data Units. Options: ■ **Disable (Default)** ■ **Rx ONLY** ■ **Tx ONLY** ■ **TX & RX**
• **Port Select**	Select port for this drop down list.
• **Optional TLV Select**	Configures the information included in the TLV field of advertised messages. ■ **System Name**: When checked the "System Name" is included in LLDP information transmitted. ■ **Port Description**: When checked the "Port Description" is included in LLDP information transmitted. ■ **System Description**: When checked the "System Description" is included in LLDP information transmitted.

- **System Capability**: When checked the "System Capability" is included in LLDP information transmitted.

- **802.3 MAC-PHY**: When checked the "802.3 MAC-PHY" is included in LLDP information transmitted.

- **802.3 Link Aggregation**: When checked the "802.3 Link Aggregation" is included in LLDP information transmitted.

- **802.3 Maximun Frame Size**: When checked the "802.3 Maximun Frame Size" is included in LLDP information transmitted.

- **802.1 PVID**: When checked the "802.1 PVID" is included in LLDP information transmitted.

Button

Apply : Click to apply changes.

LLDP Port Status

Port	State	Selected Optional TLVs
GE1	TX & RX	802.1 PVID
GE2	TX & RX	802.1 PVID
GE3	TX & RX	802.1 PVID
GE4	TX & RX	802.1 PVID
GE5	TX & RX	802.1 PVID
GE6	TX & RX	802.1 PVID
GE7	TX & RX	802.1 PVID
GE8	TX & RX	802.1 PVID
GE9	TX & RX	802.1 PVID
GE10	TX & RX	802.1 PVID
GE11	TX & RX	802.1 PVID
GE12	TX & RX	802.1 PVID
GE13	TX & RX	802.1 PVID
GE14	TX & RX	802.1 PVID
GE15	TX & RX	802.1 PVID
GE16	TX & RX	802.1 PVID
GE17	TX & RX	802.1 PVID
GE18	TX & RX	802.1 PVID
GE19	TX & RX	802.1 PVID
GE20	TX & RX	802.1 PVID
GE21	TX & RX	802.1 PVID
GE22	TX & RX	802.1 PVID
GE23	TX & RX	802.1 PVID
GE24	TX & RX	802.1 PVID
GE25	TX & RX	802.1 PVID
GE26	TX & RX	802.1 PVID

Figure 4-12-4 : LLDP Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **State**	Display the current LLDP status.
• **Selected Optional TLVs**	Display the current selected optional TLVs setting.

The VLAN Name TLV VLAN Selection and LLDP Port VLAN TLV Status screens in Figure 4-12-5 & Figure 4-12-6 appear.
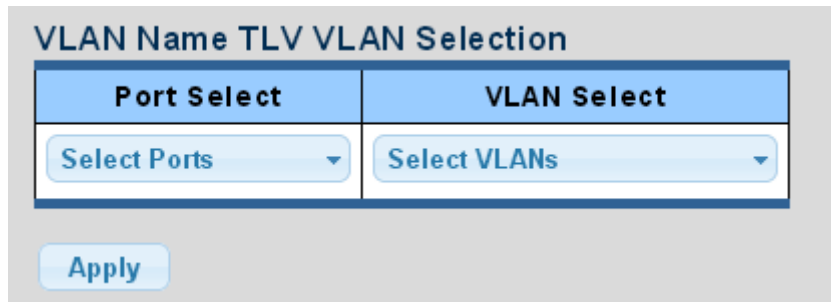
Figure 4-12-5: VLAN Name TLV VLAN Selection Page Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port from this drop down list.
• **VLAN Select**	Select VLAN from this drop down list.

Button

Apply : Click to apply changes.

▼ LLDP Port VLAN TLV Status

Port	Selected VLAN
GE1	
GE2	
GE3	
GE4	
GE5	
GE6	
GE7	
GE8	
GE9	
GE10	
GE11	
GE12	
GE13	
GE14	
GE15	
GE16	
GE17	
GE18	
GE19	
GE20	
GE21	
GE22	
GE23	
GE24	
GE25	
GE26	

Figure 4-12-6: LLDP Port VLAN TLV Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Selected VLAN**	Display the current selected VLAN.

4.12.4 LLDP Local Device

Use the LLDP Local Device Information screen to display information about the switch, such as its **MAC address**, **chassis ID**, **management IP address**, and **port information**. The Local Device Summary and Port Status screens in Figure 4-12-7 & Figure 4-12-8 appear.

LLDP Local Device

▼ Local Device Summary

Chassis ID Subtype	MAC Address
Chassis ID	00:30:4F:AF:FF:81
System Name	GS-4210-24P2S
System Description	V1
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

Figure 4-12-7: Local Device Summary Page Screenshot

The page includes the following fields:

Object	Description
• **Chassis ID Subtype**	Display the current chassis ID subtype.
• **Chassis ID**	Display the current chassis ID.
• **System Name**	Display the current system name.
• **System Description**	Display the current system description.
• **Capabilities Supported**	Display the current capabilities supported.
• **Capabilities Enabled**	Display the current capabilities enabled.
• **Port ID Subtype**	Display the current port ID subtype.

Figure 4-12-8: Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Interface**	The switch port number of the logical port.
• **LLDP Status**	Display the current LLDP status
• **LLDP MED Status**	Display the current LLDP MED Status

Detail: press the **"Detail"** button then the following detail LLDP Local Device Detail information appears. Press **"Back"** button for back to previous Port Status screen. The Global Information screens in Figure 4-12-9 appear.

Figure 4-12-9: Global Information Page Screenshot

The page includes the following fields:

Object	Description
• **Chassis ID Subtype**	Display current chassis ID Subtype information.
• **Chassis ID**	Display the current chassis ID information.
• **System Name**	Display the current system name.
• **System Description**	Display the current system description.
• **Supported System Capabilities**	Display the current supported system capabilities information.
• **Enabled System Capabilities**	Display the current enabled system capabilities information.
• **Port ID Subtype**	Display the current port ID Subtype information.
• **Port ID**	Display the current port ID information.
• **Port Description**	Display the current port description information.
• **Management Address**	Display the current management address information.

The MAC/PHY Details Information screens in Figure 4-12-10 appear.

MAC/PHY Details	
Auto-Negotiation Supported	N/A
Auto-Negotiation Enabled	N/A
Auto-Negotiation Advertised Capabilities	N/A
Operational MAU Type	N/A

Figure 4-12-10: MAC/PHY Details Information Page Screenshot

The page includes the following fields:

Object	Description
• **Auto-Negotiation Supported**	Display current auto-negotiation supported information.
• **Auto-Negotiation Enabled**	Display the current auto-negotiation enabled information.
• **Auto-Neogitaion Advertised Capailities**	Display the current auto-neogitaion advertised capailities information.
• **Operational MAU Type**	Display the current operational MAU type information.

The 802.3 Details Information screens in Figure 4-12-11 appear.

802.3 Details	
802.3 Maximum Frame Size	N/A

Figure 4-12-11: 802.3 Details Information Page Screenshot

The page includes the following fields:

Object	Description
• **802.3 Maximum Frame Size**	Display current 802.3 maximum frame size information.

The 802.3 Link Aggregation Information screens in Figure 4-12-12 appear.

802.3 Link Aggregation	
Aggregation Capability	N/A
Aggregation Status	N/A
Aggregation Port ID	N/A

Figure 4-12-12: 802.3 Link Aggregation Information Page Screenshot

The page includes the following fields:

Object	Description
• **Aggregation Capability**	Display current aggregation capability information.
• **Aggegation Status**	Display current aggregation status information.
• **Aggregation Port ID**	Display current aggregation port ID information.

The MED Details Information screens in Figure 4-12-13 appear.

MED Details	
Capabilities Supported	Capabilities, Network Policy
Current Capabilities	Capabilities, Network Policy
Device Class	Network Connectivity
PoE Device Type	N/A
PoE Power Source	N/A
PoE Power Priority	N/A
PoE Power Value	N/A
Hardware Revision	N/A
Firmware Revision	N/A
Software Revision	N/A
Serial Number	N/A
Manufacturer Name	N/A
Model Name	N/A
Asset ID	N/A

Figure 4-12-13: MED Details Information Page Screenshot

The page includes the following fields:

Object	Description
• **Capabilities Supported**	Display current capabilities supported information.
• **Current Capabilities**	Display current capabilities information.
• **Device Class**	Display current device class information.
• **PoE Device Type**	Display current PoE device type information.
• **PoE Power Source**	Display current PoE power source information.
• **PoE Power Priority**	Display current PoE power priority information.
• **PoE Power Value**	Display current PoE power value information.
• **Hardware Revision**	Display current hardware revision information.
• **Firmware Revision**	Display current firmware revision information.
• **Software Revision**	Display current software revision information.
• **Serial Number**	Display current serial number information.
• **Manufacturer Name**	Display current manufacturer name information.
• **Model Name**	Display current model name information.
• **Asset ID**	Display current asset ID information.

The 802.1 VLAN and Protocol Information screens in Figure 4-12-14 appear.

802.1 VLAN and Protocol	
PVID	N/A
VLAN Names	N/A

Figure 4-12-14: 802.1 VLAN and Protocol Information Page Screenshot

The page includes the following fields:

Object	Description
• **PVID**	Display current PVID information.
• **VLAN Names**	Display current VLAN Names information.

The Location Information screens in Figure 4-12-15 appear.

Location Information	
Civic	N/A
Coordinates	N/A
ECS ELIN	N/A

Figure 4-12-15: Location Information Page Screenshot

The page includes the following fields:

Object	Description
• **Civic**	Display current civic information.
• **Coordinates**	Display current coordinates information.
• **ECS ELIN**	Display current ECS ELIN information.

The Network Policy Table screens in Figure 4-12-16 appear.

Figure 4-12-16: Network Policy Table Page Screenshot

The page includes the following fields:

Object	Description
• **Application Type**	Display current application type information.
• **VLAN ID**	Display current VLAN ID information.
• **VLAN Type**	Display current VLAN Type information.
• **User Priority**	Display current user priority information.
• **DSCP**	Display current DSCP information.

4.12.5 LLDP Remote Device

This Page provides a status overview for all LLDP remive devices. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP Remive Device screen in Figure 4-12-17 appears.
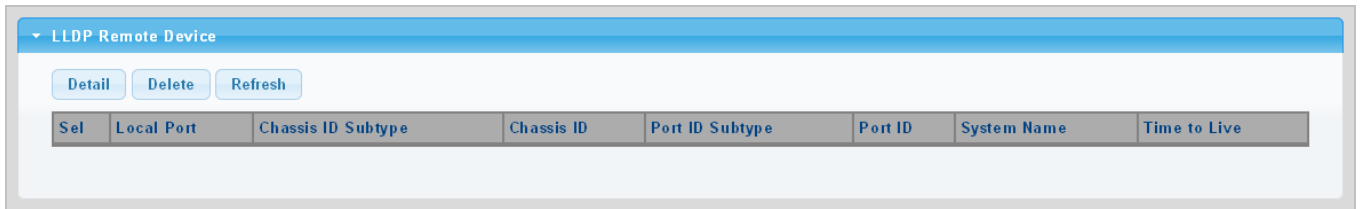
Figure 4-12-17: LLDP Remote Device Page Screenshot

The page includes the following fields:

Object	Description
• **Sel**	Disaply current sel information.
• **Local Port**	Display the current local port.
• **Chassis ID Subtype**	Display the current chassis ID subtype.
• **Chassis ID**	The Chassis ID is the identification of the neighbor's LLDP frames.
• **Port ID Subtype**	Display the current port ID subtype.
• **Port ID**	The Remote Port ID is the identification of the neighbor port.
• **System Name**	System Name is the name advertised by the neighbor unit.
• **Time to Live**	Display the current time to live.

Buttons

Delete : Click to delete LLDP remote device entry.

Refresh : Click to refresh LLDP remote device.

4.12.6 MED Network Policy

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

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

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)

2. Layer 2 priority value (IEEE 802.1D-2004)

3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

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

1. Voice

2. Guest Voice

3. Softphone Voice

4. Video Conferencing

5. Streaming Video

6. Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

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

The Voice Auto Mode Configuration, Network Policy Configuration and LLDP MED Network Policy Table screen in Figure 4-12-18 & Figure 4-12-19 appears.
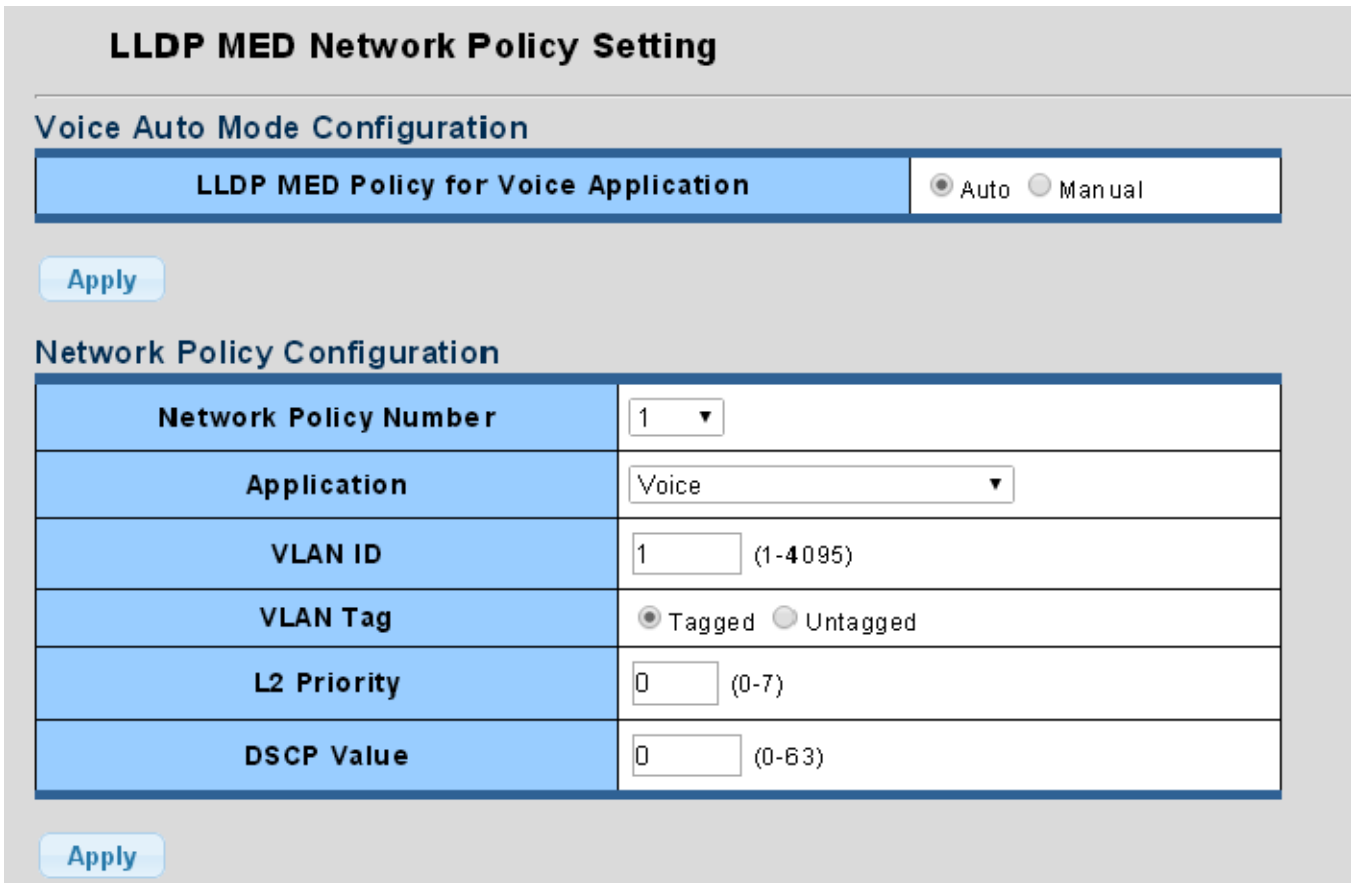
Figure 4-12-18: Voice Auto Mode Configuration and Network Policy Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **LLDP MED Policy for Voice Application**	Set the LLDP MED policy for voice application mode.　The options are shown as below: **Auto (Default)** **Manual**
• **Network Policy Number**	Select network policy number for this drop down list.
• **Application Type**	Intended use of the application types: **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. **Voice Signaling** - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar

	appliances supporting interactive voice services.
	Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
	Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
	Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
	App Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
	Video Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
• **VLAN ID**	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. The range is 1-4095.
• **VLAN Tag**	**Tagged** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003. **Untagged** indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.
• **L2 Priority**	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
• **DSCP Value**	DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Button

Apply : Click to apply changes.

Figure 4-12-19: LLDP MED Network Policy Table Page Screenshot

The page includes the following fields:

Object	Description
• **Network Policy Number**	Display the current network policy number.
• **Application**	Display the current application.
• **VLAN ID**	Display the current VLAN ID.
• **VLAN Tag**	Display the current VLAN tag status.
• **L2 Priority**	Display the current L2 priority.
• **DSCP Value**	Dusplay the current DSCP value.

Button

Delete : Click to delete LLDP MED network policy table entry.

4.12.7 MED Port Setting

The Port LLDP MED Configuration/Port Setting Table screens in Figure 4-12-20 & Figure 4-12-21 appear.

LLDP Port MED Setting

Port LLDP MED Configuration

Port Select	MED Enable	MED Optional TLVs	MED Network Policy
Select Ports ▼	Enable ▼	Select Optional TLVs ▼	Select Optional TLVs ▼

Apply

Figure 4-12-20: Port LLDP MED Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port for this drop down list.
• **MED Enable**	Enable or disable MED configuration.
• **MED Optional TVLs**	Configures the information included in the MED TLV field of advertised messages. **-Network Policy** – This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption. **-Location** – This option advertises location identification details. **-Inventory** – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.
• **MED Network Policy**	Select MED network policy for this drop down list.

Button

Apply : Click to apply changes.

▼ LLDP MED Port Setting Table

Interface	LLDP MED Status	User Defined Network Policy		Location	Inventory
		Active	Application		
GE1	Enabled	Yes		No	No
GE2	Enabled	Yes		No	No
GE3	Enabled	Yes		No	No
GE4	Enabled	Yes		No	No
GE5	Enabled	Yes		No	No
GE6	Enabled	Yes		No	No
GE7	Enabled	Yes		No	No
GE8	Enabled	Yes		No	No
GE9	Enabled	Yes		No	No
GE10	Enabled	Yes		No	No
GE11	Enabled	Yes		No	No
GE12	Enabled	Yes		No	No
GE13	Enabled	Yes		No	No
GE14	Enabled	Yes		No	No
GE15	Enabled	Yes		No	No
GE16	Enabled	Yes		No	No
GE17	Enabled	Yes		No	No
GE18	Enabled	Yes		No	No
GE19	Enabled	Yes		No	No
GE20	Enabled	Yes		No	No
GE21	Enabled	Yes		No	No
GE22	Enabled	Yes		No	No
GE23	Enabled	Yes		No	No
GE24	Enabled	Yes		No	No
GE25	Enabled	Yes		No	No
GE26	Enabled	Yes		No	No

Figure 4-12-21: LLDP MED Port Setting Table Page Screenshot

The page includes the following fields:

Object	Description
• **Interface**	The switch port number of the logical port.
• **LLDP MED Status**	Display the current LLDP MED status..
• **Active**	Display the current active status.
• **Application**	Display the current application.
• **Location**	Display the current location.
• **Inventory**	Display the current inventory.

The MED Location Configuration and LLDP MED Port Location Table screens in Figure 4-12-22 & Figure 4-12-23 appear.

MED Location Configuration

Ports	Select Ports ▼
Location Coordinate	_____ (16 pairs of hexadecimal characters)
Location Civic Address	_____ (6-160 pairs of hexadecimal characters)
Location ECS ELIN	_____ (10-25 pairs of hexadecimal characters)

Apply

Figure 4-12-22: MED Location Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Ports**	Select port for this drop down list.
• **Location Coordinate**	A string identifying the Location Coordinate that this entry should belong to.
• **Location Civic Address**	A string identifying the Location Civic Address that this entry should belong to.
• **Location ESC ELIN**	A string identifying the Location ESC ELIN that this entry should belong to.

Button

Apply : Click to apply changes.

Port	Coordinate	Civic Address	ECS ELIN
GE1			
GE2			
GE3			
GE4			
GE5			
GE6			
GE7			
GE8			
GE9			
GE10			
GE11			
GE12			
GE13			
GE14			
GE15			
GE16			
GE17			
GE18			
GE19			
GE20			
GE21			
GE22			
GE23			
GE24			
GE25			
GE26			

Figure 4-12-23: LLDP MED Port Location Table Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Coordinate**	Display the current coordinate.
• **Civic Address**	Display the current civic address.
• **ESC ELIN**	Display the current ESC ELIN.

4.12.8 LLDP Overloading

The LLDP Port Overloading screen in Figure 4-12-24 appears.

LLDP Port Overloading

▾ **LLDP Port Overloading Table**

Interface	Total(Bytes)	Left to Send(Bytes)	Status	Status								
				Mandatory TLVs	MED Capabilities	MED Location	MED Network Policy	MED Extended Power via MDI	802.3 TLVs	Optional TLVs	MED Inventory	802.1 TLVs
GE1	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE2	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE3	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE4	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE5	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE6	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE7	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE8	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE9	62	1426	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE10	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE11	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE12	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE13	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE14	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE15	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE16	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE17	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE18	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE19	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE20	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE21	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE22	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE23	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE24	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE25	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE26	63	1425	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)

Figure 4-12-24: LLDP Port Overloading Table Page Screenshot

The page includes the following fields:

Object	Description
• **Interface**	The switch port number of the logical port.
• **Toltal (Bytes)**	Total number of bytes of LLDP information that is normally sent in a packet.
• **Left to Send (Bytes)**	Total number of available bytes that can also send LLDP information in a packet.
• **Status**	Gives the status of the TLVs.
• **Mandatory TLVs**	Displays if the mandatory group of TLVs were transmitted or overloaded.
• **MED Capabilites**	Displays if the capabilities packets were transmitted or overloaded.
• **MED Location**	Displays if the location packets were transmitted or overloaded.
• **MED Network Policy**	Displays if the network policies packets were transmitted or overloaded.
• **MED Extended Power via MDI**	Displays if the extended power via MDI packets were transmitted or overloaded.
• **802.3 TLVs**	Displays if the 802.3 TLVs were transmitted or overloaded.
• **Optional TLVs**	If the LLDP MED extended power via MDI packets were sent, or if they were overloaded.
• **MED Inventory**	Displays if the mandatory group of TLVs was transmitted or overloaded.
• **802.1 TLVs**	Displays if the 802.1 TLVs were transmitted or overloaded.

4.12.9 LLDP Statistics

Use the LLDP Device Statistics screen to general statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces. The LLDP Global and Port Statistics screens in Figure 4-12-25 & Figure 4-12-26 appear.

Figure 4-12-25: LLDP Global Statistics Page Screenshot

The page includes the following fields:

Object	Description
• **Insertions**	Shows the number of new entries added since switch reboot.
• **Deletions**	Shows the number of new entries deleted since switch reboot.
• **Drops**	Shows the number of LLDP frames dropped due to that the entry table was full.
• **Age Outs**	Shows the number of entries deleted due to Time-To-Live expiring.

Buttons

Clear: Click to clear the statistics.

Refresh: Click to refresh the statistics.

LLDP Port Statistics

Port	TX Frames Total	RX Frames Total	Discarded	Errors	RX TLVs Discarded	Unrecognized	RX Ageouts Total
GE1	0	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0
GE9	0	0	0	0	0	0	0
GE10	0	0	0	0	0	0	0
GE11	0	0	0	0	0	0	0
GE12	0	0	0	0	0	0	0
GE13	0	0	0	0	0	0	0
GE14	0	0	0	0	0	0	0
GE15	0	0	0	0	0	0	0
GE16	0	0	0	0	0	0	0
GE17	0	0	0	0	0	0	0
GE18	0	0	0	0	0	0	0
GE19	0	0	0	0	0	0	0
GE20	0	0	0	0	0	0	0
GE21	0	0	0	0	0	0	0
GE22	0	0	0	0	0	0	0
GE23	0	0	0	0	0	0	0
GE24	0	0	0	0	0	0	0
GE25	0	0	0	0	0	0	0
GE26	0	0	0	0	0	0	0

Figure 4-12-26: LLDP Port Statistics Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port on which LLDP frames are received or transmitted.
• **TX Frame – Total**	The number of LLDP frames transmitted on the port.
• **RX Frame – Total**	The number of LLDP frames received on the port.
• **RX Frame – Discarded**	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
• **RX Frame – Errors**	The number of received LLDP frames containing some kind of error.
• **RX TLVs – Discarded**	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
• **RX TLVs – Unrecognized**	The number of well-formed TLVs, but with an unknown type value.
• **RX Ageout - Total**	The number of organizationally TLVs received.

4.13 Diagnostics

This section provides the system CPU / momory usage status and IP layer network diagnostics tool for troubleshoot. The diagnostic tool is designed for network manager to help them quickly diagnose problems between point to point and better service customers.

Use the Diagnastics menu items to display and configure basic administrative details of the PoE Managed Switch. Under System the following topics are provided to configure and view the system information:

This section has the following items:

- ■ **System Status**
- ■ **Ping Test**

4.13.1 System Status

The system status provides and display current system CPU and memory usage status. The system status screen in Figure 4-13-1 appears.
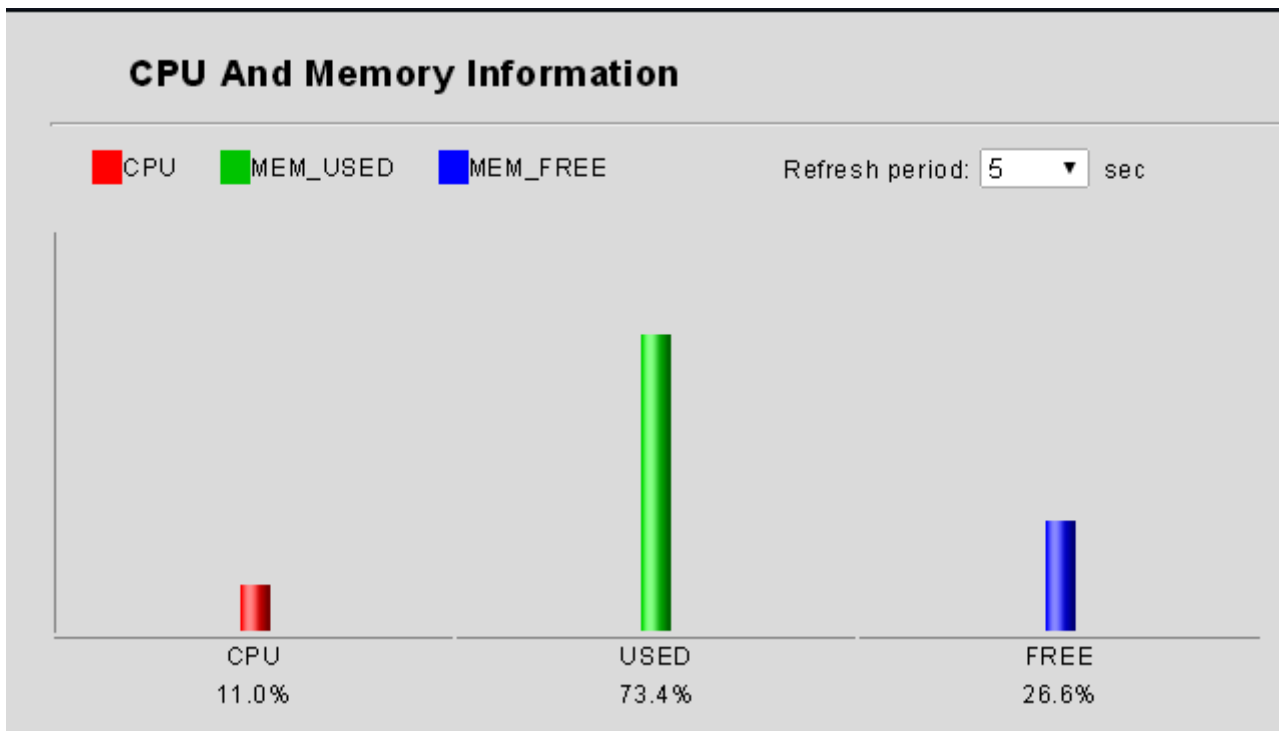
Figure 4-13-1: CPU and Memory Information Page Screenshot

The page includes the following fields:

Object	Description
• **CPU**	Display the current CPU usage status.
• **MEM_USED**	Display the current memory usage status.
• **MEM_FREE**	Display the current free memory status.
• **Refresh Period**	Provide 5 and 10 seconds for refresh period.

4.13.2 Ping Test

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues. After you press "**Apply**", ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-13-2 appears.

Figure 4-13-2: ICMP Ping Test Setting Page Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address.
• **Count**	Number of echo requests to send. The range is 1-5 and default is 4.
• **Interval (in sec)**	Send interval for each ICMP packet. The range is 1-5 and default is 1.
• **Size (in bytes)**	The payload size of the ICMP packet. Values range from 8bytes to 5120bytes.
• **Ping Results**	Display the current ping result.

Button

Apply : Click to transmit ICMP packets.
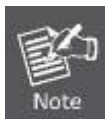
	Be sure the target IP Address is within the same network subnet of the PoE Managed Switch, or you have to set up the correct gateway IP address.

4.14 Power over Ethernet

Providing up to 24 PoE, in-line power interfaces, the GS-4210-24P2S PoE Managed Switch can easily build a power central-controlled IP phone system, IP Camera system, AP group for the enterprise. For instance, 24 camera / AP can be easily installed around the corner in the company for surveillance demands or build a wireless roaming environment in the office. Without the power-socket limitation, the GS-4210-24P2S PoE Managed Switch makes the installation of cameras or WLAN AP more easily and efficiently.

Use the PoE sub-menu items to configure the PoE function of the GS-4210-24P2S PoE Managed Switch. Under PoE sub-menu, the following topics are provided to configure and view the PoE Setting:

This section has the following items:

- ■ **PoE Global Setting**
- ■ **PoE Port Setting**
- ■ **PoE Delay Setting**

4.14.1 PoE Global Setting

This page allows adjusting the PoE budget and viewing PoE operation status and PoE chipset temperature. The PoE Global Setting screen in Figure 4-14-1 appears.

Figure 4-14-1: PoE Global Setting Page Screenshot

Button

 : Click to apply changes.

The page includes the following fields:

Object	Description
• **Maximum PoE Budget (watts)**	Allow assign PoE Budget to the PoE Managed Switch. The range is 0-300 watts and default is 300 watts.
• **Systsem Operation Status**	Display current system operation status.
• **Power Allocation**	Dislpay current power allocation value in watts.
• **PoE Temperature** • **Port 1 -8**	Display the current PoE chipset temperature of port 1-8.
• **PoE Temperature** • **Port 9 -16**	Display the current PoE chipset temperature of port 9-16.
• **PoE Temperature** • **Port 17 -24**	Display the current PoE chipset temperature of port 17-24.

4.14.2 PoE Port Setting

This page allows adjusting per port PoE budget and viewing per PoE port status. The PoE Port Setting screen in appears.
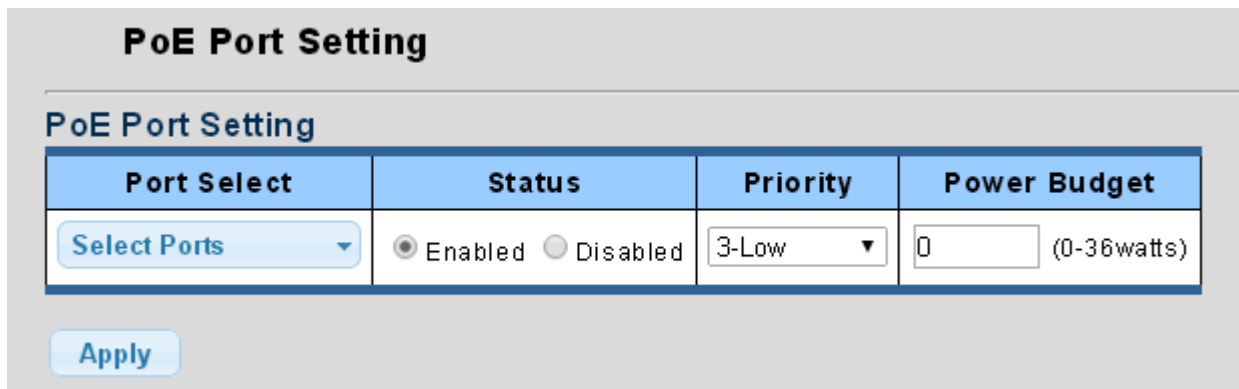
Figure 4-14-2: PoE Port Setting Page Screenshot

Button

Apply : Click to apply changes.

The page includes the following fields:

Object	Description
• **Port Select**	Select port from this drop down list.
• **Status**	Disable or enable per port PoE function.
• **Priority**	Select priority oprtions from this drop down list. The available options are: **3-Low (Default)** **2-High** **1-Critiical**
• **Power Budget**	Allow assign PoE Budget to per port of the PoE Managed Switch. The range is 0-36 watts.

▾ PoE Port Status

Port	Status	Class	Priority	Power Consumption(watts)	Power Budget(watts)
GE1	Disable	---	3	0.00	0
GE2	Disable	---	3	0.00	0
GE3	Disable	---	3	0.00	0
GE4	Disable	---	3	0.00	0
GE5	Disable	---	3	0.00	0
GE6	Disable	---	3	0.00	0
GE7	Disable	---	3	0.00	0
GE8	Disable	---	3	0.00	0
GE9	Disable	---	3	0.00	0
GE10	Disable	---	3	0.00	0
GE11	Disable	---	3	0.00	0
GE12	Disable	---	3	0.00	0
GE13	Disable	---	3	0.00	0
GE14	Disable	---	3	0.00	0
GE15	Disable	---	3	0.00	0
GE16	Disable	---	3	0.00	0
GE17	Disable	---	3	0.00	0
GE18	Disable	---	3	0.00	0
GE19	Disable	---	3	0.00	0
GE20	Disable	---	3	0.00	0
GE21	Disable	---	3	0.00	0
GE22	Disable	---	3	0.00	0
GE23	Disable	---	3	0.00	0
GE24	Disable	---	3	0.00	0

Figure 4-14-3: PoE Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Status**	Display per PoE port operation status.
• **Class**	Display per PoE port PD device class information.
• **Priority**	Display per PoE port priority information.
• **Power Consumption (watts)**	Display per PoE port power consumption information.
• **Power Budget (watts)**	Display per PoE port power budget information.

4.14.3 PoE Delay Setting

PoE delay is to delay power feeding when the switch is completely booted up

This page allows adjusting per port PoE delay time and viewing per PoE port status. The PoE Delay Setting screen in Figure 4-14-4 appears.
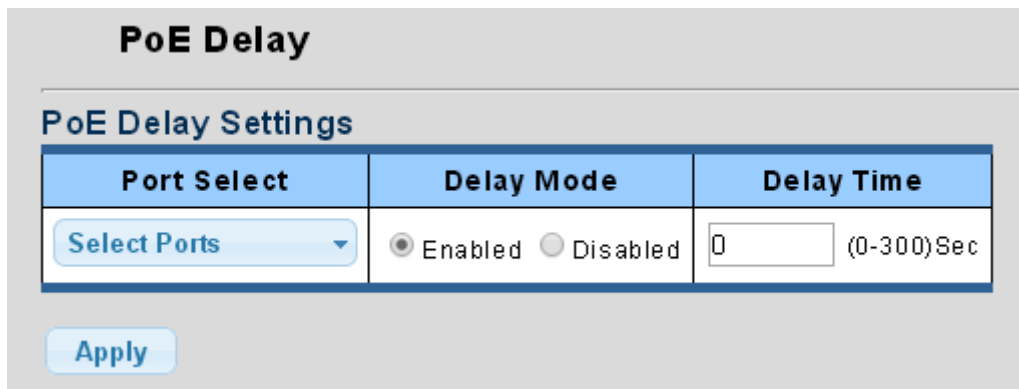
Figure 4-14-4: PoE Delay Setting Page Screenshot

Button

Apply : Click to apply changes.

The page includes the following fields:

Object	Description
• **Port Select**	Select port from this drop down list.
• **Delay Mode**	Disable or enable delay mode.
• **Delay Time**	Allow assign delay time to the PoE Managed Switch. The range is 0-300 seconds.

▼ POE Delay Status

Port	Delay Mode	Delay Time(Second)
GE1	Disable	0
GE2	Disable	0
GE3	Disable	0
GE4	Disable	0
GE5	Disable	0
GE6	Disable	0
GE7	Disable	0
GE8	Disable	0
GE9	Disable	0
GE10	Disable	0
GE11	Disable	0
GE12	Disable	0
GE13	Disable	0
GE14	Disable	0
GE15	Disable	0
GE16	Disable	0
GE17	Disable	0
GE18	Disable	0
GE19	Disable	0
GE20	Disable	0
GE21	Disable	0
GE22	Disable	0
GE23	Disable	0
GE24	Disable	0

Figure 4-14-5: PoE Delay Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Delay Mode**	Display per port delay mode status.
• **Delay Time (Second)**	Display per port delay time setting information.

288

4.14.4 Power over Ethernet Powered Device

3~5 Watts	**Voice over IP phones** Enterprise can install POE VoIP Phone, ATA and other Ethernet/non-Ethernet end-devices to the central where UPS is installed for un-interrupt power system and power control system.
6~12 Watts	**Wireless LAN Access Points** Museum, Sightseeing, Airport, Hotel, Campus, Factory, Warehouse can install the Access Point any where with no hesitation.
10~12 Watts	**IP Surveillance** Enterprise, Museum, Campus, Hospital, Bank, can install IP Camera without limits of install location – no need electrician to install AC sockets.
3~12 Watts	**PoE Splitter** PoE Splitter split the PoE 52V DC over the Ethernet cable into 5/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.
3~25 Watts	**High Power PoE Splitter** High PoE Splitter split the PoE 52V DC over the Ethernet cable into 24/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.
30 Watts	**High Power Speed Dome** This state-of-the-art design is considerable to fit in various network environments like traffic centers, shopping malls, railway stations, warehouses, airports, and production facilities for the most demanding outdoor surveillance applications- no need electrician to install AC sockets.

Note	**Since the GS-4210-24P2S PoE Managed Switch per PoE port supports 52V DC PoE power output, please check and assure the Powered Device's (PD) acceptable DC power range is from 52V DC; otherwise, it will damage the Powered Device (PD).**

4.15 RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9:

- ■ **Statistics:** Maintain basic usage and error statistics for each subnet monitored by the Agent.
- ■ **History:** Record periodical statistic samples available from Statistics.
- ■ **Alarm:** Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.
- ■ **Event:** A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

4.15.1 RMON Statistics

This Page provides a Detail of a specific RMON statistics entry; RMON Statistics screen in Figure 4-15-1 appears.

Figure 4-15-1: RMON Statistics Page Screenshot

The Page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **etherStatsDropEvents**	The total number of events in which packets were dropped by the probe due to lack of resources.
• **etherStatsOctets**	The total number of octets of data (including those in bad packets) received on the network.
• **etherStatsPkts**	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• **etherStatsBroadcastPkts**	The total number of good packets received that were directed to the broadcast address.
• **etherStatsMulticastPkts**	The total number of good packets received that were directed to a multicast address.
• **etherStatsCRCAlignErrors**	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.
• **etherStatsUnderSizePkts**	The total number of packets received that were less than 64 octets.
• **etherStatsOverSizePkts**	The total number of packets received that were longer than 1518 octets.
• **etherStatsFragments**	The number of frames which size is less than 64 octets received with invalid CRC.
• **etherStatsJabbers**	The number of frames which size is larger than 64 octets received with invalid CRC.
• **etherStatsCollisions**	The best estimate of the total number of collisions on this Ethernet segment.
• **etherStatsPkts64Octets**	The total number of packets (including bad packets) received that were 64 octets in length.
• **etherStatsPkts65to127Octets**	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
• **etherStatsPkts128to255Octets**	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
• **etherStatsPkts256to511Octets**	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
• **etherStatsPkts512to1023Octets**	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
• **etherStatsPkts1024to1518Octets**	The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length.

Buttons

Clear : Click to clear the RMON statistics.

4.15.2 RMON Event

Configure RMON Event table on this Page. The RMON Event screens in Figure 4-15-2 & Figure 4-15-3 appear.

Figure 4-15-2: RMON Event Settings Page Screenshot

The Page includes the following fields:

Object	Description
• **Select Index**	Select index for this drop down list to create new index or modify index.
• **Index**	Indicates the index of the entry. The range is from 1 to 65535.
• **Type**	Indicates the notification of the event, the possible types are: ■ **None**: The total number of octets received on the interface, including framing characters. ■ **Log**: The number of uni-cast packets delivered to a higher-layer protocol. ■ **SNMP-Trap**: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ■ **Log and Trap**: The number of inbound packets that are discarded even the packets are normal.
• **Community**	Specify the community when trap is sent, default is **"public"**.
• **Owner**	Indicates the owner of this event, the string length is from 0 to 31, default is a null string.

• **Description**	Indicates description of this event, the string length is from 0 to 127, default is a null string.

Button

Apply : Click to apply changes.

Figure 4-15-3: RMON Event Status Page Screenshot

The Page includes the following fields:

Object	Description
• **Index**	Display the current event index.
• **Event Type**	Display the current event type.
• **Community**	Display the current community for SNMP trap.
• **Description**	Display the current event description.
• **Last Sent Time**	Display the current last sent time.
• **Owner**	Display the current event owner.
• **Action**	Click **Delete** to delete RMON event entry.

4.15.3 RMON Event Log

This Page provides an overview of RMON Event Log. The RMON Event Log Table screen in Figure 4-15-4 appears.
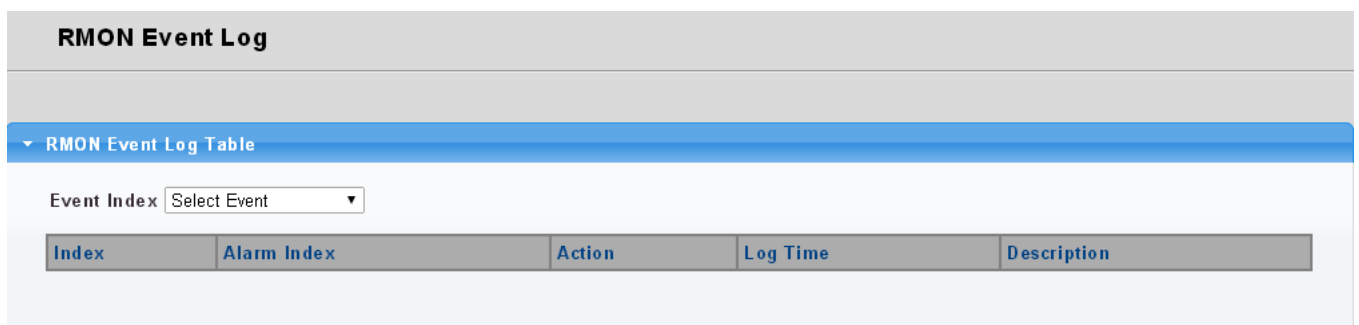
Figure 4-15-4: RMON Event Log Table Page Screenshot

The Page includes the following fields:

Object	Description
• **Select Index**	Select index from this drop down list.
• **Index**	Indicates the index of the log entry.
• **Alarm Index**	Indicates the alarm index of the log entry.
• **Action**	Indicates the action of the log entry.
• **Log Time**	Indicates Event log time.
• **Description**	Indicates the Event description.

4.15.4 RMON Alarm

Configure RMON Alarm setting on this Page. The RMON Alarm screens in Figure 4-15-5 & Figure 4-15-6 appear.

Figure 4-15-5: RMON Alarm Setting Page Screenshot

The Page includes the following fields:

Object	Description
• **Select Index**	Select index for this drop down list to create the new index or modify the index.
• **Index**	Indicates the index of the alarm entry. The range is 1-65535.
• **Sample Port**	Select port from this drop down list.
• **Sample Variable**	Indicates the particular variable to be sampled, the possible variables are: ■ **DropEvents**: The total number of events in which packets were dropped due to lack of resources. ■ **Octets**: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits. ■ **Pkts**: The total number of frames (bad, broadcast and multicast) received and transmitted. ■ **BroadcastPkts**: The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets. ■ **MulticastPkts**: The total number of good frames received that were directed to this multicast address. ■ **CRCAlignErrors**: The number of CRC/alignment errors (FCS or alignment errors). ■ **UnderSizePkts**: The total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **OverSizePkts**: The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed. ■ **Fragments**: The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error. ■ **Jabbers**: The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets), and had either an FCS or alignment error. ■ **Collisions**: The best estimate of the total number of collisions on this Ethernet segment. ■ **Pkts64Octets**: The total number of frames (including bad packets) received andtransmitted that were 64 octets in length (excluding framing bits but including FCS octets). ■ **Pkts65to127Octets**: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified

	range (excluding framing bits but including FCS octets).
	■ **Pkts128to255Octets**: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
	■ **Pkts256to511Octets**: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
	■ **Pkts512to1023Octets**: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
	■ **Pkts1024to1518Octets**: The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
• **Sample Interval**	Sample interval (1–2147483647)
• **Sample Type**	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: ■ **Absolute**: Get the sample directly (default). ■ **Delta**: Calculate the difference between samples.
• **Rising Threshold**	Rising threshold value (0–2147483647).
• **Falling Threshold**	Falling threshold value (0–2147483647).
• **Rising Event**	Event to fire when the rising threshold is crossed.
• **Falling Event**	Event to fire when the falling threshold is crossed.
• **Owner**	Specify an owner for the alarm.

Button

Apply : Click to apply changes.

▼ RMON Alarm										
Index	Sample Port	Sample Variable	Sample Interval	Sample Type	Rising Threshold	Falling Threshold	Rising Event	Falling Event	Owner	Action

Figure 4-15-6: RMON Alarm Status Page Screenshot

The Page includes the following fields:

Object	Description
• **Index**	Indicates the index of Alarm control entry.
• **Sample Port**	Display the current sample port.
• **Sample Variable**	Display the current sample variable.
• **Sample Interval**	Display the current interval.
• **Sample Type**	Display the current sample type.
• **Rising Threshold**	Display the current rising threshold.
• **Falling Threshold**	Display the current falling threshold.
• **Rising Event**	Display the current rising event.
• **Falling Event**	Display the current falling event.
• **Owner**	Display the current owner.
• **Action**	Click **Delete** to delete RMON alarm entry.

4.15.5 RMON History

Configure RMON History table on this Page. The RMON History screens in Figure 4-15-7 & Figure 4-15-8 appear.

Figure 4-15-7: RMON History Table Page Screenshot

The Page includes the following fields:

Object	Description
• **Select Index**	Select index for this drop down list to create the new index or modify the index
• **Index**	Indicates the index of the history entry. The range is 1-65535.
• **Sample Port**	Select port from this drop down list
• **Bucket Requested**	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 65535, default value is 50.
• **Interval**	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
• **Owner**	Specify an owner for the history. The range is 1-31 charactors.

Button

Apply : Click to apply changes.
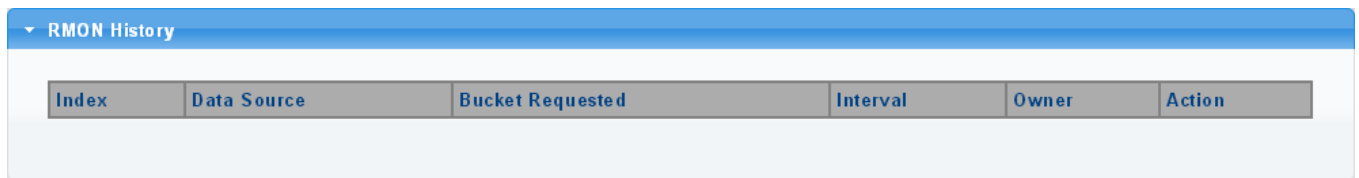
Figure 4-15-8: RMON History Status Page Screenshot

The Page includes the following fields:

Object	Description
• **Index**	Display the current index.
• **Data Source**	Display the current data source.
• **Bucket Requested**	Display the current bucket requested.
• **Interval**	Display the current interval.
• **Owner**	Display the current owner.
• **Action**	Click **Delete** to delete RMON history entry.

4.15.6 RMON History Log

This Page provides a detail of RMON history entries; screen in Figure 4-15-9 appears.

Figure 4-15-9: RMON History Status Page Screenshot

The Page includes the following fields:

Object	Description
• **History Index**	Select history index from this drop down list

4.16 Maintenance

Use the Maintenance menu items to display and configure basic configurations of the PoE Managed Switch. Under maintenance the following topics are provided to back up, upgrade, save and restore the configuration. This section has the following items:

■ **Factory Default**   You can reset the configuration of the switch on this page.

■ **Reboot Switch**   You can restart the switch on this page. After restart, the switch will boot normally.

■ **Backup Manager**   You can back up the switch configuration.

■ **Upgrade Manager**   You can upgrade the switch configuration.

4.16.1 Factory Default

You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in Figure 4-16-1 appears and clicks to reset the configuration to Factory Defaults.

Figure 4-16-1: Factory Default Page Screenshot

After the "**Factory**" button is pressed and rebooted, the system will load the default IP settings as follows:

◦ Default IP address: **192.168.0.100**

◦ Subnet mask: **255.255.255.0**

◦ Default Gateway: **192.168.0.254**

◦ The other setting value is back to disable or none.

> To reset the PoE Managed Switch to the Factory default setting, you can also press the hardware reset button on the front panel for about 10 seconds. After the device is rebooted, uou can login the management WEB interface within the same subnet of 192.168.0.xx.
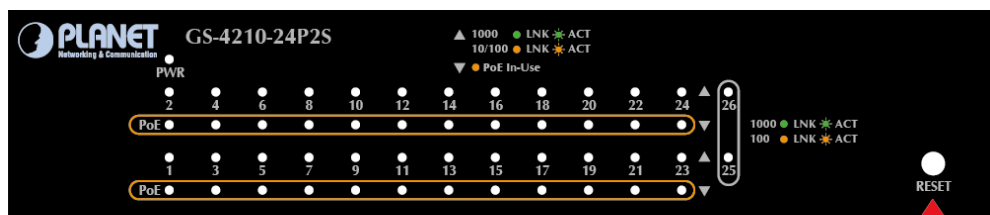
Hardware Reset button

4.16.2 Reboot Switch

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user has to re-login the WEB interface about 60 seconds later. The Reboot Switch screen in Figure 4-16-2 appears and clicks to reboot the system.

Reboot Switch

Reboot

Figure 4-16-2: Reboot Switch Page Screenshot

4.16.3 Backup Manager

This function allows backup of the current image or configuration of the PoE Managed Switch to the local management station. The Backup Manager screen in Figure 4-16-3 appears.

Backup Manager

Backup Manager

Backup Method	TFTP ▼
Server IP	
Backup Type	◉ Image ◯ Startup configuration ◯ Backup configuration ◯ Flah log ◯ Buffer log
Image	◉ FW-GS-4210-24P2S_v1.0b140611.bix (Active) ◯ FW-GS-4210-24P2S_v1.0b140611.bix (Backup)
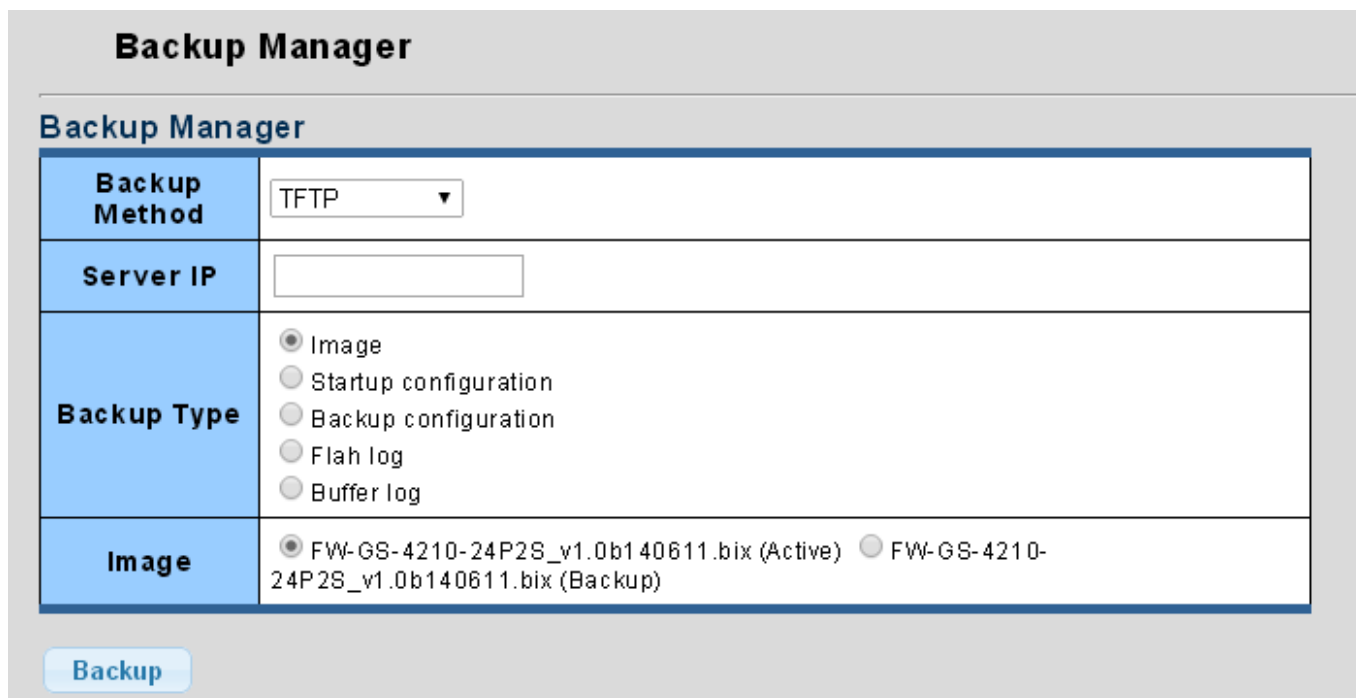
Backup

Figure 4-16-3: Backup Manager Page Screenshot

The page includes the following fields:

Object	Description
• **Backup Method**	Select backup method from this drop down list. The optios are TFTP and HTTP.
• **Server IP**	Fill in your TFTP server IP address.
• **Backup Type**	Select backup type.
• **Image**	Select active or backup image.

Button

 : Click to backup image, configuration or log.

4.16.4 Upgrade Manager

This function allows reload the current image or configuration of the PoE Managed Switch to the local management station. The

Upgrade Manager screen in Figure 4-16-4 appears.

Figure 4-16-4: Upgrade Manager Page Screenshot

The page includes the following fields:

Object	Description
• **Upgrade Method**	Select upgrade method from this drop down list. The optios are TFTP and HTTP.
• **Server IP**	Fill in your TFTP server IP address.
• **File Name**	The name of firmware image or configuration.
• **Upgrade Type**	Select upgrade type.
• **Image**	Select active or backup image.

Button

 : Click to upgrade image or configuration.

4.16.5 Configuation Manager

In the PoE Managed Switch, the running configuration file stores in the RAM. In the current version, the running configuration sequence of running-config can be saved from the RAM to FLASH by click **"SAVE"** then "**Save Configurations to FLASH**" function, so that the running configuration sequence becomes the startup configuration file, which is called configuration save. This page also provides to save all applied changes and set the current configuration as a startup configuration or backup configuration. The startup-configuration file will be loaded automatically across a system reboot, the configuration manager screen in Figure 4-16-5 appears.

Figure 4-16-5: Configuration Manager Page Screenshot

The Page includes the following fields:

Object	Description
• **Source File**	Provide Running configuration option.
• **Destination File**	Provide "Startup configuration" and "Backup configuration" options.

Button

Apply : Click to apply changes.

4.16.6 Enable Password

The page allows configuring system password, the enable password screen in Figure 4-16-6 appears.

Figure 4-16-6: Enable Password Page Screenshot

The Page includes the following fields:

Object	Description
• **Privilege Value**	Provide 0-15 option.
• **Password Type**	Provide **"Clear Text"** and **"Encrypted"** options.
• **Password**	Allow input the new password and available range is 30 characters.
• **Retype Password**	Allow input the new password again for confirm.

Button

Apply : Click to apply changes.

Figure 4-16-7: Local Enable Password Page Screenshot

The Page includes the following fields:

Object	Description
• **Privilege Value**	Display current privilege value information.
• **Password Type**	Display current password type information.
• **Modify**	Click **Delete** to delete password entry.

5. COMMAND LINE INTERFACE

5.1 Accessing the CLI

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

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

Logon to the Console

Once the terminal is connected to the device, power on the PoE Managed Switch and the terminal will **run self testing procedures**.

Then, the following message asks to login user name and password. The factory default user name and password are shown as follows and the login screen in Figure 5-1 appears.

> Username: **admin**
> Password: **admin**

1. On"**Username**" &"**Password**"prompt, enter "**admin**".

2. The user can now enter commands to manage the PoE Managed Switch. For a detailed description of the commands, please refer to the following chapters.
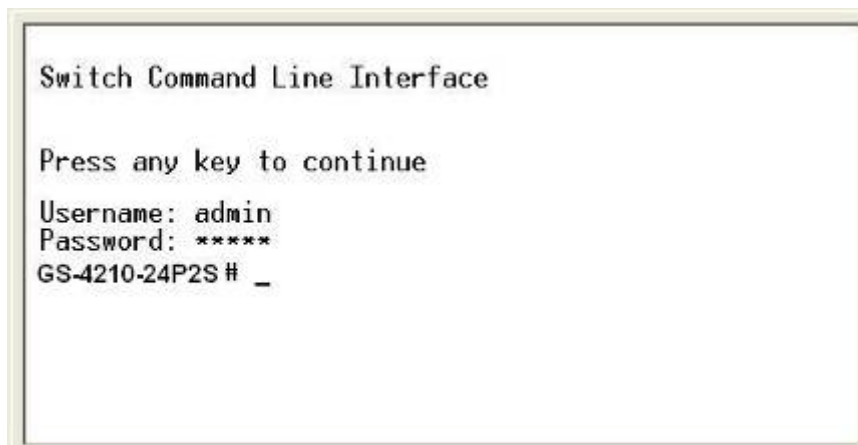
Figure 5-1: PoE Managed Switch Console Login Screen

	1.	For security reason, please change and memorize the new password after this first setup.
Note	2.	Only accept command in lowercase letter under console interface.

Configure IP address
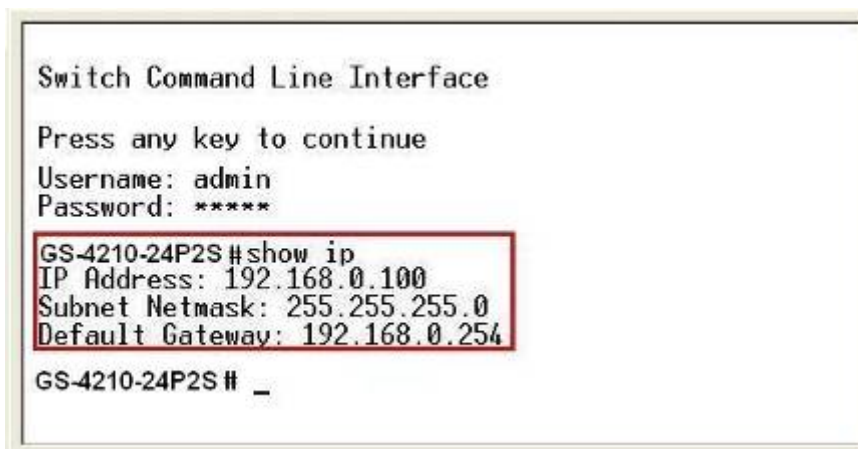
The PoE Managed Switch is shipped with default IP address as follows:

IP Address: **192.168.0.100**

Subnet Mask: **255.255.255.0**

To check the current IP address or modify a new IP address for the PoE Managed Switch, please use the procedures as follows:

◼ **Display of the current IP address**

1. On"**GS-4210-24P2S#**" prompt, enter "**show ip**".

2. The screen displays the current IP address, Subnet Mask and Gateway shown in Figure 5-2.

Figure 5-2: IP Information Screen

◼ **Configuration of the IP address**

3. On " **GS-4210-24P2S#**" prompt, enter "**configure**".

4. On "**GS-4210-24P2S (config)#**" prompt, enter the following command and press **<Enter>** as shown in Figure 5-3.

GS-4210-24P2S (config)# **ip address 192.168.1.100 mask 255.255.255.0**
GS-4210-24P2S (config)# **ip default-gateway 192.168.1.254**

The previous command would apply the following settings for the PoE Managed Switch.

IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254

```
GS-4210-24P2S# show ip
IP Address: 192.168.0.100
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.0.254
GS-4210-24P2S# configure
GS-4210-24P2S(config)# ip address 192.168.1.100 mask 255.255.255.0
GS-4210-24P2S(config)# ip default-gateway 192.168.1.254
GS-4210-24P2S(config)#
```

Figure 5-3: Setting IP Address Screen

5. Repeat Step 1 to check if the IP address is changed.

If the IP is successfully configured, the PoE Managed Switch will apply the new IP address setting immediately. You can access the Web interface of PoE Managed Switch through the new IP address.

> If you do not familiar with console command or the related parameter, enter "**?**" anytime in console to get the help description.

5.2 Telnet Login

The PoE Managed Switch also supports telnet for remote management. The PoE Managed Switch asks for user name and password for remote login when using telnet, please use **"admin"** for username & password.

```
Telnet 192.168.0.100

Switch Command Line Interface (Version v1.0b140611)


Username: admin
Password: *****
GS-4210-24P2S#
```

Figure 5-4: Telnet Login Screen

6. Command Line Mode

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes supports specific software commands.

Mode-based Command Hierarchy

The **Command Line Interface (CLI)** groups all the commands in appropriate modes by the nature of the commands. Examples of the CLI command modes are described below. Each of the command modes supports specific switch's commands.

The CLI Command Modes table captures the command modes, the prompts visible in that mode and the exit method from that mode.

Command Mode	Access Method	Prompt	Exit or Access Previous Mode
User Mode	This is the first level of access. Perform basic tasks and list system information.	GS-4210-24P2S>	Enter exit command
Privileged Mode	From the User Mode, enter the enable command.	GS-4210-24P2S #	To exit to the User Mode, enter exit .
Global Config Mode	From the Privileged Mode, enter the configuration command.	GS-4210-24P2S (Config)#	To exit to the Privileged Mode, enter the exit command.

Table 6-1: CLI Command Modes

The CLI is divided into various modes. The commands in one mode are not available until the operator switches to that particular mode. The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, and displayss a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

User Mode

When the operator logs into the CLI, the User Mode is the initial mode. The User Mode contains a limited set of commands. The command prompt shown at this level is:

Command Prompt: GS-4210-24P2S >

Privileged Mode

To have access to the full suite of commands, the operator must enter the Privileged Mode. The Privileged Mode requires password authentication. From Privileged Mode, the operator can issue any Exec command to enter the Global Configuration mode. The command prompt shown at this level is:

Command Prompt: GS-4210-24P2S #

Global Config Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the Interface Configuration mode. The command prompt at this level is:

Command Prompt: GS-4210-24P2S (Config)#

From the Global Config mode, the operator may enter the following configuration modes:

6.1 User Mode Commands

6.1.1 enable command

Description:

Turn on privileged mode command

Syntax:

enable

Example:

```
GS-4210-24P2S> enable
Password:
GS-4210-24P2S#
```

6.1.2 exit command

Description:

Exit current mode and down to previous mode

Syntax:

exit

Example:

```
GS-4210-24P2S# exit
GS-4210-24P2S>
```

6.1.3 ping command

Description:

Send ICMP ECHO_REQUEST to network hosts

Syntax:

ping HOSTNAME (Host name)

Example:

```
GS-4210-24P2S> ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100): 56 data bytes
64 bytes from 192.168.0.100: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.0 ms
--- 192.168.0.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
GS-4210-24P2S>
```

6.1.4 Show Command

show arp

Description:

Show the IP ARP translation table

Syntax:

show arp

Example:

```
GS-4210-24P2S> show arp
Address                 HWtype    HWaddress           Flags Mask       Iface
192.168.0.100           ether     C8:9C:DC:EC:D6:DD   C                eth0
GS-4210-24P2S>
```

show history

Description:

List the last several history commands

Syntax:

show history

Example:

```
GS-4210-24P2S> show history
```

show info

Description:

Show basic information

Syntax:

show info

Example:

```
GS-4210-24P2S> show info
```

show ip

Description:

Show the IP Address, Subnet Mask, Default Gateway

Syntax:

show ip

Example:

```
GS-4210-24P2S> show ip
IP Address: 192.168.0.100
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.0.254
GS-4210-24P2S>
```

show privilege

Description:

Show the local user privilege level

Syntax:

show privilege

Example:

```
GS-4210-24P2S> show privilege
Current CLI Username:   admin
Current CLI Privilege: 15
GS-4210-24P2S>
```

show version

Description:

Show the system hardware and software status

Syntax:

show version

Example:

```
GS-4210-24P2S> show version
Loader Version     : 2011.12.41872
Loader Date        : May 22 2014 - 19:28:43
Firmware Version :   v1.0b140611
Firmware Date      : Wed Jun 11 10:13:28 CST 2014
Magic Number       : 83800000
GS-4210-24P2S>
```

6.1.5 traceroute command

Description:

Trace route to network hosts

Syntax:

traceroute HOSTNAME (The IP address or hostname address to trace)

Example:

GS-4210-24P2S> traceroute 192.168.0.100

6.2 Privileged Mode Commands

6.2.1 clear command

clear arp

Description:

Clear entries in the ARP cache

Syntax:

clear arp A.B.C.D (IP address to clear)

clear arp (the entire ARP cache is cleared)

Example:

GS-4210-24P2S# clear arp 192.168.0.100

GS-4210-24P2S#

GS-4210-24P2S# clear arp

GS-4210-24P2S#

clear GVRP

Description:

Clear the GVRP configuration

Syntax:

clear GVRP error-statistics (GVRP Error Statistics information)

clear GVRP statistics (GVRP Statistics information)

Example:

GS-4210-24P2S# clear gvrp error-statistics

GS-4210-24P2S# clear gvrp statistics

GS-4210-24P2S#

clear interfaces

Description:

Clear the Interface status and configuration

Syntax:

clear interface LAG <1-8> counters

clear interfaces GigabitEthernet <1-26> counters

Example:

```
GS-4210-24P2S# clear interfaces lag 1 counters
GS-4210-24P2S# clear interfaces GigabitEthernet 1 counters
GS-4210-24P2S#
```

clear ip arp

Description:

Clear the IP configuration

Syntax:

clear ip arp inspection interfaces LAG <1-8> statistics

clear ip arp inspection interfaces GigabitEthernet <1-26> statistics

Example:

```
GS-4210-24P2S# clear ip arp inspection interfaces lag 1 statistics
GS-4210-24P2S# clear ip arp inspection interfaces GigabitEthernet 1 statistics
GS-4210-24P2S#
```

clear ip dhcp

Description:

Clear the DHCP configuration

Syntax:

clear ip dhcp snooping database statistics

clear ip dhcp snooping interfaces LAG <1-8> statistics

clear ip dhcp snooping interfaces GigabitEthernet <1-26> statistics

Example:

```
GS-4210-24P2S# clear ip dhcp snooping database statistics
GS-4210-24P2S# clear ip dhcp snooping interfaces lag 1 statistics
GS-4210-24P2S# clear ip dhcp snooping interface GigabitEthernet 1 statistics
GS-4210-24P2S#
```

clear ip igmp

Description:

Clear the IGMP configuration

Syntax:

clear ip igmp snooping groups dynamic / static

clear ip igmp snooping statistics

clear ip dhcp snooping vlan x static-mac xx:xx:xx:xx:xx:xx

Example:

```
GS-4210-24P2S# clear ip igmp snooping groups dynamic
GS-4210-24P2S# clear ip igmp snooping groups static
GS-4210-24P2S# clear ip igmp snooping statistics
GS-4210-24P2S# clear ip igmp snooping vlan 1 static-mac 00:30-4F:00:00:01
GS-4210-24P2S#
```

clear ipv6

Description:

Clear the ipv6 information

Syntax:

clear ipv6 mld snooping groups dynamic / static

clear ipv6 mld snooping statistics

clear ipv6 mld snooping vlan x static-mac xx:xx:xx:xx:xx:xx

Example:

```
GS-4210-24P2S# clear ipv6 mld snooping groups dynamic
GS-4210-24P2S# clear ipv6 mld snooping groups static
GS-4210-24P2S# clear ipv6 mld snooping statistics
GS-4210-24P2S# clear ipv6 mld snooping vlan 1 static-mac 00:30:4F:00:00:01
GS-4210-24P2S#
```

clear line

Description:

Clear identify a specific line for configuration

Syntax:

clear line ssh / telnet

Example:

```
GS-4210-24P2S# clear line ssh
GS-4210-24P2S# clear line telnet
GS-4210-24P2S#
```

clear lldp

Description:

Clear lldp configuration

Syntax:

clear line lldp statistics

Example:

```
GS-4210-24P2S# clear lldp statistics
GS-4210-24P2S#
```

clear logging

Description:

Clear log configuration

Syntax:

clear logging buffered / flash

Example:

```
GS-4210-24P2S# clear logging buffered
GS-4210-24P2S# clear logging flash
GS-4210-24P2S#
```

clear mac

Description:

Clear MAC configuration

Syntax:

clear mac address-table dynamic interface lag x

clear mac address-table dynamic interface GigabitEthernet x

clear mac address-table dynamic vlan x

Example:

```
GS-4210-24P2S# clear mac address-table dynamic interfaces lag 1

GS-4210-24P2S# clear mac address-table dynamic interfaces GigabitEthernet 1

GS-4210-24P2S# clear mac address-table dynamic vlan 1

GS-4210-24P2S#
```

clear rmon

Description:

Clear RMON information

Syntax:

clear rmon interfaces lag x statistics

clear rmon interfaces GigabitEthernet x statistics

Example:

```
GS-4210-24P2S# clear rmon interfaces lag 1 statistics

GS-4210-24P2S# clear rmon interfaces GigabitEthernet 1 statistics

GS-4210-24P2S#
```

6.2.2 clock command

Description:

Manage the system clock

Syntax:

clock set HH:MM:SS:Month: Date: Year

Example:

```
GS-4210-24P2S# clock set 13:36:00 jul 3 2014

13:36:00 DFL(UTC+8) Jul 03 2014

GS-4210-24P2S#
```

6.2.3 configure command

Description:

Enter Global Config mode

Syntax:

configure

Example:

```
GS-4210-24P2S# configure
GS-4210-24P2S(config)#
```

6.2.4 copy command

Description:

Copy from one file to another

Syntax:

copy backup-config / flash:// / running-config / startup-config / tftp://   running-config / startup-config / tftp://

Example:

```
GS-4210-24P2S# copy running-config   startup-config
Success
GS-4210-24P2S#
```

6.2.5 debug command

Description:

Debug Options

Syntax:

debug acl all / common / reserve / user-defined

Example:

```
GS-4210-24P2S# debug acl all
GS-4210-24P2S# debug acl common
GS-4210-24P2S# debug acl reserve
GS-4210-24P2S# debug acl user-defined
GS-4210-24P2S#
```

6.2.6 delete command

Description:

Delete a file from the flash file system

Syntax:

delete backup-config / flash:// / startup-config / system image x

Example:

```
GS-4210-24P2S# delete backup-config
GS-4210-24P2S# delete flash://
GS-4210-24P2S# delete startup-config
GS-4210-24P2S# delete system image 0
GS-4210-24P2S#
```

6.2.7 disable command

Description:

Turn off privileged mode command

Syntax:

disable

Example:

```
GS-4210-24P2S# disable
GS-4210-24P2S>
```

6.2.8 end command

Description:

End current mode and change to enable mode

Syntax:

end

Example:

```
GS-4210-24P2S(config)# end
GS-4210-24P2S#
```

6.2.9 exit command

Description:

Exit current mode and down to previous mode

Syntax:

exit

Example:

```
GS-4210-24P2S# exit
GS-4210-24P2S>
```

6.2.10 no command

Description:

Negate command

Syntax:

no debug acl all / common / reserve / user-defined

Example:

```
GS-4210-24P2S# no debug acl all
GS-4210-24P2S# no debug acl common
GS-4210-24P2S# no debug acl reserve
GS-4210-24P2S# no debug acl user-defined
GS-4210-24P2S#
```

6.2.11 ping command

Description:

Send ICMP ECHO_REQUEST to network hosts

Syntax:

ping HOSTNAME (Host name)

Example:

```
GS-4210-24P2S> ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100): 56 data bytes
64 bytes from 192.168.0.100: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.0 ms
--- 192.168.0.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
GS-4210-24P2S>
```

6.2.12 reboot command

Description:

Halt and perform a cold restart

Syntax:

reboot

Example:

```
GS-4210-24P2S# reboot
*Jul 03 14:22:09: %System-4: System reboot
```

6.2.13 renew command

Description:

RenewIP configuration

Syntax:

renew ip dhcp snooping database

Example:

```
GS-4210-24P2S# renew ip dhcp snooping database
GS-4210-24P2S#
```

6.2.14 restore-defaults command

Description:

Restore to default

Syntax:

restore-defaults

Example:

```
GS-4210-24P2S# restore-defaults

Restore Default Success. Do you want to reboot now? (y/n)y

Rebooting now...

*Jan 01 08:16:00: %System-4: System reboot
```

6.2.15 save command

Description:

Save running configuration to flash

Syntax:

save

Example:

```
GS-4210-24P2S# save

Success

GS-4210-24P2S#
```

6.2.16 show command

Description:

Show running system information

Syntax:

show specific item

Example:

```
GS-4210-24P2S# show version

Loader Version    : 2011.12.41872

Loader Date       : May 22 2014 - 19:28:43

Firmware Version : v1.0b140611

Firmware Date     : Wed Jun 11 10:13:28 CST 2014

Magic Number     : 83800000

GS-4210-24P2S#
```

6.2.17 ssl command

Description:

Setup SSL host keys

Syntax:

ssl

Example:

```
GS-4210-24P2S# ssl

Generating a 1024 bit RSA private key

...........................++++++

writing new private key to '/mnt/ssh/ssl_key.pem'

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:2

string is too short, it needs to be at least 2 bytes long

Country Name (2 letter code) [AU]:TW

State or Province Name (full name) [Some-State]:TW

Locality Name (eg, city) []:Taipei

Organization Name (eg, company) [Internet Widgits Pty Ltd]:PLANET

Organizational Unit Name (eg, section) []:GS-4210-24P2S

Common Name (e.g. server FQDN or YOUR name) []:Marc

Email Address []:marcl@planet.com.tw

GS-4210-24P2S#
```

6.2.18 traceroute command

Description:

Trace route to network hosts

Syntax:

traceroute HOSTNAME (The IP address or hostname address to trace)

Example:

```
GS-4210-24P2S> traceroute 192.168.0.100
```

6.2.19 udld command

Description:

Configure global UDLD setting

Syntax:

udld reset

Example:

```
GS-4210-24P2S# udld reset

GS-4210-24P2S# *Jan 01 08:16:26: %UDLD-5: No ports are disabled by UDLD
```

6.3 Global Config Mode Commands

6.3.1 aaa Command

Description:

AAA (Authentication, Authorization, Accounting)

Syntax:

aaa accounting commands / exec / system / update

aaa authentication enable / login

6.3.2 boot Command

Description:

Booting Operations

Syntax:

boot host auto-config

boot system image0/1

6.3.3 bridge Command

Description:

Global bridge table configuration

Syntax:

bridge multicast reserved-address xx:xx:xx:xx:xx:xx bridge / discard / peer

6.3.4 class-map Command

Description:

Create class map and enter class map configuration mode. Use no form in order to delete the class

Syntax:

class-map WORD<0-32> (specified the name of the class map).

6.3.5 clock Command

Description:

Manage the system clock

Syntax:

clock source local / sntp

clock summer-time

clock timezone

6.3.6 dos Command

Description:

DoS information

Syntax:

dos

daeqsa-deny   Destination MAC equals to source MAC

icmp-frag-pkts-deny   Fragmented ICMP packets

icmp-ping-max-length   DoS information

icmpv4-ping-max-check   Check ICMPv4 ping maximum packets size

icmpv6-ping-max-check   Check ICMPv6 ping maximum packets size

ipv6-min-frag-size-check   Check minimum size of IPv6 fragments

ipv6-min-frag-size-length   DoS information

land-deny   Source IP equals to destination IP

nullscan-deny   NULL Scan Attacks

pod-deny   Ping of Death Attacks

smurf-deny   Smurf Attacks

smurf-netmask   DoS information

syn-sportl1024-deny   SYN packets with sport less than 1024

synfin-deny   SYN and FIN bits set in the packet

synrst-deny   SYNC and RST bits set in the packet

tcp-frag-off-min-check   TCP fragment packet with offset equals to one

tcpblat-deny   Source TCP port equals to destination TCP port

tcphdr-min-check   Check minimum TCP header

tcphdr-min-length   DoS information

udpblat-deny   Source UDP port equals to destination UDP port

xma-deny   Xmascan: sequence number is zero and the FIN, URG and PSH bits are set

6.3.7 dot1x Command

Description:

802.1x configuration

Syntax:

dot1x guest-vlan<1-4094> VLAN ID (e.g. 100)

6.3.8 do Command

Description:

To run exec commands in current mode

Syntax:

do SEQUENCE (Exec Command)

6.3.9 enable Command

Description:

Local Enable Password

Syntax:

enable password / privilege / secret

6.3.10 end Command

Description:

End current mode and change to enable mode

Syntax:

end

6.3.11 errdisable Command

Description:

Error Disable

Syntax:

errdisable recovery cause / interval

6.3.12 exit Command

Description:

Exit current mode and down to previous mode

Syntax:

Exit

6.3.13 gvrp Command

Description:

GVRP configuration

Syntax:

gvrp time join / leave / leaveall

6.3.14 hostname Command

Description:

Set system's network name

Syntax:

hostname WORD (this system's network name)

6.3.15 interface Command

Description:

Select an interface to configure

Syntax:

Interface GigabitEthernet / LAG / range

6.3.16 ip Command

Description:

IP configuration

Syntax:

Ip

acl   This command creates an ACL, which perform classification on layer 3 fields and enters ip-access configuration mode.

address	IPv4 Address
arp	ARP configuration
default-gateway	Set default gateway IP address
dhcp	DHCP configuration
dns	Domin Name Server
http	HTTP server configuration
https	HTTPS server configuration
igmp	IGMP Configuration
source	IP Source Guard Configuration
ssh	SSH (Secure Shell) configuration
telnet	Telnet daemon configuration

6.3.17 ipv6 Command

Description:

IPV6 configuration

Syntax:

ipv6

acl   This command creates an ACL, which perform classification onlayer 3 fields and enters to ipv6-access configuration mode.

address	Set IPv6 address and prefix
autoconfig	Enable Ipv6 auto-configuration
default-gateway	Set IPv6 gateway
dhcp	Set IPv6 DHCP Client
mld	MLD Configuration

6.3.18 jumbo-frame Command

Description:

Jumbo Frame configuration

Syntax:

jumbo-frame <64-9216> (Maximum frame size)

6.3.19 l2 Command

Description:

L2 information

Syntax:

l2 igmp snooping unknown-multicast action drop / flood

6.3.20 lacp Command

Description:

LACP Configuration

Syntax:

lacp system-priority <1-65535> (LACP system priority)

6.3.21 lag Command

Description:

Link Aggregation Group Configuration

Syntax:

lag load-balance src-dst-mac / src-dst-mac-ip

6.3.22 line Command

Description:

To identify a specific line for configuration

Syntax:

line console / ssh / telnet

6.3.23 lldp Command

Description:

LLDP Configuration

Syntax:

lldp

holdtime-multiplier   Configure LLDP holdtime multiplier

lldpdu   Configure LLDP PDU handling when LLDP is disabled

med   LLDP MED configuration

reinit-delay   Configure LLDP reinitialization delay

tx-delay   Configure LLDP TX delay

tx-interval   Configure LLDP transmission interval

6.3.24 logging Command

Description:

Log Configuration

Syntax:

logging

buffered   RAM

flash   Flash

host   Remote syslog host

6.3.25 mac Command

Description:

MAC Configuration

Syntax:

mac

acl   This command enters the extended MAC ACL configuration in order to create layer 2 extended ACL.

address-table   MAC address table configuration

6.3.26 management-VLAN Command

Description:

Management VLAN configuration

Syntax:

management-vlan vlan <1-4094>   VLAN ID (e.g. 100)

6.3.27 mirror Command

Description:

Mirror configuration

Syntax:

mirror session <1-4> Session ID (e.g. 1-4)configuraton destination / source interface / GigabitEthernet <1-26> GigabitEthernet

device number

6.3.28 no Command

Description:

Negate command

Syntax:

no

6.3.29 policy-map Command

Description:

This command create policy map and enter policy map configuration mode. Use no form to delete the policy map

Syntax:

policy-map WORD<0-32> (Enter the policy-map name)

6.3.30 port-security Command

Description:

Port security Configuration

Syntax:

port-security

6.3.31 qos Command

Description:

Enable / Disable QoS on the device and enter the QoS mode (advance / basic)

Syntax:

qos

advanced   Enable/Disable QoS on the device and enter the QoS mode (advance/basic).

advanced-mode   Set the trust mode when the default action is ports-trusted in advanced mode.

aggregate-policer   Configure a policer that can be applied to multiple classes within the same policy map. Use the no form of

the command to remove policer.

basic   Set system QoS advance mode.

map   Configure the QoS maps.

queue   Queue configuration

trust   Configure the global trust mode . Use the no form to return untrusted state.

6.3.32 radius Command

Description:

RADIUS server information

Syntax:

radius default-config / host

6.3.33 rate-limit Command

Description:

Rate limit configuration of the specified incoming traffic

Syntax:

rate-limit egress / ingress

6.3.34 rmon Command

Description:

RMON information

Syntax:

rmon alarm / event / history

6.3.35 Snmp Command

Description:

SNMP information

Syntax:

snmp

community	Set community or security name string
engineid	SNMP engine id setting
group	Set access group string
host	Trap or inform host
trap	Snmp class trap setting
user	Set user Settings
view	Set view string

6.3.36 sntp Command

Description:

Simple Network Time Protocol

Syntax:

sntp host

6.3.37 spanning-tree Command

Description:

Spanning-tree configuration

Syntax:

Spanning-tree

bpdu	action for bpdu packet
forward-delay	Sets the forward-delay parameter
hello-time	Sets the hello-time parameter
max-hops	Sets the max-hops parameter
maximum-age	Changes the interval between messages the spanning tree receive s from the root switch
mode	Spanning tree protocol type
mst	Multiple spanning tree configuration
pathcost	Spanning tree path-cost method
priority	Sets the priority for specified instance
tx-hold-count	Set spanning-tree tx hold count, in seconds

6.3.38 storm-control Command

Description:

Storm control configuration

Syntax:

Storm-control

ifg   Interframe configuration

unit   Unit configuration

6.3.39 system Command

Description:

System information

Syntax:

contact   Set host contact

location   Set host location

name   Set host name

6.3.40 tacacs Command

Description:

TACACS+ server information

Syntax:

tacacs

default-config   TACACS+ server default parameters

host   TACACS+ server host

6.3.41 udld Command

Description:

Configure global UDLD setting

Syntax:

udld

aggressive   Enable UDLD protocol in aggressive mode on fiber ports except wher e locally configured

enable   Enable UDLD protocol on fiber ports except where locally configured

message   Set UDLD message parameters

6.3.42 username Command

Description:

Local User Configuration

Syntax:

username USERNAME   Local user name

nopassword   No password for this user

password   Use clear text password

privilege   Local user privilege level

secret   Use encrypted password

6.3.43 vlan Command

Description:

VLAN Configuration

Syntax:

vlan

VLAN-LIST   VLAN List (e.g. 3,6-8): The range of VLAN ID is 1 to 4094

protocol-vlan   802.1v protocol VLAN configuration

6.3.44 voice-vlan Command

Description:

Voice VLAN Configuration

Syntax:

voice vlan <1-4094> (Specifies the Voice VLAN Identifier)

7. SWITCH OPERATION

7.1 Address Table

The Switch is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This in-formation comes from the learning process of Ethernet Switch.

7.2 Learning

When one packet comes in from any port, the Switch will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

7.3 Forwarding & Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the Ethernet Switching will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

7.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques.   A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The Ethernet Switch scans the destination address from the packet-header, searches the routing table pro-vided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. How-ever, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to signifi-cantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The Switch performs "Store and forward" therefore, no error packets occur.   More reliably, it reduces the re-transmission rate.

No packet loss will occur.

7.5 Auto-Negotiation

The STP ports on the Switch have built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	100Base-TX port will set to:
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100Base-TX/Full-Duplex)

8. POWER OVER ETHERNET OVERVIEW

What is PoE?

The PoE is an abbreviation of Power over Ethernet; the PoE technology means a system to pass electrical power safely, along with data on Ethernet UTP cable. The IEEE standard for PoE technology requires Category 5 cable or higher for high power PoE levels, but can operate with category 3 cable for low power levels. Power is supplied in common mode over two or more of the differential pairs of wires found in the Ethernet cables and comes from a power supply within a PoE-enabled networking device such as an Ethernet switch or can be injected into a cable run with a mid-span power supply.

The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350mA) to each device. Only 12.95 W is assured to be available at the powered device as some power is dissipated in the cable. The updated IEEE 802.3at-2009 PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power. The 2009 standard prohibits a powered device from using all four pairs for power

The 802.3af / 802.3at define two types of source equipment: Mid-Span and End-Span.

Mid-Span
Mid-Span device is placed between legacy switch and the powered device. Mid-Span is tap the unused wire pairs 4/5 and 7/8 to carry power, the other four is for data transmit.

End-Span
End-Span device is direct connecting with power device. End-Span could also tap the wire 1/2 and 3/6.

PoE System Architecture
The specification of PoE typically requires two devices: the **Powered Source Equipment (PSE)** and the **Powered Device (PD)**. The PSE is either an End-Span or a Mid-Span, while the PD is a PoE-enabled terminal, such as IP Phones, Wireless LAN, etc. Power can be delivered over data pairs or spare pairs of standard CAT-5 cabling.

Powered Source Equipment (PSE)

Power sourcing equipment (PSE) is a device such as a switch that provides (sources) power on the Ethernet cable. The maximum allowed continuous output power per cable in IEEE 802.3af is 15.40 W. A later specification, IEEE 802.3at, offers 25.50 W. When the device is a switch, it is commonly called an End-span (although IEEE 802.3af refers to it as endpoint). Otherwise, if it's an intermediary device between a non PoE capable switch and a PoE device, it's called a Mid-span. An external PoE injector is a Mid-span device.

Powered device

A powered device (PD) is a device powered by a PSE and thus consumes energy. Examples include wireless access points, IP Phones, and IP cameras. Many powered devices have an auxiliary power connector for an optional, external, power supply. Depending on the PD design, some, none, or all power can be supplied from the auxiliary port, with the auxiliary port sometimes acting as backup power in case of PoE supplied power failure.

How Power is Transferred Through the Cable
A standard CAT5 Ethernet cable has four twisted pairs, but only two of these are used for 10BASE-T and 100BASE-TX. The specification allows two options for using these cables for power, shown in Figure 1 and Figure 2:
The spare pairs are used. Figure 1 shows the pair on pins 4 and 5 connected together and forming the positive supply, and the

pair on pins 7 and 8 connected and forming the negative supply. (In fact, a late change to the spec allows either polarity to be used).

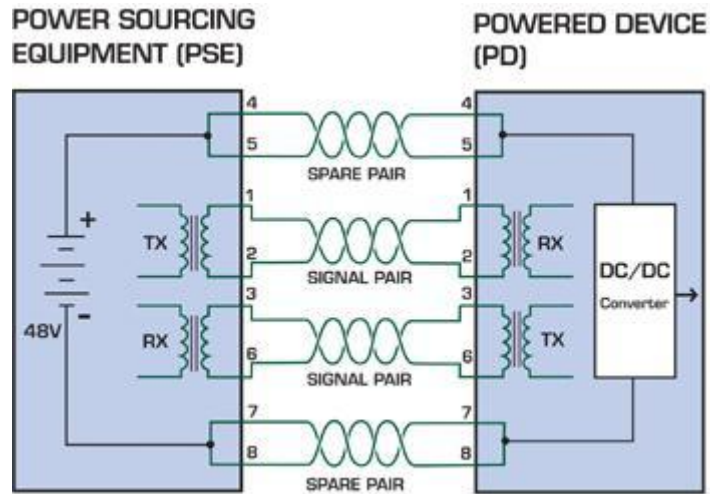**Figure 8-1:** Power Supplied over the Spare Pins

The data pairs are used. Since Ethernet pairs are transformer coupled at each end, it is possible to apply DC power to the center tap of the isolation transformer without upsetting the data transfer. In this mode of operation the pair on pins 3 and 6 and the pair on pins 1 and 2 can be of either polarity.
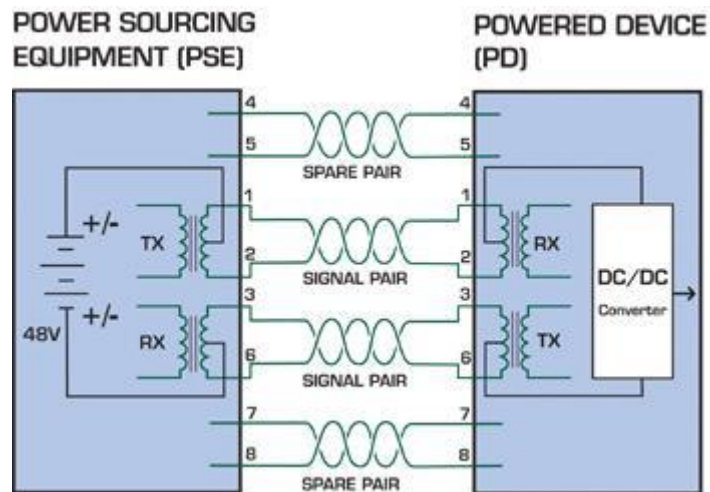

Figure 8-2: Power Supplied over the Data Pins

9. TROUBLESHOOTING

This chapter contains information to help you solve your issue. If the PoE Managed Switch is not functioning properly, make sure the PoE Managed Switch is set up according to instructions in this manual.

■ **The Link LED is not lit**

Solution:

Check the cable connection and remove duplex mode of the PoE Managed Switch.

■ **Some stations cannot talk to other stations located on the other port**

Solution:

Please check the VLAN settings, trunk settings, or port enabled / disabled status.

■ **Performance is bad**

Solution:

Check the full duplex status of the PoE Managed Switch. If the PoE Managed Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

■ **Why the Switch doesn't connect to the network**

Solution:

1. Check the LNK/ACT LED on the PoE Managed Switch.
2. Try another port on the PoE Managed Switch.
3. Make sure the cable is installed properly.
4. Make sure the cable is the right type.
5. Turn off the power. After a while, turn on power again.

■ **100Base-TX port link LED is lit, but the traffic is irregular**

Solution:

Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

■ **Switch does not power up**

Solution:

1. AC power cord not inserted or faulty
2. Check whether the AC power cord is inserted correctly
3. Replace the power cord if the cord is inserted correctly, check that the AC power source is working by connecting a different device in place of the switch.
4. If that device works, refer to the next step.
5. If that device does not work, check the AC power

APPENDIX A

A.1 Switch's RJ-45 Pin Assignments 1000Mbps, 1000Base T

| Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	MDI Media Dependent Interface	MDI-X Media Dependent Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ-45 pin assignment
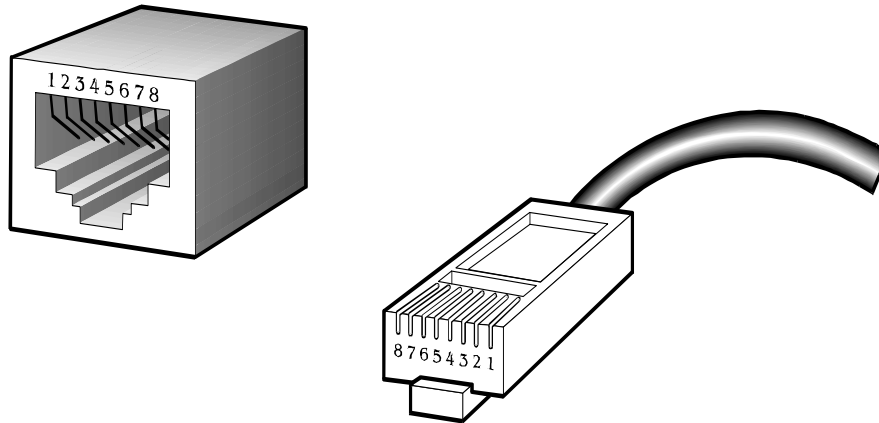
The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

Straight-through Cable		SIDE 1	SIDE 2
	SIDE 1	1 = White / Orange	1 = White / Orange
		2 = Orange	2 = Orange
		3 = White / Green	3 = White / Green
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Green
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown
Crossover Cable		SIDE 1	SIDE 2
	SIDE 1	1 = White / Orange	1 = White / Green
		2 = Orange	2 = Green
		3 = White / Green	3 = White / Orange
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Orange
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown

Figure A-1: Straight-through and Crossover Cable

Please make sure your connected cables are with the same pin assignment and color as the above table before deploying the cables into your network.

EC Declaration of Conformity

For the following equipment:

*Type of Product	:	24-Port 10/100/1000T 802.3at PoE + 2-Port 100/1000X SFP Managed Switch
*Model Number	:	GS-4210-24P2S

* Produced by:

Manufacturer's Name	:	**Planet Technology Corp.**
Manufacturer's Address	:	10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.).

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC).
For the evaluation regarding the EMC, the following standards were applied:

EN 55022	(2010+AC: 2011)
EN 61000-3-2	(2006+A1:2009+A2:2009)
EN 61000-3-3	(2013)
EN 55024	(2010)
IEC 61000-4-2	(2008)
IEC 61000-4-3	(2006+A1:2007+A2:2010)
IEC 61000-4-4	(2012)
IEC 61000-4-5	(2005)
IEC 61000-4-6	(2013)
IEC 61000-4-8	(2009)
IEC 61000-4-11	(2004)

Responsible for marking this declaration if the:

☒ **Manufacturer**   ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)**

Person responsible for making this declaration

Name, Surname   **Kent Kang**

Position / Title :   **Product Manager**

Taiwan	**15th, Aug., 2014**	*(signature)*
Place	*Date*	*Legal Signature*

PLANET TECHNOLOGY CORPORATION