PLANET
Networking & Communication

User's Manual

GSW-1602SF

GSW-2404SF

10/100/1000Mbps

16/24-Port Web Smart

Gigabit Ethernet Switch

Trademarks

Copyright © PLANET Technology Corp. 2010.

Contents subject to which revision without prior notice.

PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.

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 whose 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.

Without removing power cable, the device will still consuming power from the power source. In the view of Saving the Energy and reduce the unnecessary power consuming, 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 16/24-Port 10/100/1000Mbps Web Smart Gigabit Ethernet Switch User's Manual

FOR MODELS: GSW-1602SF / GSW-2404SF

REVISION: 3.1 (NOVEMBER 2010)

Part No.: 2080-A82070-004

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Package Contents

Check the contents of your package for following parts:

- Web Smart Gigabit Ethernet Switch x1
- Quick Installation Guide x 1
- User's manual CD x 1
- Power Cord x 1
- Rubber feet x 4
- Two rack-mounting brackets with attachment screws x1

If any of these are missing or damaged, please contact your dealer immediately, if possible, retain the carton including the original packing material, and use them against to repack the product in case there is a need to return it to us for repair.

In the following section, the term **"Web Smart Gigabit Switch"** means the two Switch devices, ie. GSW-1602SF and GSW-2404SF; term of **"switch"** can be any third switches.

1.2 Product Description

The PLANET GSW-1602SF / GSW-2404SF is a 16/24-Port 10/100/1000Mbps Web Smart Gigabit Ethernet Switch with non-blocking wire-speed performance. With 32/48Gbps internal switching fabric, the GSW-1602SF / GSW-2404SFcan handle extremely large amounts of data transmission in a secure topology linking to a backbone or high-power servers. The GSW-1602SF / GSW-2404SF could recognize up to 8K MAC Address table and provides 340KB /500KB on-chip frame buffer. The GSW-1602SF / GSW-2404SF offers wire-speed packet transfer performance without risk of packet loss. The high data throughput, it can provide the most convenient for user to upgrade their network to Gigabit environment.

Product Overview

PLANET GSW-1602SF / GSW-2404SF is a Web Smart Gigabit Ethernet Switch with 16/24 RJ-45 10/100/1000Mbps ports for high-speed network connectivity. GSW-1602SF provide two shared SFP module slots (share with port 15, 16) and GSW-2404SF provide four shared SFP module slots (share with port 21, 22, 23,24).

These mini-GBIC slots can be 1000Base-SX/LX through SFP (Small Factor Pluggable) interfaces, the distance can be extended from 100 meters (TP), 550 meters (Multi-mode fiber), up to above 10/20/30/40/50/70/120 kilometers (Single-mode fiber).

The GSW-1602SF / GSW-2404SF also supports store-and-forward forwarding scheme to ensure low latency and high data integrity, eliminates unnecessary traffic and relieves congestion on critical network paths. With an intelligent address recognition algorithm, GSW-1602SF / GSW-2404SF could recognize up to 8K different MAC address and enables filtering and forwarding at full wire speed.

The GSW-1602SF / GSW-2404SF can also automatically identify and determine the correct transmission speed and half / full duplex mode of the attached devices with its 16/24 ports, the Gigabit ports with 9KB jumbo frame feature supported, can handle extremely large amounts of data transmission in a secure topology linking to a backbone or high-power servers.

1.3 How to Use This Manual

This Web Smart Gigabit Ethernet Switch User Manual is structured as follows:

- **Section 2, Installation**

    It explains the functions of Web Smart Gigabit Switch and how to physically install the Web Smart Gigabit Switch.

- **Section 3, Switch Management**

    It contains information about the managed methods of Web Smart Gigabit Switch.

- **Section 4, Configuration**

    It contains information about the Smart function of Web Smart Gigabit Switch.

Section 5, Switch operation

    It contains Switch operation information of Web Smart Gigabit Switch.

Section 6, Troubleshooting

    It contains Troubleshoting information of Web Smart Gigabit Switch.

Appendix A

    It contains cable information of Web Smart Gigabit Switch.

1.4 Product Features

▶ **Physical Port**

GSW-1602SF

- ■ **16-Port 10/100/1000Base-T** Gigabit Ethernet RJ-45
- ■ **2 mini-GBIC/SFP slots**, shared with Port-15 and Port-16

GSW-2404SF

- ■ **24-Port 10/100/1000Base-T** Gigabit Ethernet RJ-45
- ■ **4 mini-GBIC/SFP slots**, shared with Port-21 to Port-24

▶ **General Features**

- ■ Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standard
- ■ Supports Auto-negotiation and Half-Duplex / Full-Duplex modes for all 10Base-T/100Base-TX and 1000Base-T ports
- ■ Each Switching ports support auto-negotiation-10/20Mbps, 100/200Mbps and 1000/2000Mbps supported
- ■ Auto-MDI/MDI-X detection on each RJ-45 port, support CSMA/CD protocol
- ■ Prevents packet loss with back pressure (Half-Duplex) and IEEE 802.3x PAUSE frame flow control (Full-Duplex)
- ■ High performance Store and Forward architecture, broadcast storm control, runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
- ■ 8K MAC address table, automatic source address learning and ageing
- ■ 32/48Gbps switch fabric, non-blocking switch architecture
- ■ 9K Jumbo Frame support at all speed (10/100/1000Mbps)

▶ **Layer 2 Features**

- ■ Support VLANs
  - Port-based VLAN
  - IEEE 802.1Q tag-based VLAN
  - Q-in-Q tunneling
  - Up to 256 VLANs groups, out of 4094 VLAN IDs
- ■ Support Link Aggregation
  - up to 8 trunk groups
  - up to 12 ports per trunk group with 24Gbps bandwidth (Full Duplex Mode)
  - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
- ■ Spanning Tree Protocol
  - RSTP, IEEE 802.1w (Rapid Spanning Tree Protocol)
- ■ Port Mirroring to monitor the incoming or outgoing traffic on a particular port
- ■ Mini-GBIC module built-in information display
- ■ Cable Diagnostics technology and ICMP Ping function

- ■ Link Layer Discovery Protocol (LLDP) for discover basic information about neighboring devices on the local broadcast domain

- ■ Green Networking for energy saving

▶ **Quality of Service**

- ■ 4 priority queues on all switch ports

- ■ 8 mapping ID to 4 priority queues

- ■ Traffic class assignment based on IEEE 802.1p tag, or DSCP field

- ■ Multicast and Broadcast Storm Control as well as Flooding Control

- ■ Rate Limit bandwidth control at both inband and outband in steps of 128kbps

▶ **Multicast**

- ■ Supports IGMP Snooping v1 and v2

- ■ Querier mode support

- ■ Multicast Address Table for 256 groups display

▶ **Security**

- ■ IEEE 802.1X Port-Base access control, RADIUS ServerAuthentication

- ■ Source IP filter per port to block unwanted access

- ■ Static MAC Address assign destination MAC address at specifies port

▶ **Management**

- ■ PLANET Smart Discovery Utility

- ■ Switch Management Interface

- ■ Web switch management

- ■ SNMP v1, v2c switch management

- ■ Accesses through SNMPv1, v2c and get requests.

- ■ Firmware upgrade through Web interface

- ■ Configuration upload / download through Web interface

- ■ Support SNMPv1 with RFC-1213/1573-Interface group, Ethernet MIB

- ■ SNMPv1 Trap

1.5 PRODUCT SPECIFICATION

Product	GSW-1602SF	GSW-2404SF
Hardware Specification		
10/100/1000Mbps Copper Ports	16-Port Auto-MDI/MDI-X	24-Port Auto-MDI/MDI-X
SFP/mini-GBIC Slots	2, shared with Port-15 and Port-16	4, shared with Port-21~Port-24
Switch Architecture	Store-and-Forward	
Switch Throughput@64Bytes	23.8Mpps	35.7Mpps
Switch Fabric	32Gbps / non-blocking	48Gbps / non-blocking
Share Data Buffer	340KB	500KB
Address Table	8K entries	
Flow Control	Back pressure for Half-Duplex , IEEE 802.3x Pause Frame for Full-Duplex	
Jumbo Frame	9Kbytes	9Kbytes
Power Consumption	Max.19 Watts / 64 BTU	Max.26 Watts / 88 BTU
Dimensions (W x D x H)	440 x 120 x 44mm, 1U height	
Weight	1.57kg	1.67kg
Power Requirement	AC 100~240V, 50/60Hz , 1A	
Temperature	Operating: 0~50 Degree C / Storage: -40~70 Degree C	
Humidity Operating	Operating: 5% to 90% , non-condensing / Storage: 5% to 90% , non-condensing	
Layer 2 Function		
Management Interface	Web Browser, SNMPv1, v2c	
Firmware Upgrade	Web interface	
Configuration backup and restore	Yes, through web interface	
Port Configuration	■ Port disable/enable. ■ Auto-negotiation 10/100/1000Mbps full and half duplex mode selection. ■ Flow Control disable / enable. ■ Inband and outband bandwidth control. ■ Port description. ■ Frame Length setting	
Port Statistics	Displays per port Ethernet traffic receive counter information	
SFP module built-in information display	Yes	
Port Mirroring	Monitor the incoming or outgoing traffic on a particular port	
VLAN	Port-based VLAN IEEE 802.1Q Tagged Based VLAN ,up to 256 VLAN groups Q-in-Q VLAN	
Link Aggregation	IEEE 802.3ad LACP / Static Trunk Supports 12 groups of 8-Port trunk	
Rapid Spanning Tree	Yes	

IGMP Snooping	IGMP (v1/v2) Snooping, up to 256 multicast Groups IGMP Querier

QoS	Traffic classification based, Strict priority and WRR
	4-level priority for switching
	   - 802.1p priority
	   - DSCP field in IP Packet

Storm Control	■ Broadcast storm control ■ Multicast storm control ■ Flooded Unicast storm control
IEEE 802.1x Authentication	Yes
Filter Configuration	Source IP filter per port to block unwanted access
MAC Address Filter	Static MAC Address assign destination MAC address at specifies port
Diagnostics	Cable Diagnostics technology and ICMP Ping function
Link Layer Discovery Protocol (LLDP)	Discover basic information of neighboring devices on the local broadcast domain
Green Networking	Energy save for per port link up / link down operation mode
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-2863 Interface MIB Q-Bridge MIB RMON Group 1 statistics
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3z 1000Base- SX/LX IEEE 802.3ab 1000Base-T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1Q VLAN Tagging IEEE 802.1w Rapid spanning tree protocol IEEE 802.1p Class of service IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP

2. INSTALLATION

This section describes the functionalities of Web Smart Gigabit Switch components and guides how to install it on the desktop or shelf. Basic knowledge of networking is assumed. Please read this chapter completely before continuing.

2.1 Hardware Description

2.1.1 Switch Front Panel

The unit front panel provides a simple interface monitoring the switch. Figure 2-1 & 2-2 shows a front panel of GSW-1602SF / GSW-2404SF.

GSW-1602SF Front Panel
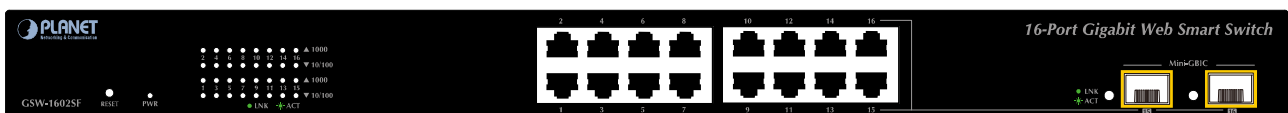
Figure 2-1 PLANET GSW-1602SF Front Panel

GSW-2404SF Front Panel
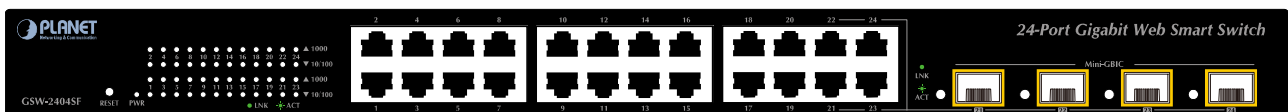
Figure 2-2 PLANET GSW-2404SF Front Panel

■ **Gigabit TP interface**

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

■ **Gigabit SFP slots**

   1000Base-SX/LX mini-GBIC slot, SFP (Small Factor Pluggable) transceiver module: From 550 meters (Multi-mode fiber), up to 10/30/50/70/120 kilometers (Single-mode fiber).

■ **Reset button**

   At the left of front panel, the reset button is designed for reboot the Web Smart Switch without turn off and on the power. The following is the summary table of Reset button functions:

Reset Button Pressed and Released	Function
About **1~3 second**	Reboot the Web Smart Switch

More than **5** seconds	Reset the Web Smart Switch to Factory Default configuration. The Web Smart Switch will then reboot and load the default settings as below: ◦ Default Password: **admin** ◦ Default IP address: **192.168.0.100** ◦ Subnet mask: **255.255.255.0** ◦ Default Gateway: **192.168.0.1**

2.1.2 LED Indicators

The front panel LEDs indicates instant status of port links, data activity and system power, helps monitor and troubleshoot when needed.

■ **LED of GSW-1602SF / GSW-2404SF**

| LED	Color	Function
PWR	**Green**	**Lights** to indicate that the Switch is powered on.
1000 LNK/ACT	**Green**	**Lights** to indicate that port is successfully connecting to the network at 1000Mbps. **Blinks** to indicate that port is receiving or sending data. **Off** to indicate that port is successfully connecting to the network at 10/100Mbps.
10/100 LNK/ACT	**Orange**	**Lights** to indicate that port is successfully connecting to the network at 10/100Mbps. **Blinks** to indicate that port receiving or sending data. **Off** to indicate that port is successfully connecting to the network at 1000Mbps.
SFP LNK/ACT	**Green**	**Lights** to indicate that port is successfully connecting to the network at 1000Mbps through SFP interface. **Blinks** to indicate that port is receiving or sending data.
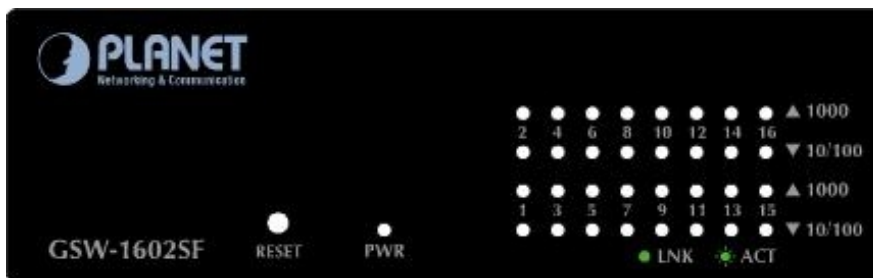
Figure 2-3 PLANET GSW-1602SF LED panel
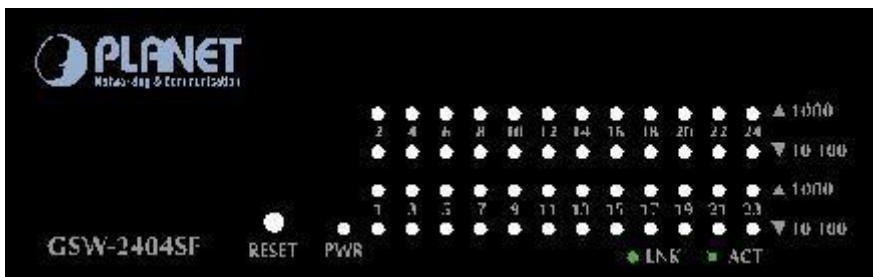
Figure 2-4 PLANET GSW-2404SF LED panel

	To press 5 seconds and release the RESET button. The GSW-1602SF / GSW-2404SF will back to the factory default mode (Except IP address). Be sure that you backup the current configuration of GSW-1602SF/GSW-2404SF; else the entire configuration will be erased when pressing the *"RESET"* button.
Note	

2.1.3 Switch Rear Panel

The rear panel of the Web Smart Gigabit Switch indicates an AC inlet power socket, which accepts input power from 100 to 240V AC, 50-60Hz.

■ **GSW-1602SF / GSW-2404SF**

Figure 2-5 Rear Panel of GSW-1602SF / GSW-2404SF

■ **AC Power Receptacle**

For compatibility with electric service in most areas of the world, the Web Smart Switch's power supply automatically adjusts to line power in the range 100-240VAC and 50/60 Hz.

Plug the female end of the power cord firmly into the receptalbe on the rear panel of the Web Smart Switch. Plug the other end of the power cord into an electric service outlet then the power will be ready.

	■ The device is a power-required device, it means, it will not work till it is powered. If your networks should 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.
Note	■ In some area, installing a surge suppression device may also help to protect your Web Smart Switch from being damaged by unregulated surge or current to the Switch or the power adapter.

2.2 Install the GSW-1602SF/GSW-2404SF

This section describes how to install your GSW-1602SF/GSW-2404SF Web Smart Gigabit Switch and make connections to the Switch. Please read the following topics and perform the procedures in the order being presented. PLANET GSW-1602SF/GSW-2404SF Web Smart Gigabit Switch do not need software configuration. To install your GSW-1602SF/GSW-2404SF on a desktop or shelf, simply complete the following steps.

2.2.1 Desktop Installation

To install a GSW-1602SF/GSW-2404SF on a desktop or shelf, simply complete the following steps:

Step1: Attach the rubber feet to the recessed areas on the bottom of the Web Smart Gigabit Switch.

Step2: Place the GSW-1602SF/GSW-2404SF on a desktop or shelf near an AC power source.

Step3: Keep enough ventilation space between the Web Smart Gigabit Switch and the surrounding objects.

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

Step4: Connect your GSW-1602SF/GSW-2404SF to network devices.

  A. Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the GSW-1602SF/GSW-2404SF.

  B. Connect the other end of the cable to the network devices such as printer servers, workstations or routers…etc.

> **Note** Connection to the Web Smart Gigabit 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 Web Smart Gigabit Switch.

  A. Connect one end of the power cable to the GSW-1602SF/GSW-2404SF.

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

When the GSW-1602SF/GSW-2404SF receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the Web Smart Gigabit Switch in a **19-inch** standard rack, follow the instructions described below.

Step1: Place your GSW-1602SF/GSW-2404SF on a hard flat surface, with the front panel positioned towards your front side.

Step2: Attach a rack-mount bracket to each side of the Web Smart Gigabit Switch with supplied screws attached to the package. Figure 2-6 shows how to attach brackets to one side of the Web Smart Gigabit Switch.
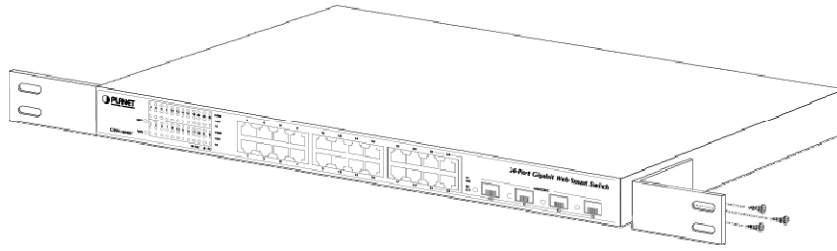
Figure 2-6 Attaching the brackets to the Web Smart Gigabit Switch

You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate your 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 Web Smart Gigabit Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-7.
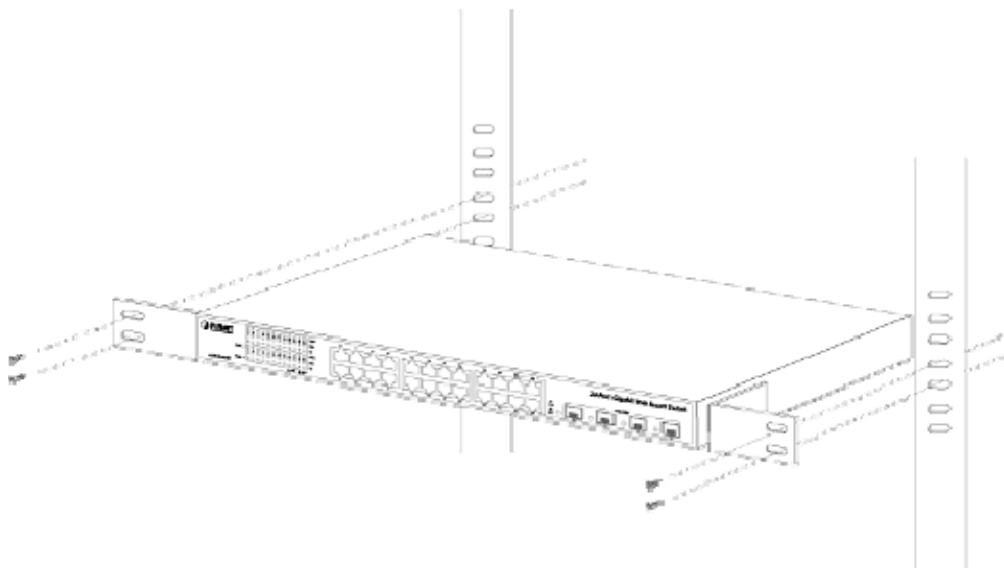
Figure 2-7 Mounting the Web Smart Gigabit Switch in a Rack

Step6: Precede with the steps 4 and steps 5 of session **2.2.1 Desktop Installation** to connect the network cabling and supply power to your Web Smart Gigabit 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-plug and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Web Smart Gigabit Switch. As the Figure 2-8 appears.

Figure 2-8 Plug-in the SFP transceiver

Approved PLANET SFP Transceivers

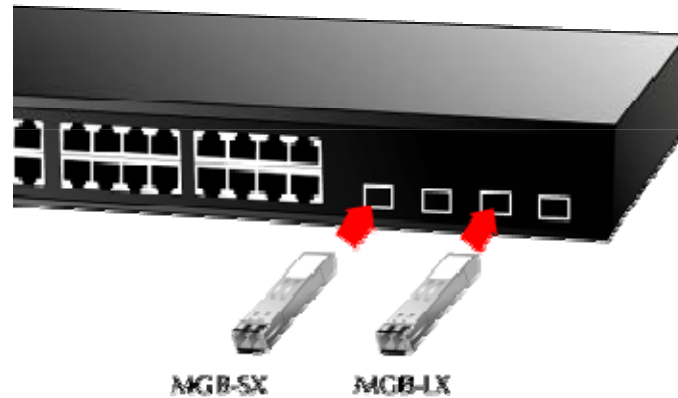PLANET GSW-1602SF/GSW-2404SF support both single mode and multi mode SFP transceiver. The following list of approved PLANET SFP transceivers is correct at the time of publication:

■MGB-SX SFP (1000BASE-SX SFP transceiver)

■MGB-LX SFP (1000BASE-LX SFP transceiver)

It recommends using PLANET SFPs on the Web Smart Gigabit Switch. If you insert a SFP transceiver that is not supported, the Web Smart Gigabit Switch will not recognize it.

Before connect the other switches, workstation or Media Converter.

1. Make sure both side of the SFP transceiver are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.

2. Check the fiber-optic cable type match the SFP transceiver model.

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

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

Connect the fiber cable

1. Attach the duplex LC connector on the network cable into the SFP transceiver.

2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a Media Converter..

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

4. Check the Link mode of the SFP port if the link failed. Co works with some fiber-NICs or Media Converters, set the Link mode to **"1000 Force"** is needed.

3. SWITCH MANAGEMENT

This chapter describes how to manage the GSW-1602SF/GSW-2404SF. Topics include:

- Overview

- Management methods

- Assigning an IP address to the GSW-1602SF/GSW-2404SF

- Logging on to the GSW-1602SF/GSW-2404SF

3.1 Overview

This chapter gives an overview of switch management. The GSW-1602SF/GSW-2404SF provides a simply Web browser interface. Using this interface, you can perform various switch configuration and management activities, including:

	Main Function
System	**System Information**
	IP Configuration
	User Authentication
	Firmware Upgrade
	Configuration Download
	Configuration Upload
	Factory Default
	System Reboot
SNMP	**System Configuration**
	System Information
Port Management	**Port Configuration**
	Port Statistics Overview
	Port Statistics Detail
	SFP Module Information
	Port Mirror Configuration
Link Aggregation	**Static Aggregation**
	LACP Port Configuration
	LACP System Status
	LACP Port Status
VLAN	**VLAN Basic Information**
	VLAN Port Configuration
	VLAN Membership

Rapid Spanning Tree	**System Configuration**
	Port Configuration
	Port Status
Multicast	**IGMP Snooping Configuration**
	IGMP Snooping Status
	Multicast Address Table
Quality of Service	**QoS Configuration**
	Storm Control Configuration
802.1X Authentication	**802.1X System Configuration**
	802.1X Port Configuration
Filter Configuration	**Source IP Filter**
MAC Address Table	**Aging Time Configuration**
	Static MAC Address
	Dynamic MAC Address Table
LLDP	**LLDP Configuration**
	LLDP Neighbors Table
	LLDP Statistics
Diagnostics	**Ping**
	Cable Diagnostics
Green Networking	**Energy Saving mode configure**

Please refer to the following Chapter 4 for more details.

3.2 Management Methods

The way to manage the GSW-1602SF/GSW-2404SF:

  - Web Management via a network connection.

3.2.1 Web Management

The PLANET Web Smart Gigabit Switch provides a built-in browser interface. You can manage the

GSW-1602SF/GSW-2404SF remotely by having a remote host with web browser, such as Microsoft Internet Explorer,

Netscape Navigator or Mozilla Firefox.

Using this management method:

The GSW-1602SF/GSW-2404SF must have an Internet Protocol (IP) address accessible for the remote host. The screen

in Figure 3-1 appears.
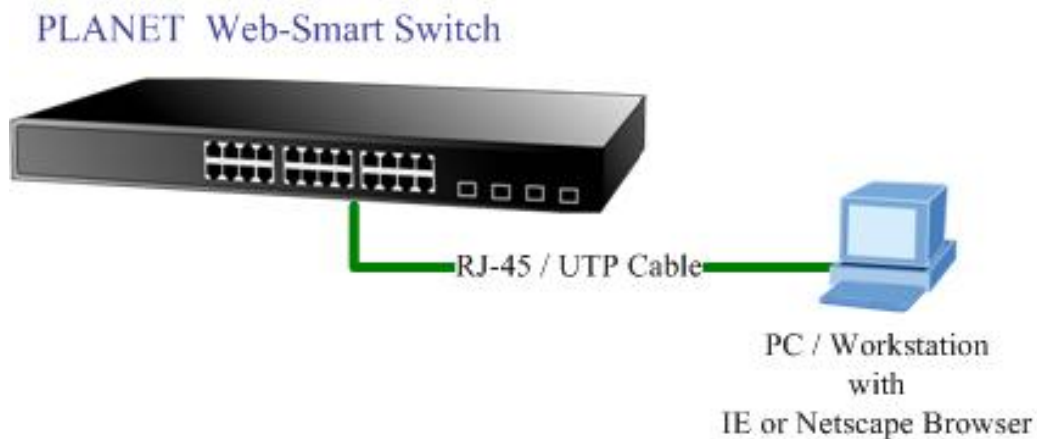
Figure 3-1 Web Management via Ethernet

3.2.2 PLANET Smart Discovery Utility

For easily list the GSW-1602SF/GSW-2404SF in your Ethernet environment, the Planet Smart Discovery Utility from user's

manual CD-ROM is an ideal solution.

The following install instructions guiding you for run the Planet Smart Discovery Utility.

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

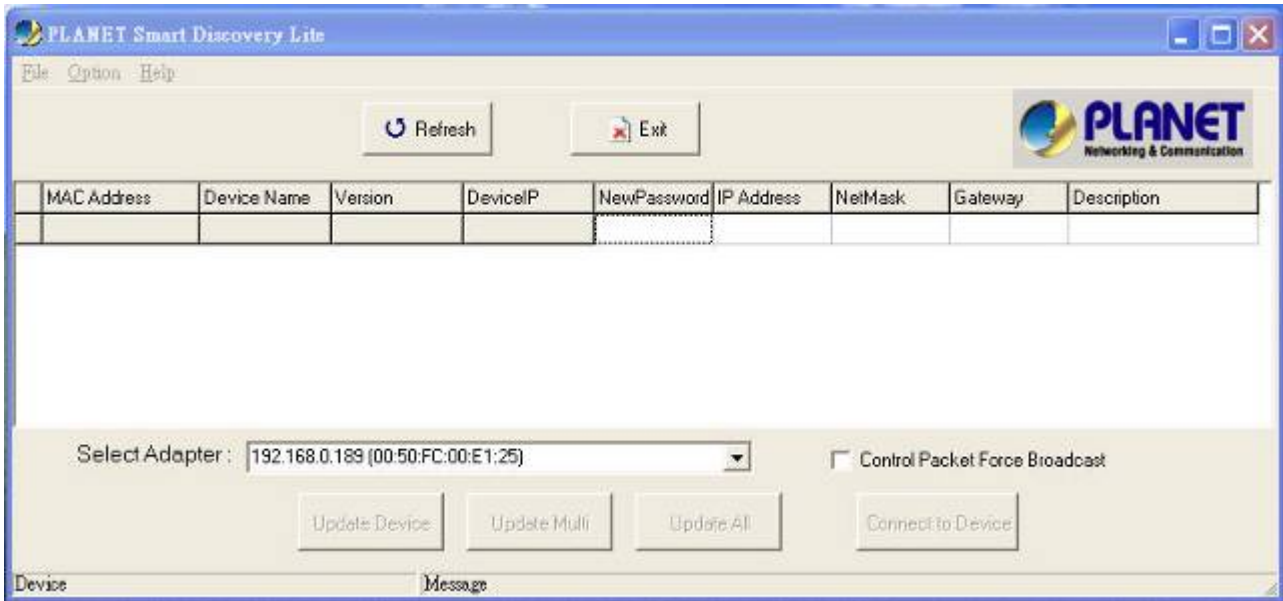2. Run this utility and the following screen appears.

Figure 3-2 Planet Smart Discovery Utility Screen

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

3. Press **"Refresh"** button for list current connected devices in the discovery list, the screen is shown as follow.
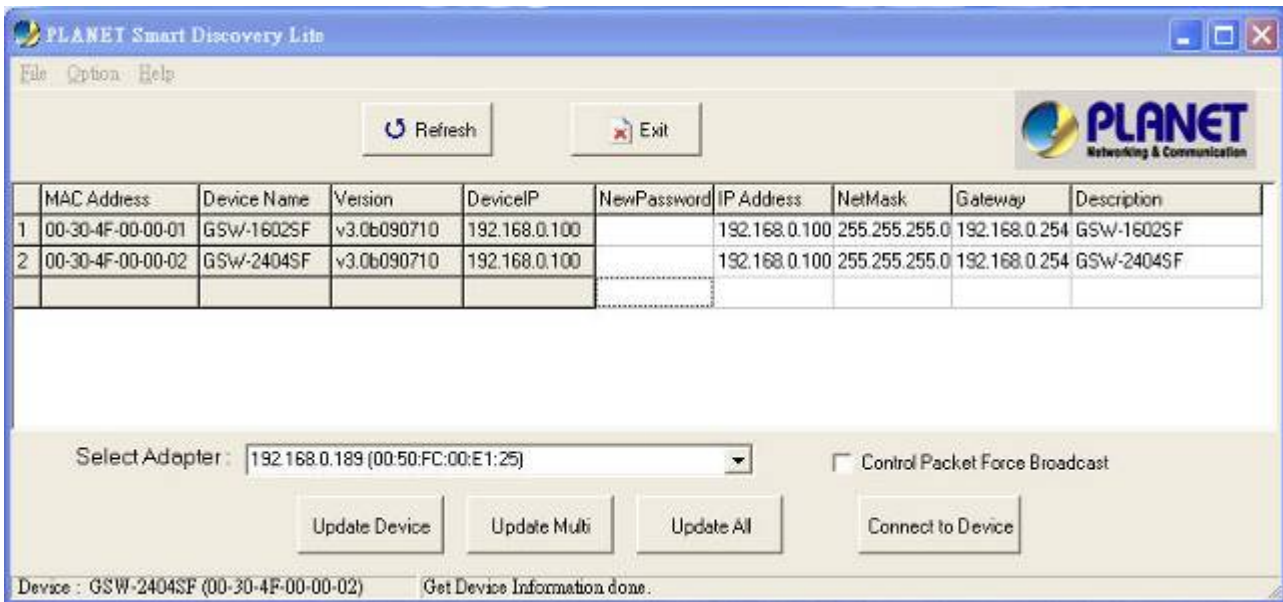
Figure 3-3 Planet Smart Discovery Utility Screen

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

2. After setup completed, press **"Update Device"**, **"Update Multi"** or **"Update All"** button to take affect. The meaning of the 3 buttons above are shown as 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 finding in **"Option"** tools bar.

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

4. Press **"Connect to Device"** button then the Web login screen appears in Figure 3-4.

5. Press **"Exit"** button to shutdown the planet Smart Discovery Utility.

3.2.3 Login the Switch

Before you start configure the GSW-1602SF/GSW-2404SF, please note the GSW-1602SF/GSW-2404SF is configured through an Ethernet connection, make sure the manager PC must be set on the same **IP subnet address**, for example, the default IP address of the Web Smart Gigabit Switch is *192.168.0.100* (the factory-default IP address), 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.

Use Internet Explorer 7.0 or above Web browser, enter default IP address *http://192.168.0.100*

To access the Web interface then the Web login screen appears in Figure 3-4 appears.

	The following screen based on GSW-2404SF, for GSW-1602SF the display will be the same to GSW-2404SF.

Figure 3-4 Web Login Screen of GSW-2404SF

After entering the password (default password is **"admin"**) in login screen (Figure 3-4 appears). The Web main screen appears as Figure 3-5.

Figure 3-5 Web Main Screen of GSW-2404SF

	1. For security reason, please change and memorize the new password after this first setup.
Note	2. Only accept command in lowercase letter under Web interface.

4. CONFIGURATION

The GSW-1602SF/GSW-2404SF Web Smart Gigabit Switch provide Web interface for Switch smart function configuration and make the Switch operate more effectively - They can be configured through the Web Browser. A network administrator can manage and monitor the GSW-1602SF /GSW-2404SF from the local LAN. This section indicates how to configure the Web Smart Gigabit Switch to enable its smart function.

Note	1. The following screen based on GSW-2404SF, for GSW-1602SF the display will be the same to GSW-2404SF.
	2. Recommend to use Web browser with Internet Explorer 7.0 and Firefox 3.0 or above for further management.

4.1 Main Menu

After a successful login, the main screen appears, the main screen displays the Switch status. The screen in Figure 4-1 appears.

Figure 4-1 Web Main Screen of GSW-2404SF

As listed at the left of the main screen, the configurable smart functions are shown as below:

◆ **System** – provide system Information, IP Configuration, User Authentication, Firmware Upgrade, Configuration Download, Configuration Upload, Factory Default and System Reboot. Explain in section 4.2.

◆ **SNMP** – provide System Configuration and System Information. Explain in section 4.3.

◆ **Port Management** – provide Port Configuration, Port Statistics Overview, Port Statistics Detail, SFP Module Information and Port Mirror Configuration. Explain in section 4.4.

◆ **Link Aggregation** – provide Static Aggregation, LACP Port Configuration, LACP System Status and LACP Port Status. Explain in section 4.5.

◆ **VLAN** – provide VLAN Basic Information, VLAN Port Configuration and VLAN Membership. Explain in section 4.6.

◆ **Rapid Spanning Tree –** provide System Configuration, Port Configuration and Port Status. Explain in section 4.7.

◆ **Multicast** – provide IGMP Snooping Configuration, IGMP Snooping Status and Multicast Address Table. Explain in section 4.8.

◆ **Quality of Service** – provide QoS Configuration and Storm Control Configuration. Explain in section 4.9.

◆ **802.1X Authentication –** provide 802.1X System Configuration and 802.1X Port Configuration. Explain in section 4.10.

◆ **Filter Configuration** – per port traffic filter based on IP address. Explain in section 4.11.

◆ **MAC Address Table** – provide Aging Time Configuration, Static MAC Address Configuration and Dynamic MAC Address Table. Explain in section 4.12.

◆ **Diagnostics** – provide Ping Parameters and Cable Diagnostics. Explain in section 4.13.

◆ **LLDP** – provide LLDP Configuration, LLDP Neighbor Table and LLDP Statistics. Explain in section 4.14.

◆ **Green Networking** – provide Green Networking Configuration for energy saving. Explain in section 4.15.

◆ **Logout** – provide Logout function of Web Smart Gigabit Switch. Explain in section 4.16.

4.2 System

4.2.1 System Information

The System Information page provides information for the current device information. System Information page helps a switch manager to identify the versions, MAC Address and IP Subnet Address etc. The screen in Figure 4-2 appears.
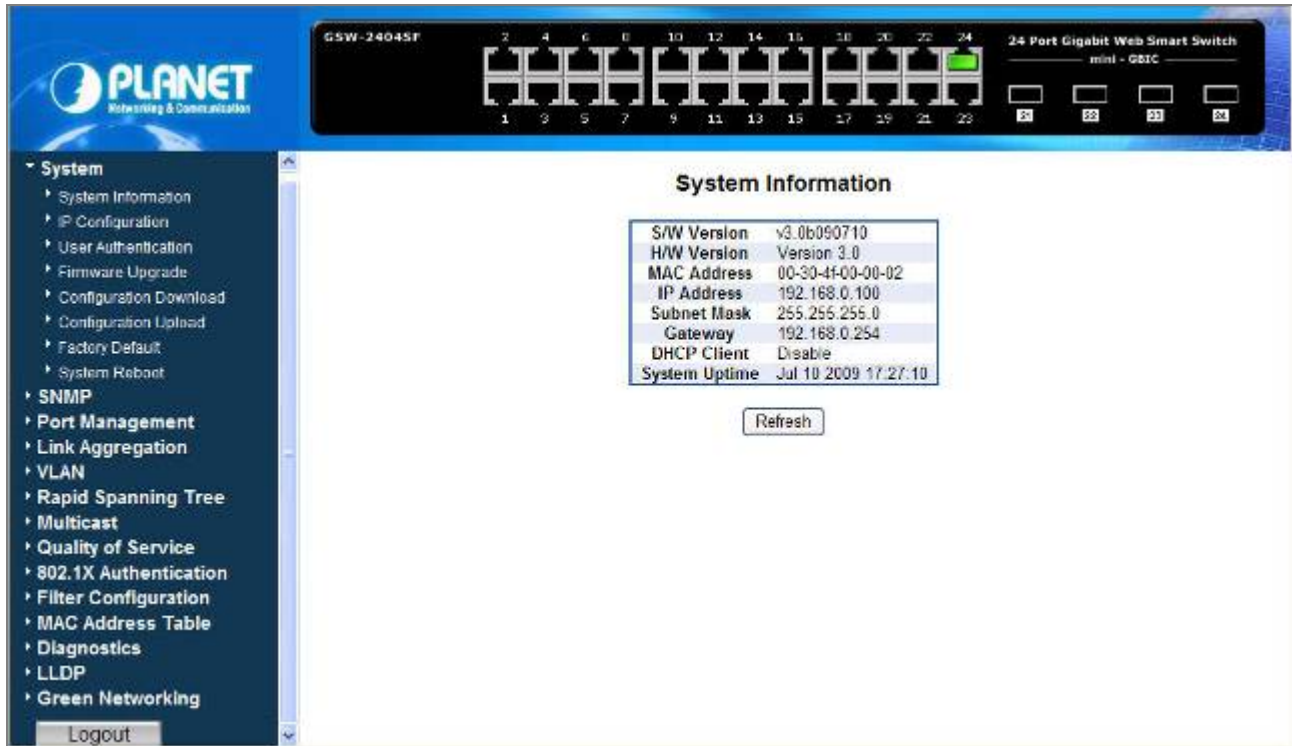

Figure 4-2 System Information screen

The page includes the following fields; see the **table 4-1** description of the system information.

• Item	Description
S/W Version	The current firmware version running on the device.
H/W Version	The current hardware version of the device
MAC Address	Display the device MAC address.
IP Address	The current IP Address of the device. The IP Address could be manual assigned or get via **DHCP** server.
Subnet Mask	The current IP Subnet Mask setting on the device.
Gateway	The current Gateway of the device.
DHCP Client	If the IP address is got and assigned via a **DHCP** server, the field shows the IP Address of the **DHCP** Client.
System Uptime	Display the firmware made time of the device.
Refresh button	Press this button to refresh current web page.

Table 4-1 Description of the system information

4.2.2 IP Configuration

The IP Configuration includes the DHCP Client, IP Subnet Address and Management VLAN Setting. The screen in Figure 4-3 appears.
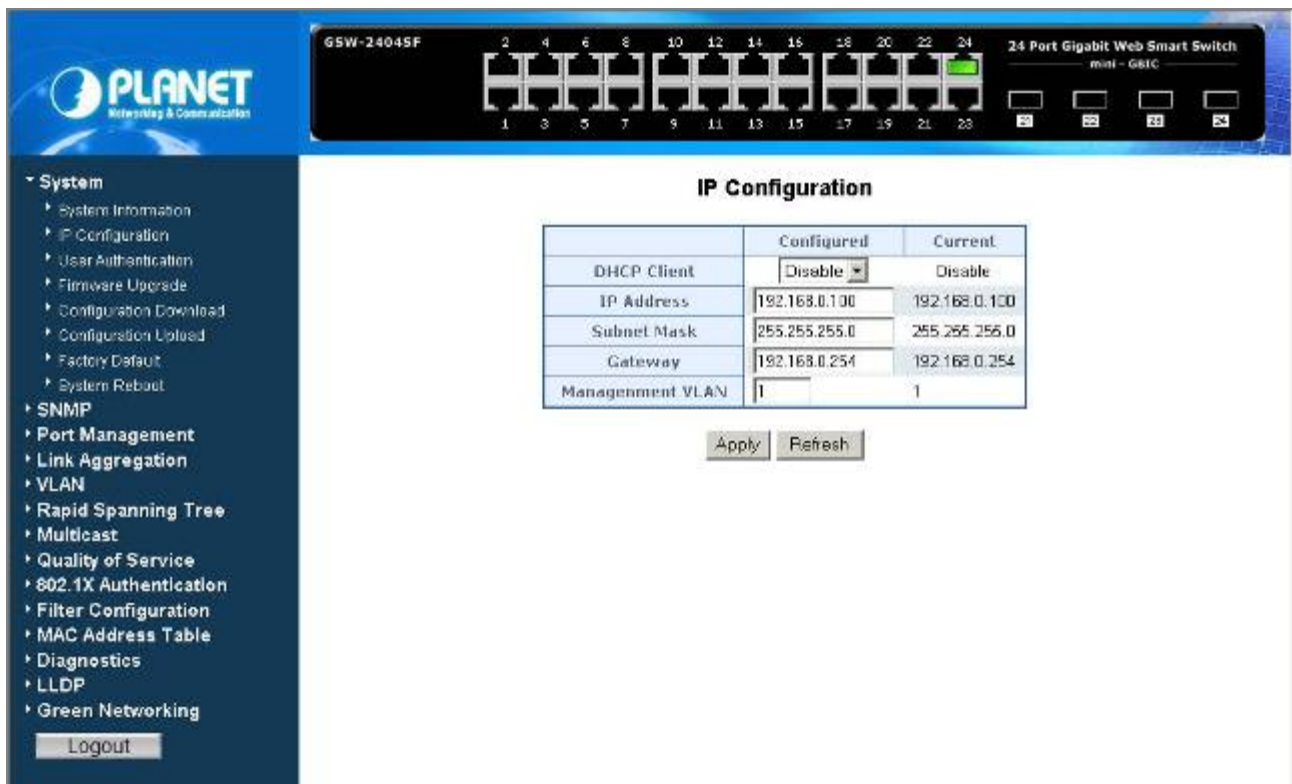

Figure 4-3 IP Configuration screen

The page includes the following configurable data; see the **table 4-2** description of the IP Configuration.

Item	Description
Configured	
DHCP Client	Choose what the Web Smart Gigabit Switch should do following power-up: transmit a **DHCP** request, or manual setting (Disable). The factory default is **"Disable"**.
IP Address	The IP address of the Web Smart Gigabit Switch. The factory default value is **192.168.0.100**
Subnet Mask	The IP subnet mask for the Web Smart Gigabit Switch. The factory default value is **255.255.255.0**
Gateway -	The default gateway for the Web Smart Gigabit Switch. The factory default value is **192.168.0.254**
Management VLAN	Specifies the management VLAN ID of the Web Smart Gigabit Switch. It may be configured to any value in the range of **1 to 4094**. The management VLAN is used for management of the Web Smart Gigabit Switch.
Current	
DHCP Client	Display current DHCP Client Status, Disable or Enable.

IP Address	Display current IP address of the Web Smart Gigabit Switch.
Subnet Mask	Display current IP subnet mask for the Web Smart Gigabit Switch.
Gateway	Display current gateway for the Web Smart Gigabit Switch.
Management VLAN	Display current management VLAN ID of the Web Smart Gigabit Switch.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch and system will reboot for take affect.
Refresh	Press this button for refresh IP Configuration screen of Web Smart Gigabit Switch.

Table 4-2 Description of the IP Configuration

4.2.3 User Authentication

The User Authentication provides change default password to another new password. The screens in Figure 4-4 & Figure 4-5 appears.
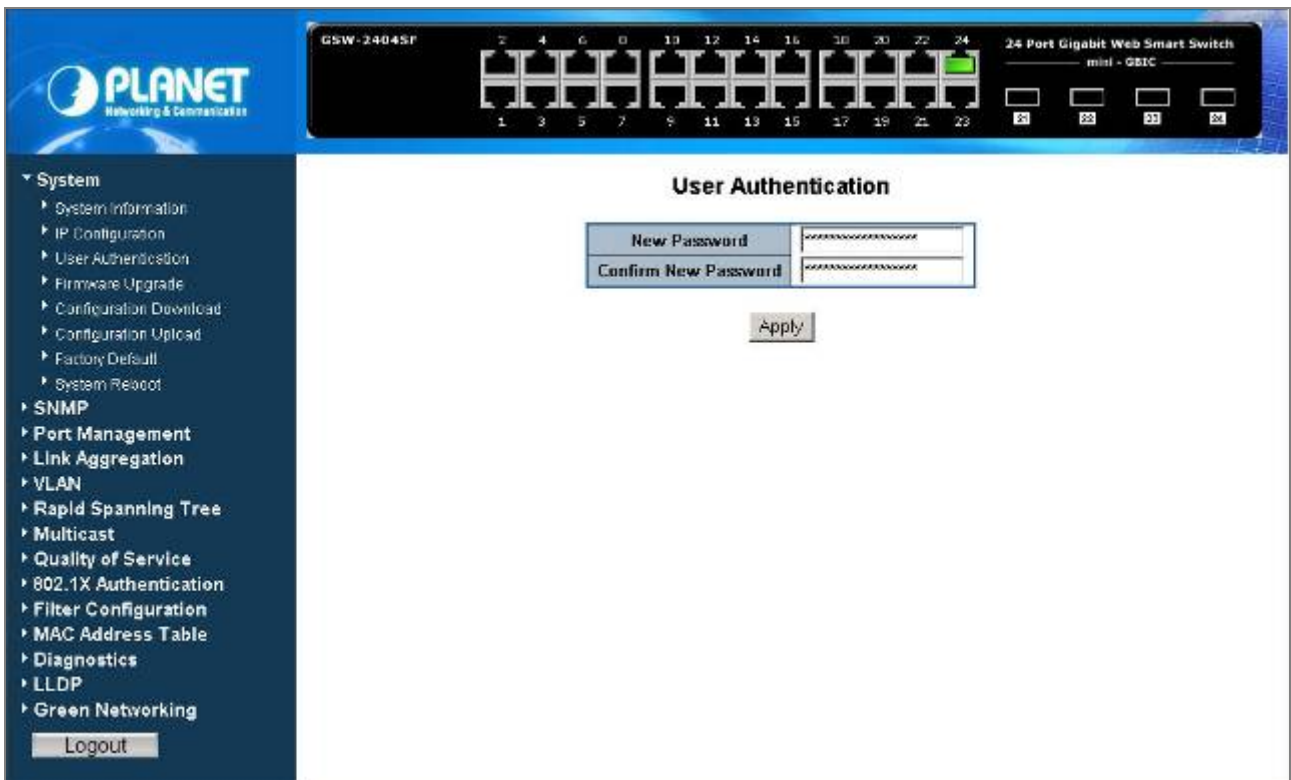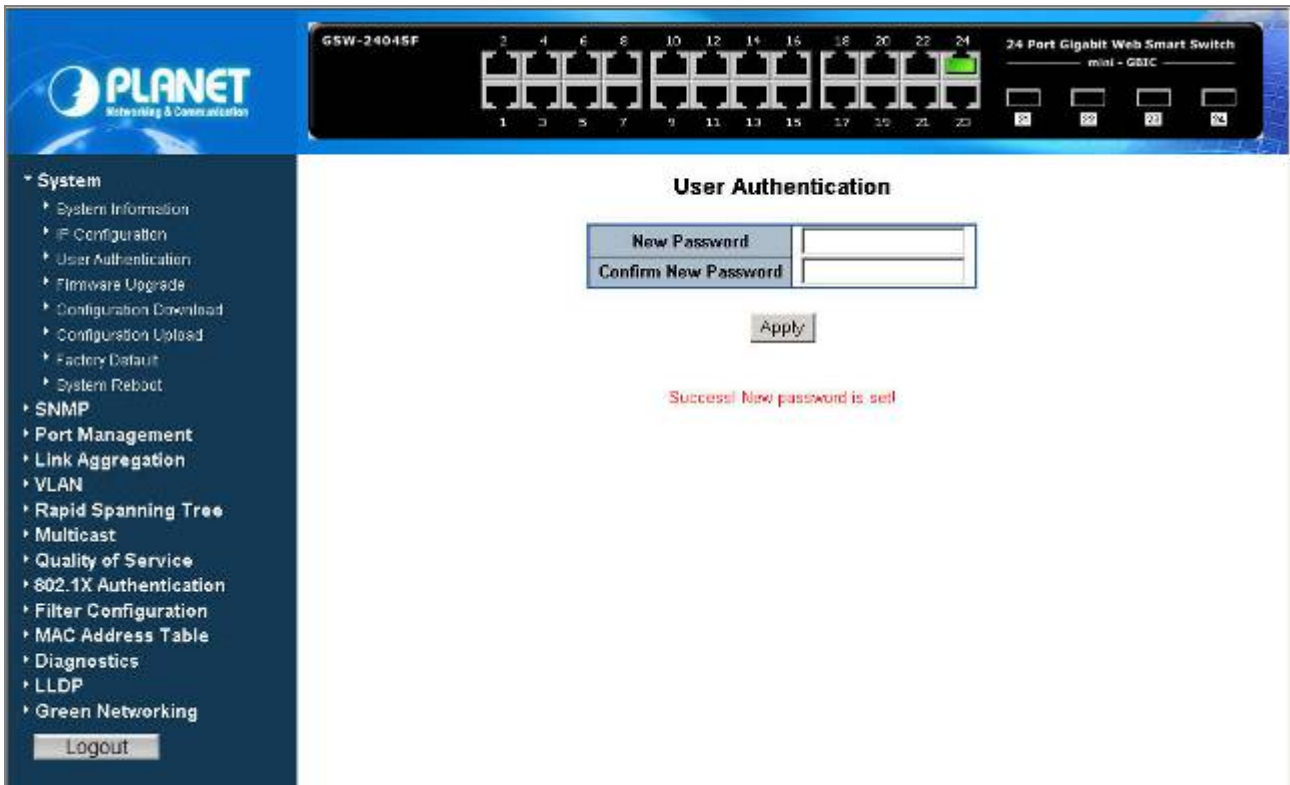

Figure 4-4 User Authentication screen

Figure 4-5 User Authentication screen

Note	Up to 16 characters is allowed for the new password assign.

4.2.4 Firmware Upgrade

This section provides firmware upgrade of the Web Smart Gigabit Switch, the screen in Figure 4-6 appears.
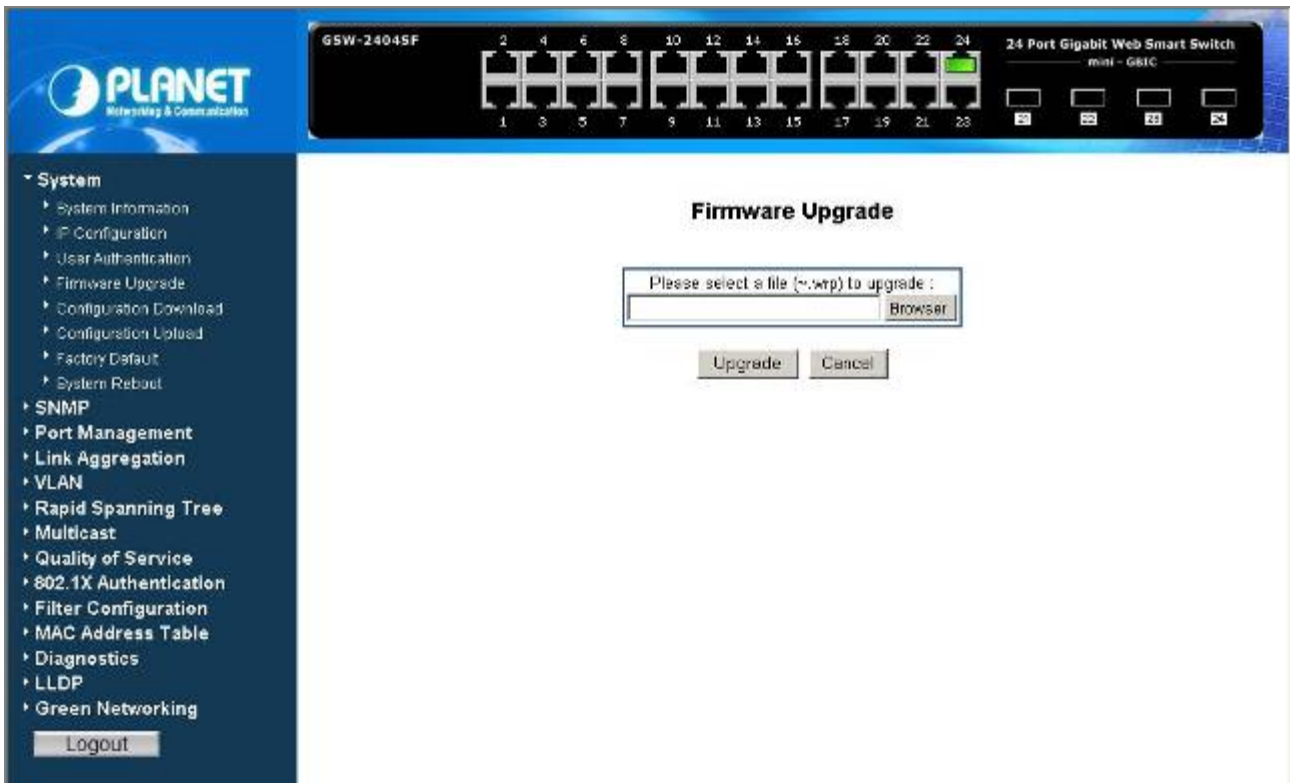
Figure 4-6 Firmware Upgrade screen

Press **"Browser"** button to find the firmware location administrator PC, the screen in Figure 4-7 appears.
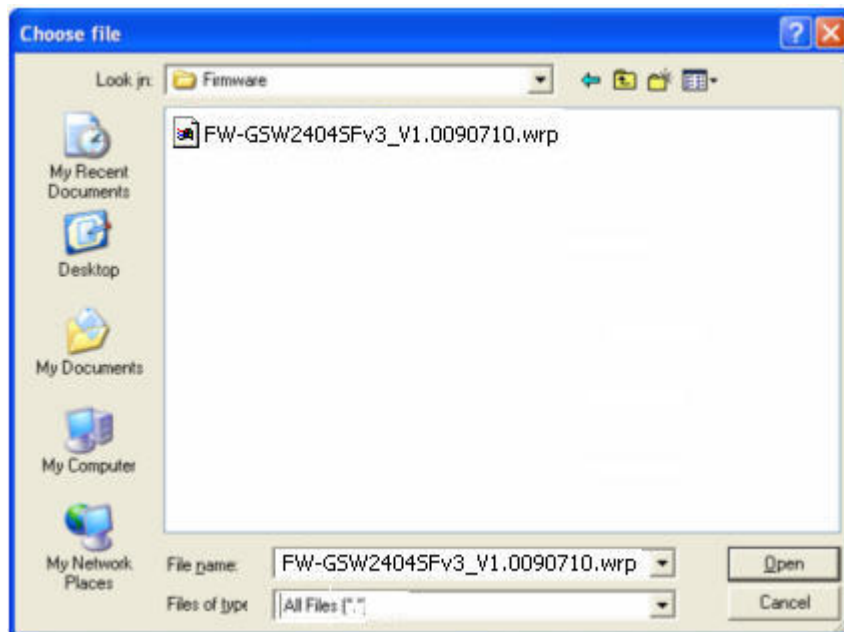
Figure 4-7 Firmware Upgrade screen

After find the firmware location from administrator PC, press "Upgrade" button to start the firmware upgrade process. The screen in Figure 4-8 & 4-9 appears.
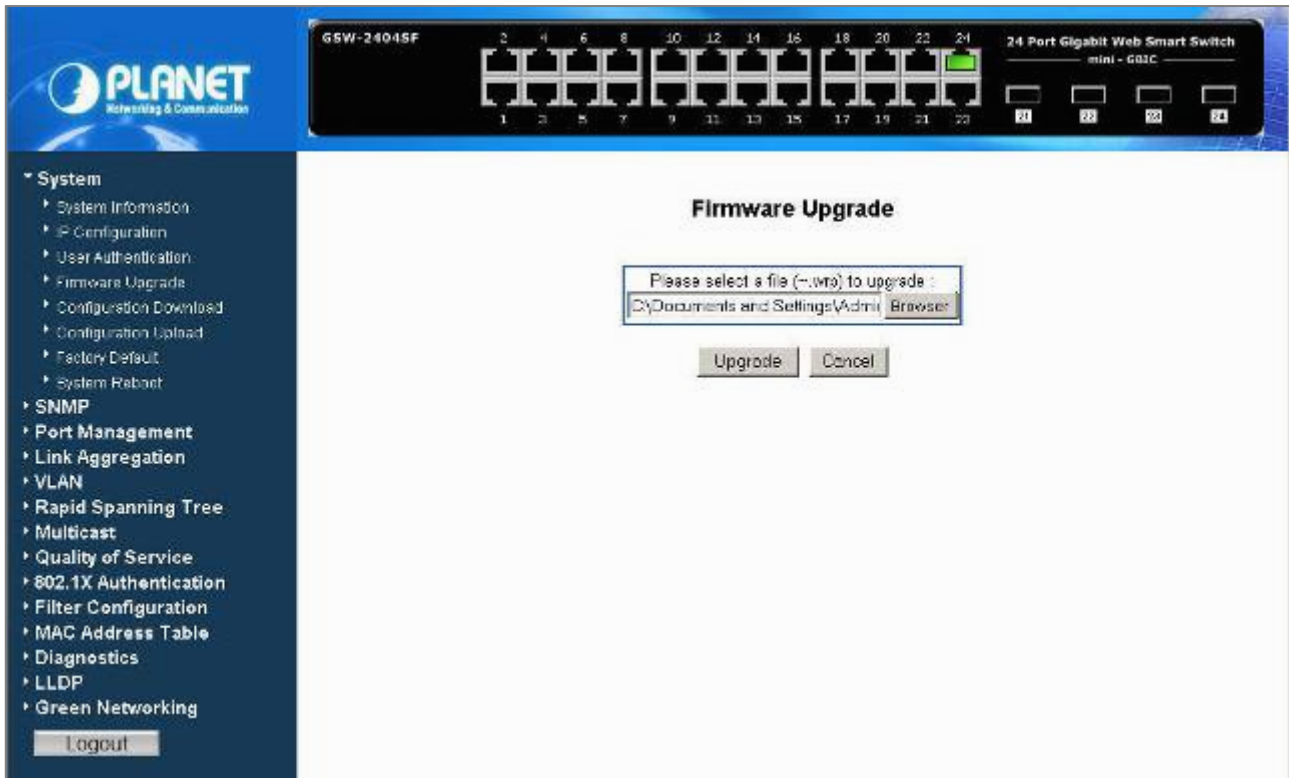
Figure 4-8 Firmware Upgrade screen
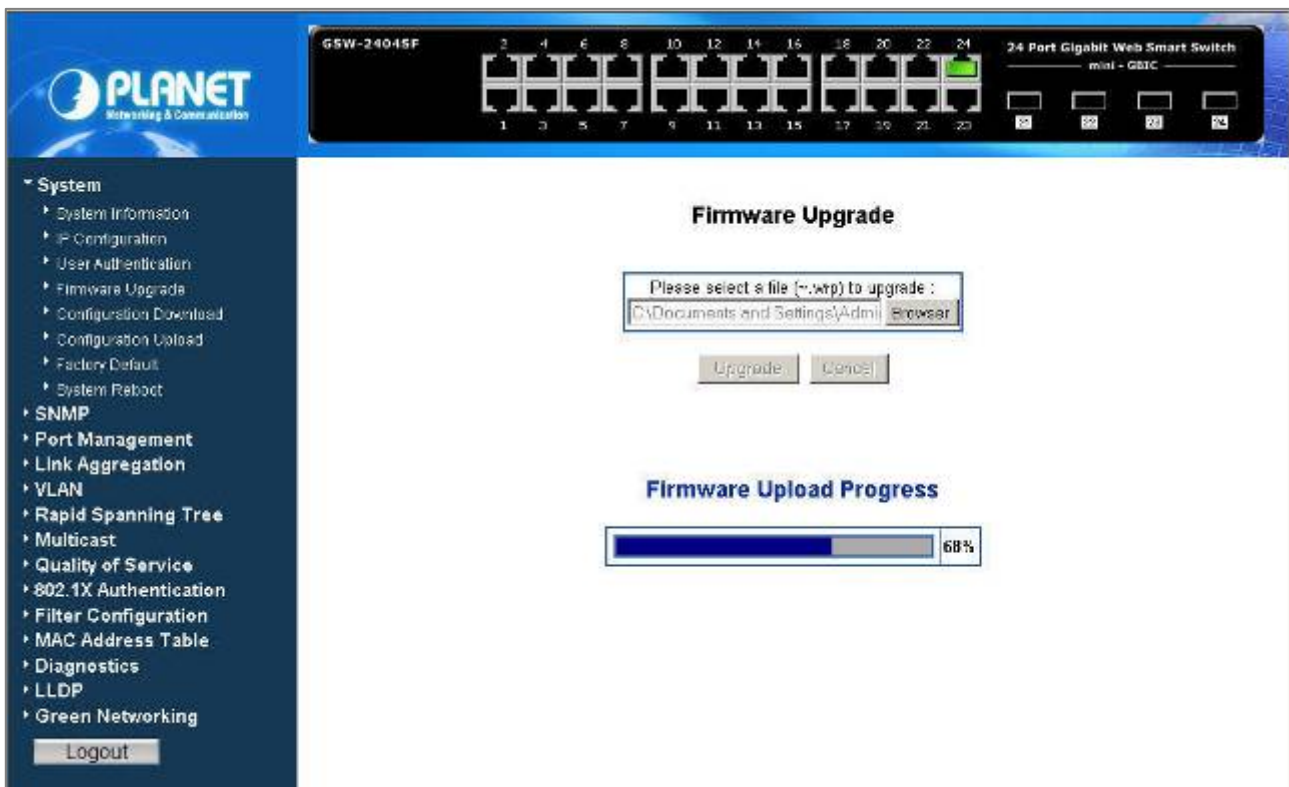
Figure 4-9 Firmware Upgrade screen

Once the software be loaded to the system successfully. The following screen appears. Click the "**Yes**" button to activate the new software immediately. The system will load the new software after reboot. The screen in Figure 4-10 & 4-11 appears.
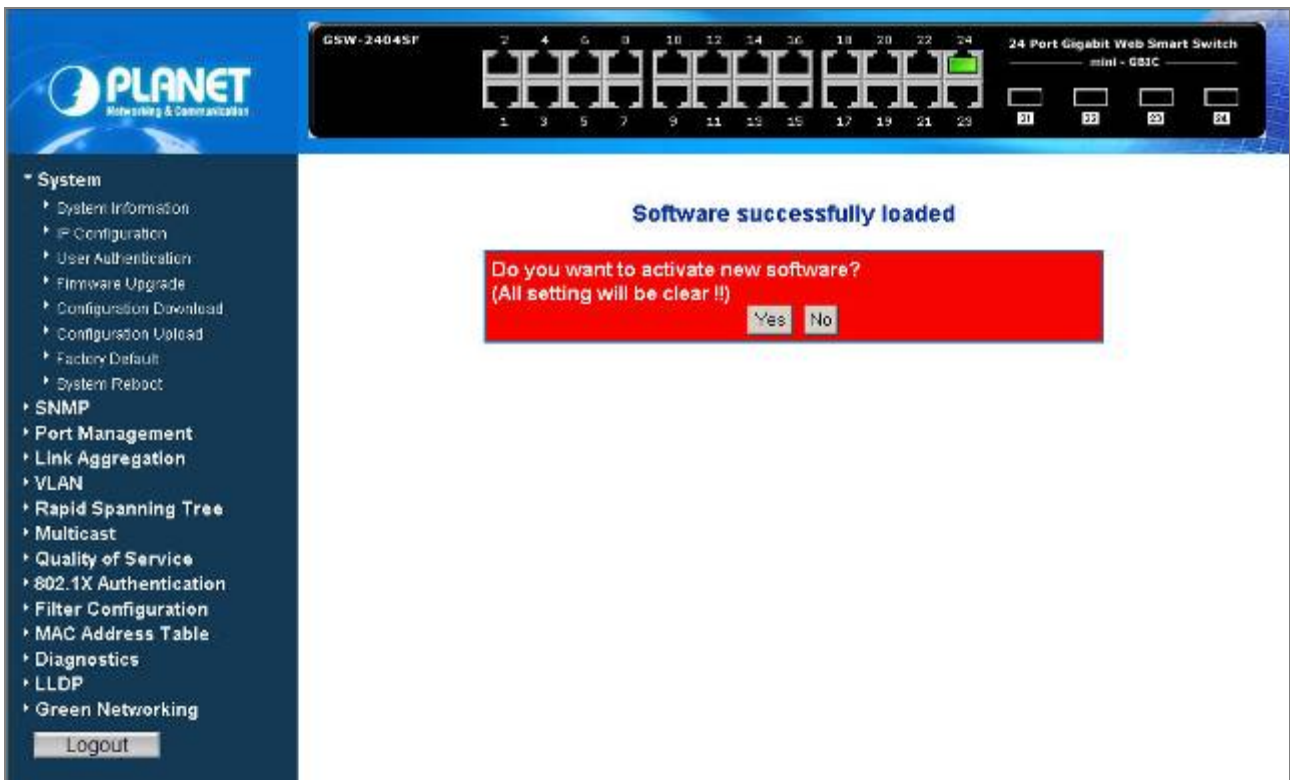
Figure 4-10 Firmware Upgrade Successfully screen

Figure 4-11 Firmware Upgrade Reboot screen

Please wait for a while for system reboot. After device reboot then can use the latest firmware of the Web Smart Gigabit Switch.

Figure 4-12 Web login screen of Web Smart Gigabit Switch

	Strong recommend not to power off the Web Smart Gigabit Switch during firmware upgrade process.
Note	

4.2.5 Configuration Download

This section provides Configuration Download of the Web Smart Gigabit Switch, the screen in Figure 4-13 appears.
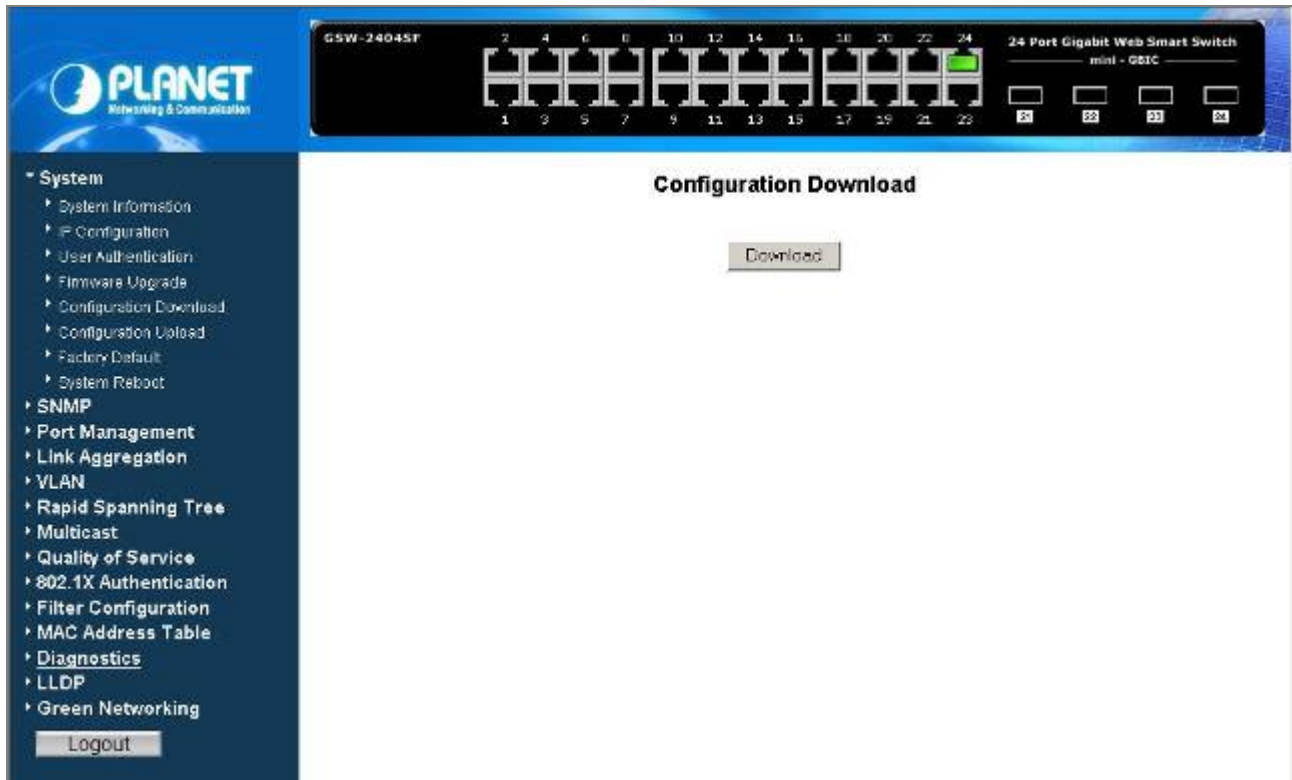
Figure 4-13 Configuration Download screen

Press **"Download"** button to download and save the backup configuration file into the location of administrator PC.

The screen in Figure 4-14 & 4-15 appears.
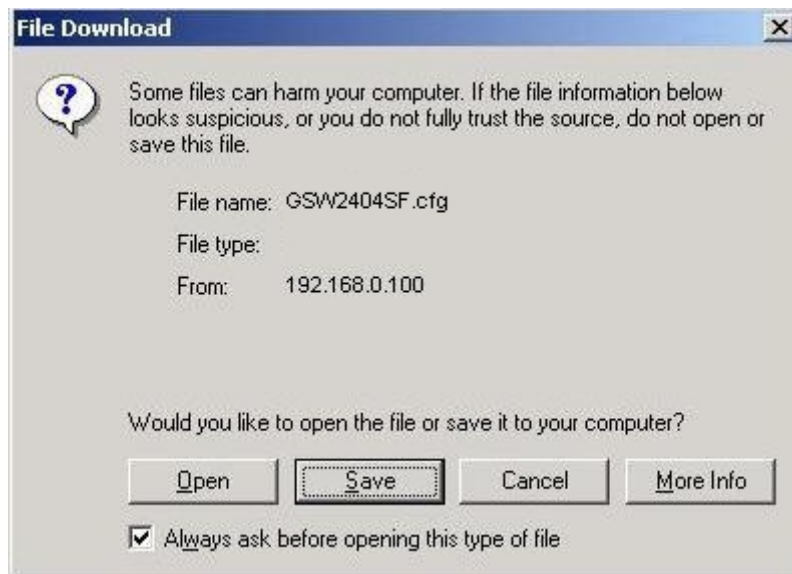
Figure 4-14 Configuration Download screen
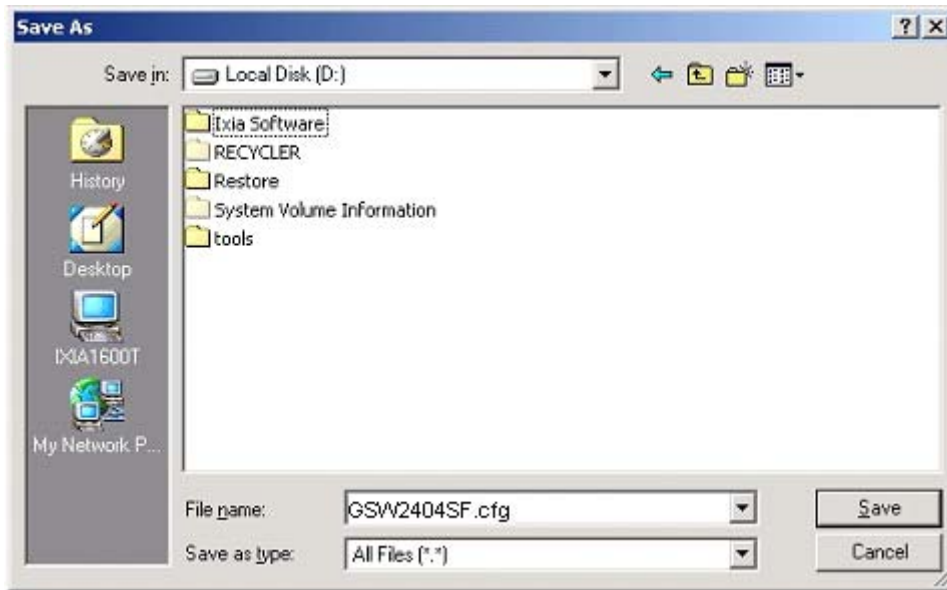
Figure 4-15 Configuration Download screen

Recommend to use Web browser with Internet Explorer 7.0 and Firefox 3.0 or above for configuration Download function.

4.2.6 Configuration Upload

This section provides Configuration Upload of the Web Smart Gigabit Switch, the screen in Figure 4-16 appears.
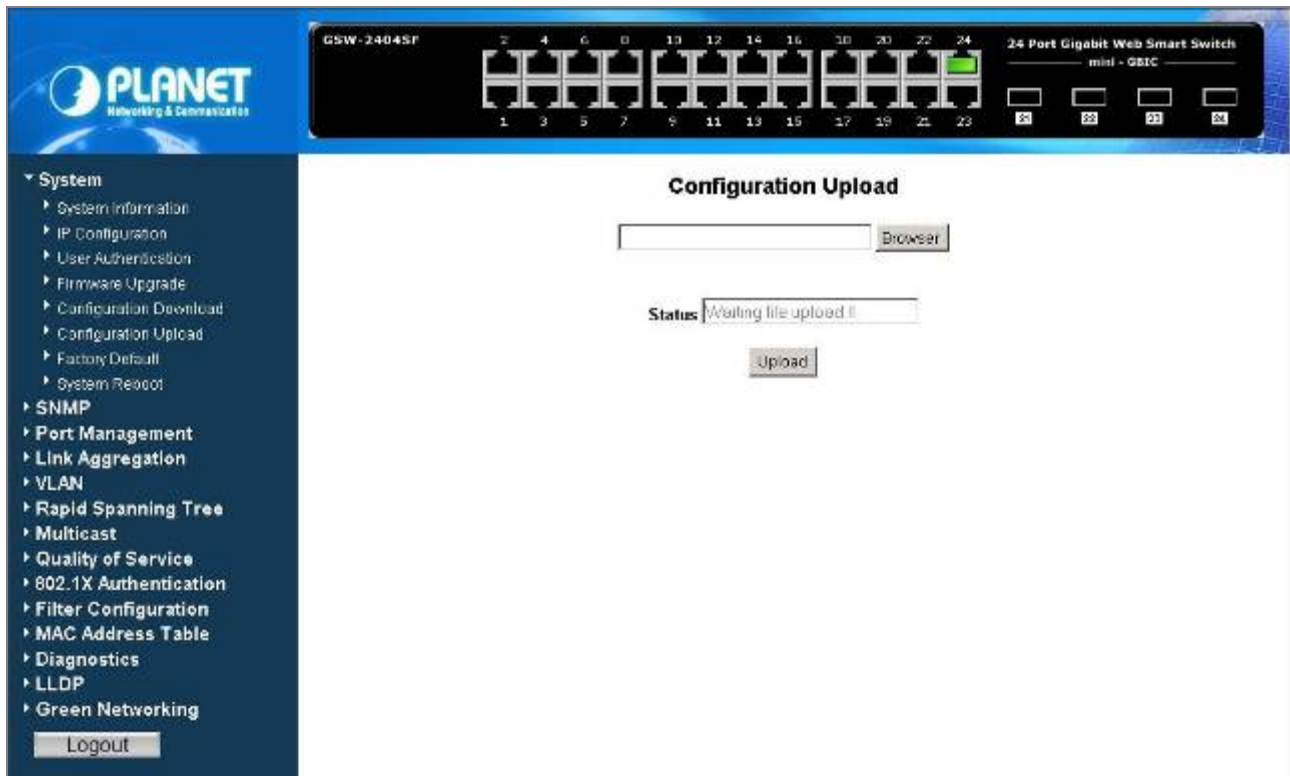
Figure 4-16 Configuration Upload screen

Press **"Browser"** button to find the backup configuration file location of administrator PC, the screen in Figure 4-17 appears.
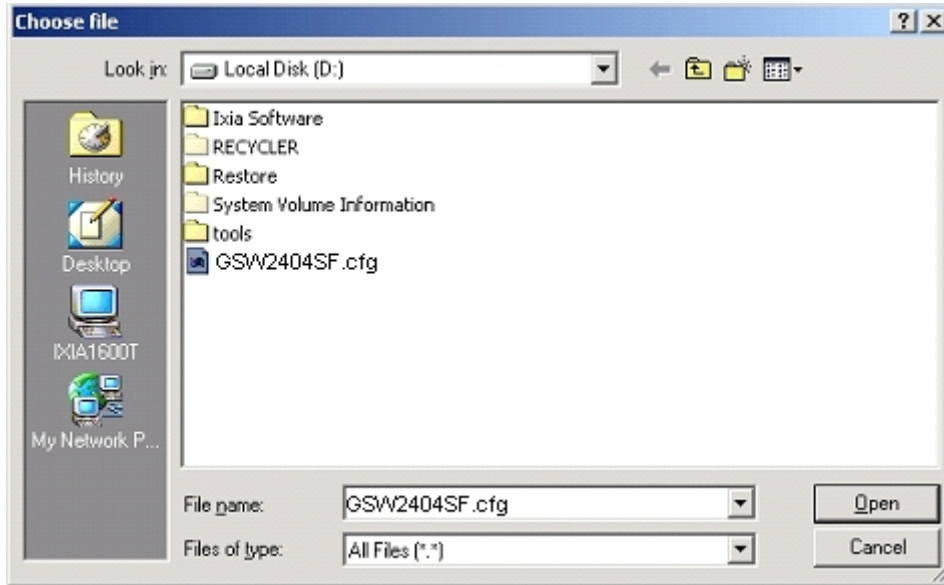
Figure 4-17 Configuration Upload screen

After find the backup configuration file location from administrator PC. The screen in Figure 4-18 appears.
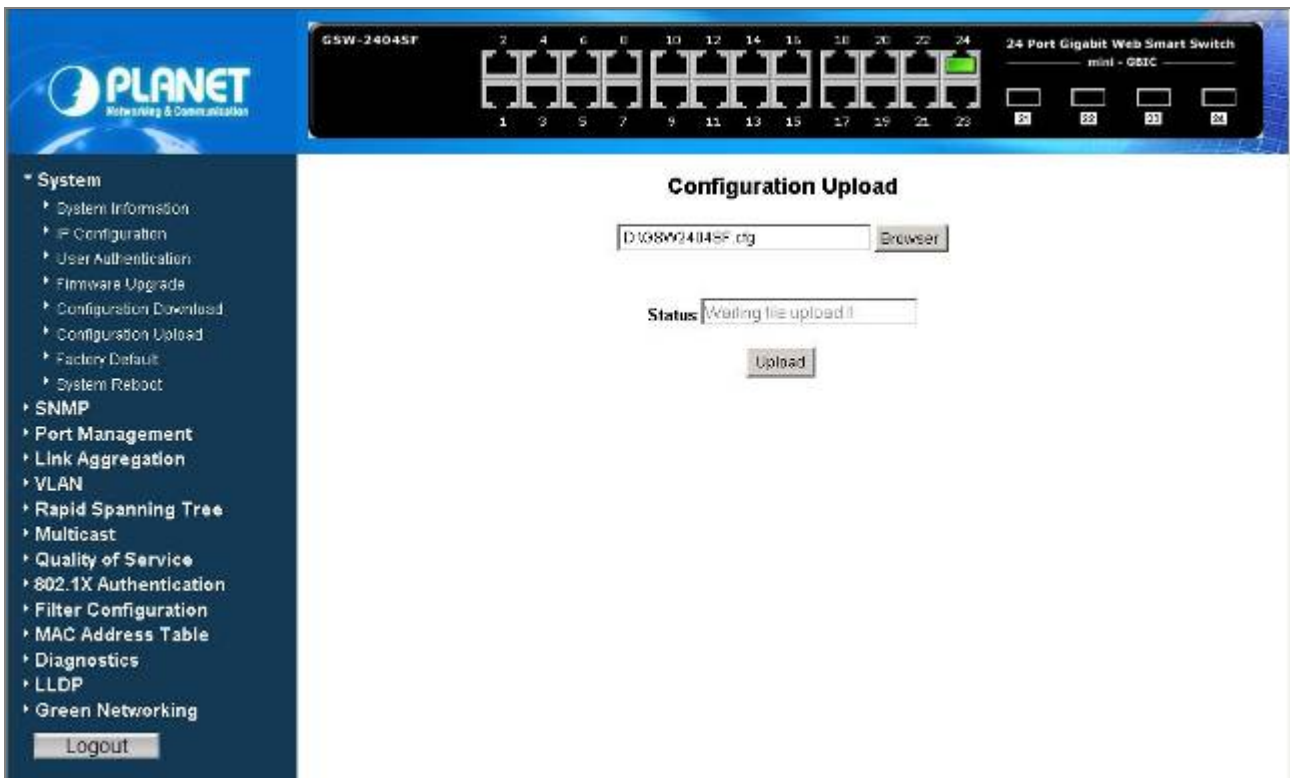
Figure 4-18 Configuration Upload screen

Press **"Upload"** button to start the Configuration Upload process, and wait for 90 seconds for complete Configuration Upload process. The screen in Figure 4-19 & 4-20 appears.
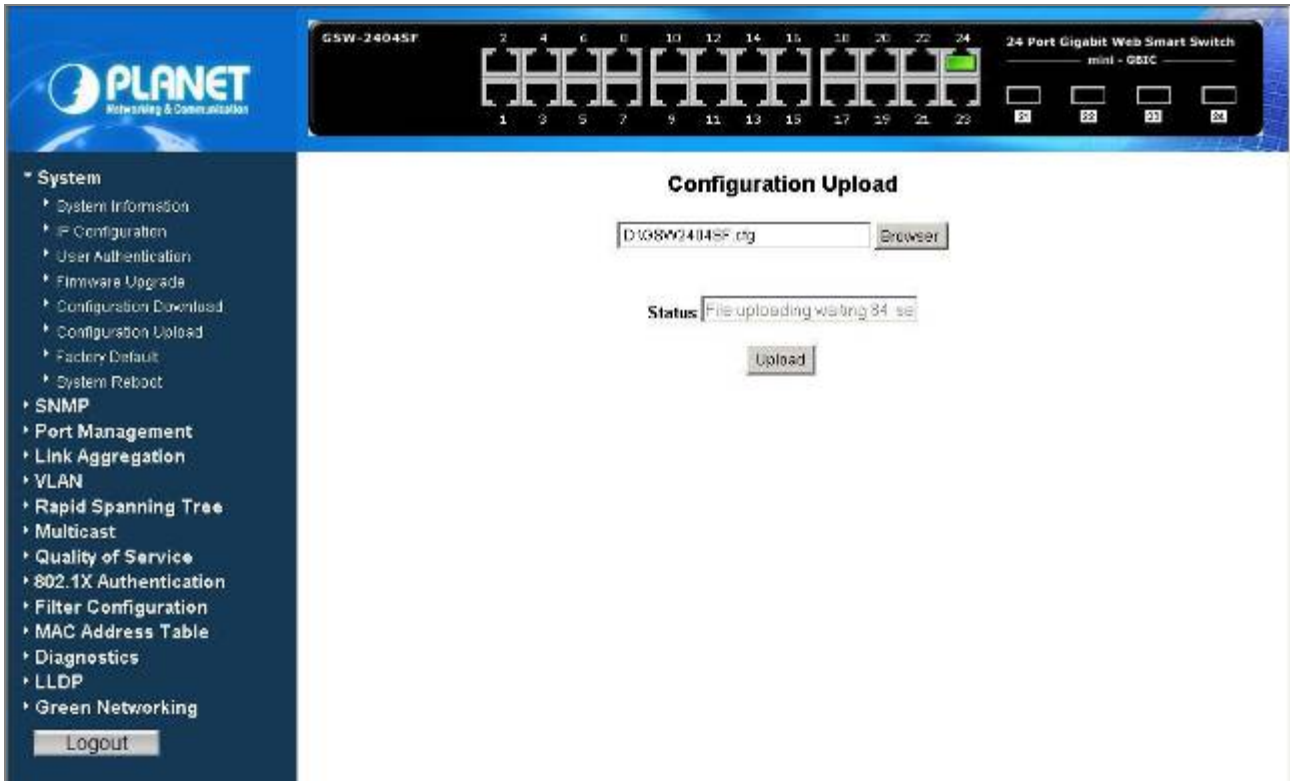
Figure 4-19 Configuration Upload screen
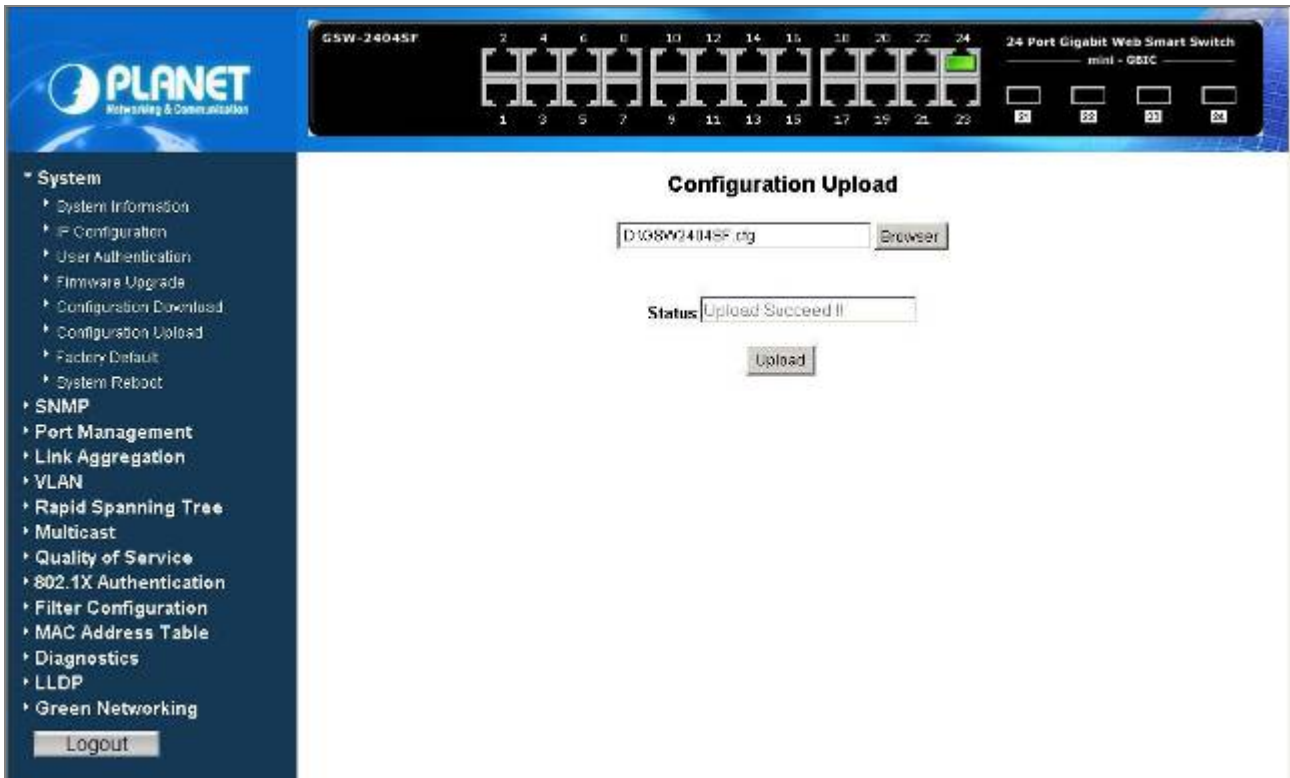
Figure 4-20 Configuration Upload screen

Please refresh current Web page of Web Smart Gigabit Switch and following screen appears in Figure 4-21.
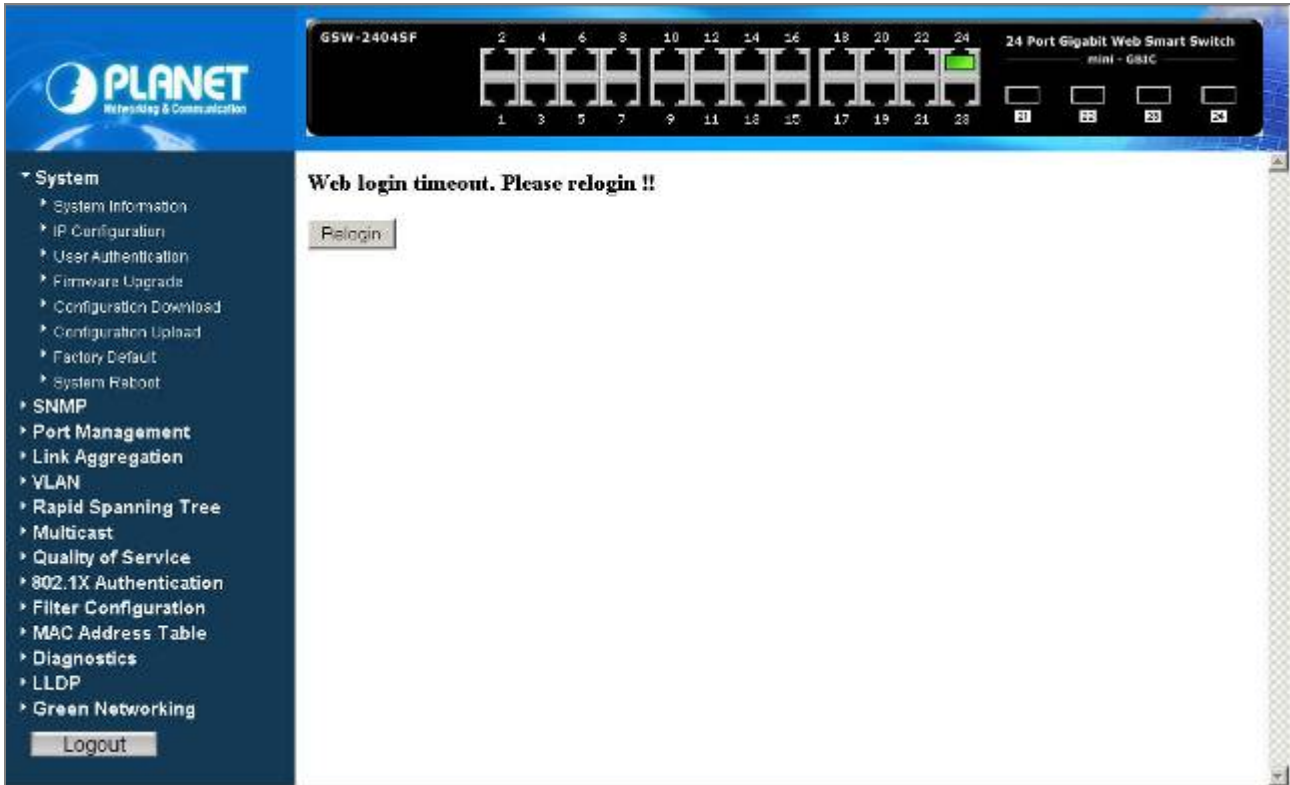
Figure 4-21 Configuration Upload screen

Please re-Login the Web interface of Web Smart Gigabit Switch for exist configuration application.

Note	Recommend to use Web browser with Internet Explorer 7.0 and Firefox 3.0 or above for configuration Upload function.

4.2.7 Factory Default

This section provides Factory Default function of the Web Smart Gigabit Switch, the screen in Figure 4-22 appears.
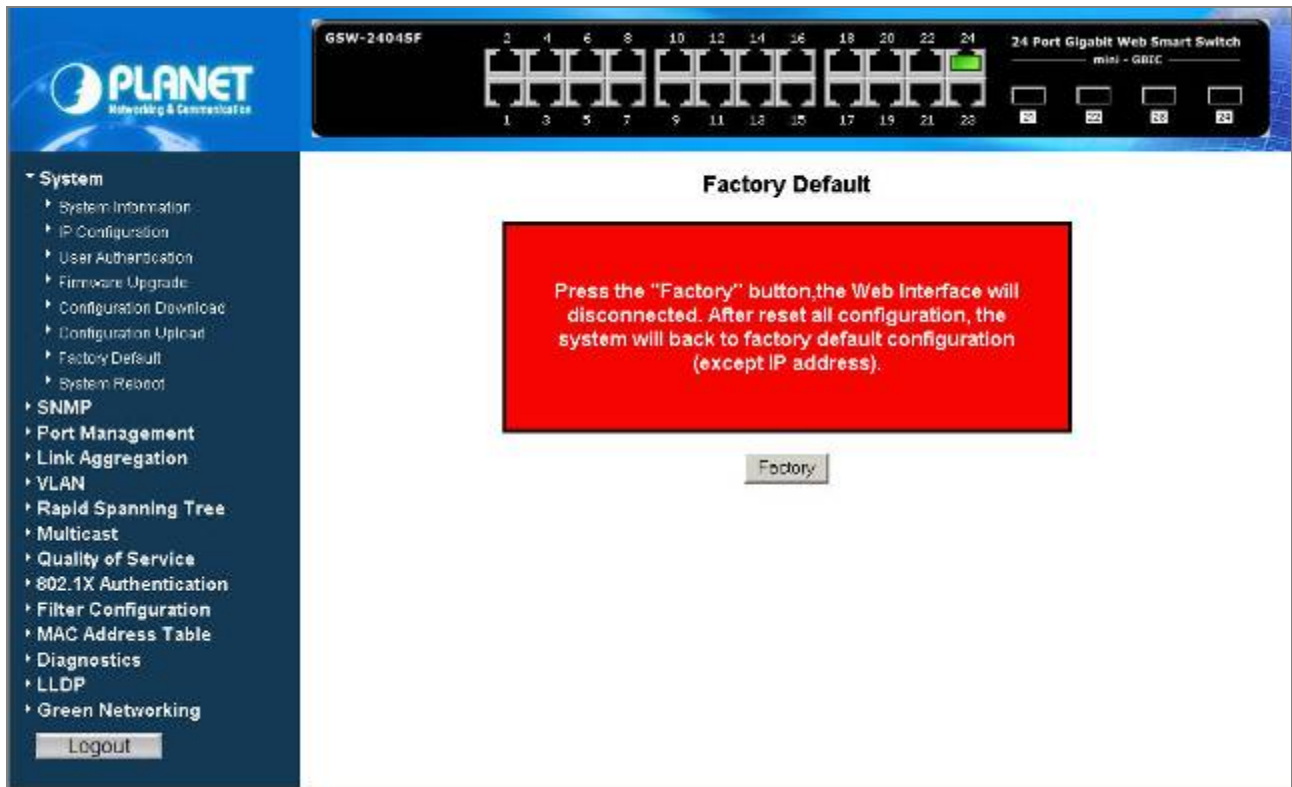
Figure 4-22 Factory Default screen

Press **"Factory"** Button for start the factory default process of Web Smart Gigabit Switch, the screen in Figure 4-23 appears.

Figure 4-23 Factory Default screen

Please wait for 24 seconds for complete Factory Default process. The Web main screen in Figure 4-24 appears.

Figure 4-24 Web Main screen

4.2.8 Reboot

This section provides Reboot function of the Web Smart Gigabit Switch, the screen in appears.
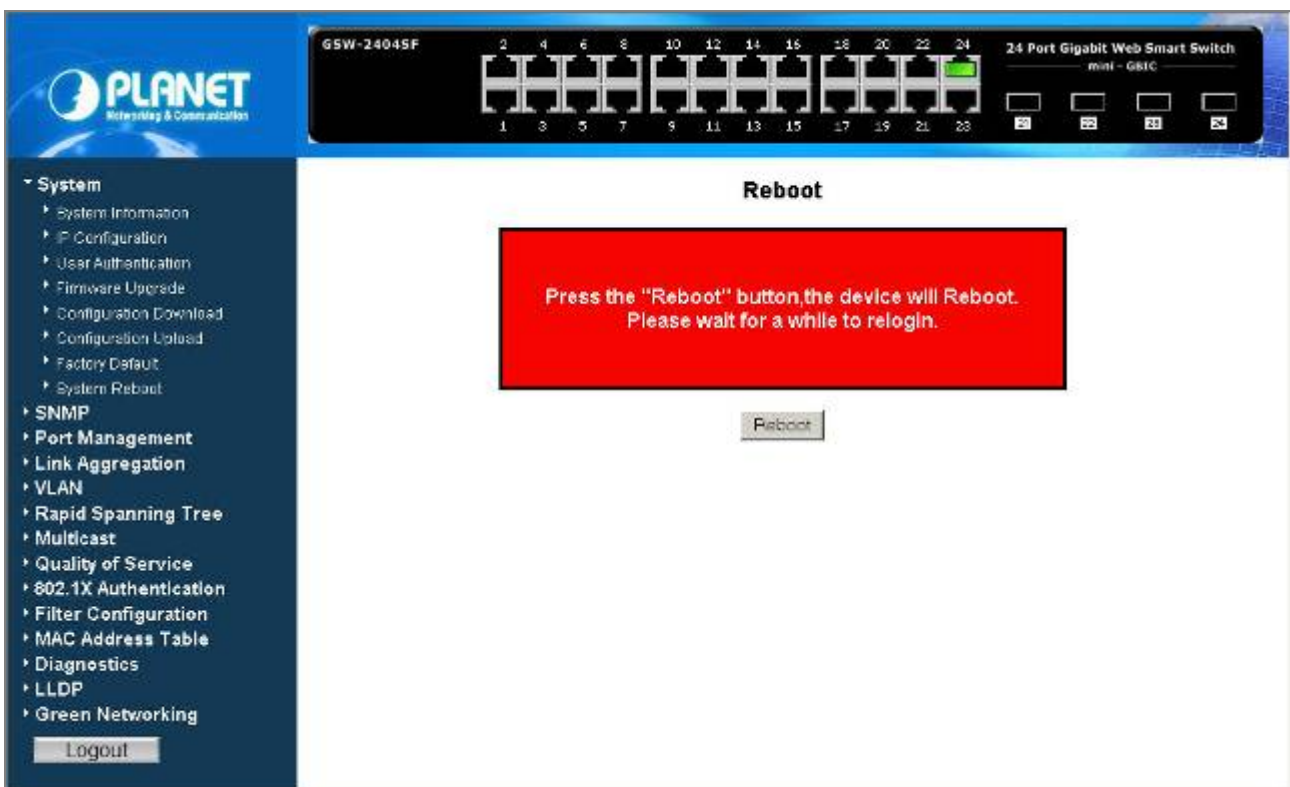
Figure 4-25 Reboot screen

Press **"Reboot"** Button for start the Reboot process of Web Smart Gigabit Switch, the screen in Figure 4-26 appears.

System Reboot will take a couple of seconds...

Waiting 1 0

Figure 4-26 Reboot screen

Please wait for 25 seconds for complete Reboot process. The Web login screen will appears, please login the Web Smart Gigabit Switch for further application.

4.3 SNMP

4.3.1 Theory

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

4.3.2 System Configuration

The SNMP System Configuration page provides SNMP parameters. SNMP System Configuration page helps a switch manager to configure SNMP functions. The screen in Figure 4-27 appears.
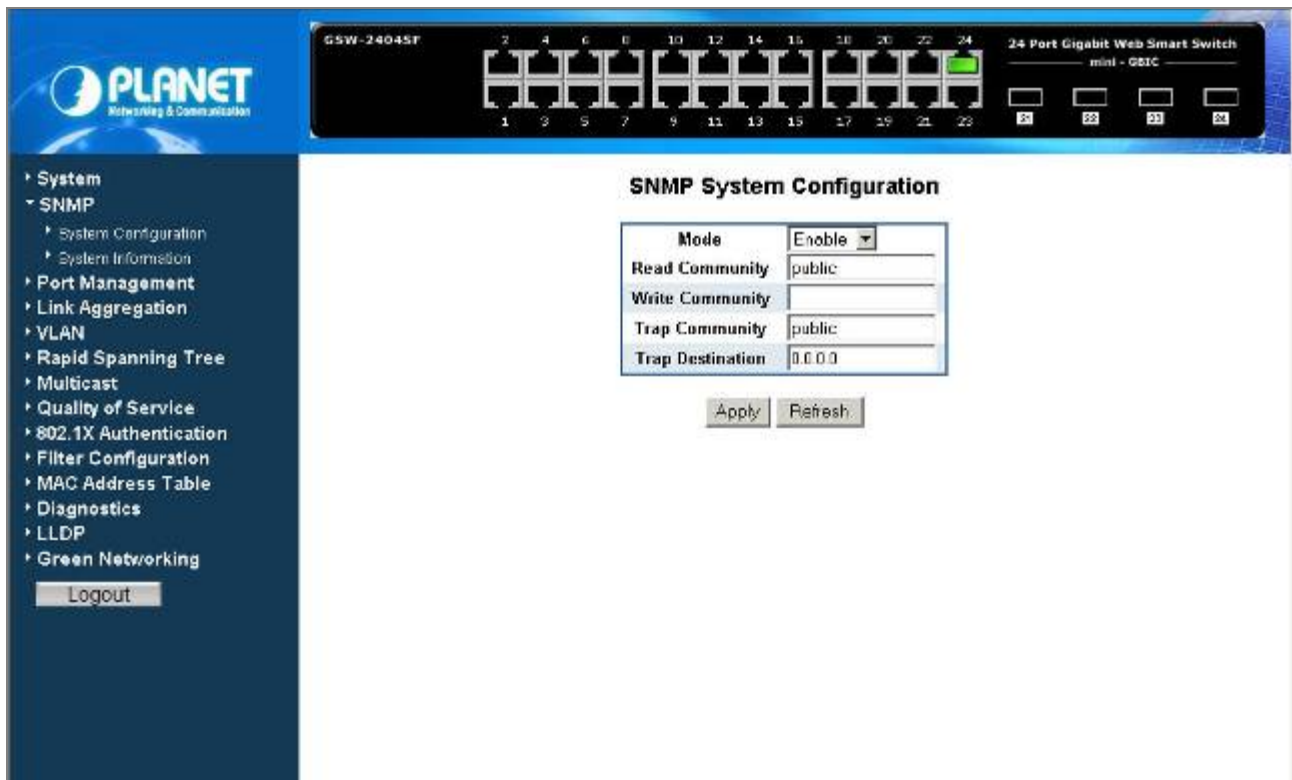
Figure 4-27 SNMP System Configuration screen

The page includes the following configurable data; see the **table 4-3** description of the SNMP System Configuration.

Item	Description
Mode	Enable or Disable the **SNMP** function of the device. While set to enable, the manager could remotely get the interface status and received the traps information. Default mode is **Enable**.
Read Community	Functions as a password and used to authenticate the access right of the device. The Read Community is restricted to read-only, for all MIBs except the community table, for which there is no access. Up to 8 characters is allowed.
Write Community	Functions as a password and used to authenticate the access right of the device. The Write Community accesses the device both read and write - configure to the device via **SNMP**. Up to 8 characters is allowed.
Trap Community	Identifies the community string of the trap manager. Up to 8 characters is allowed.
Trap Destination	The Trap function enables the Switch to monitor the Trap through the SNMP software, set the Trap IP Address of the manager workstation where the trap to be sent
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh System Configuration screen of Web Smart Gigabit Switch.

Table 4-3 Description of the SNMP System Configuration

4.3.3 System Information

The System Information page provides information input for the current device information. System Information page helps a switch manager to define System Name, System Contact and System Location. The screen in Figure 4-28 appears.
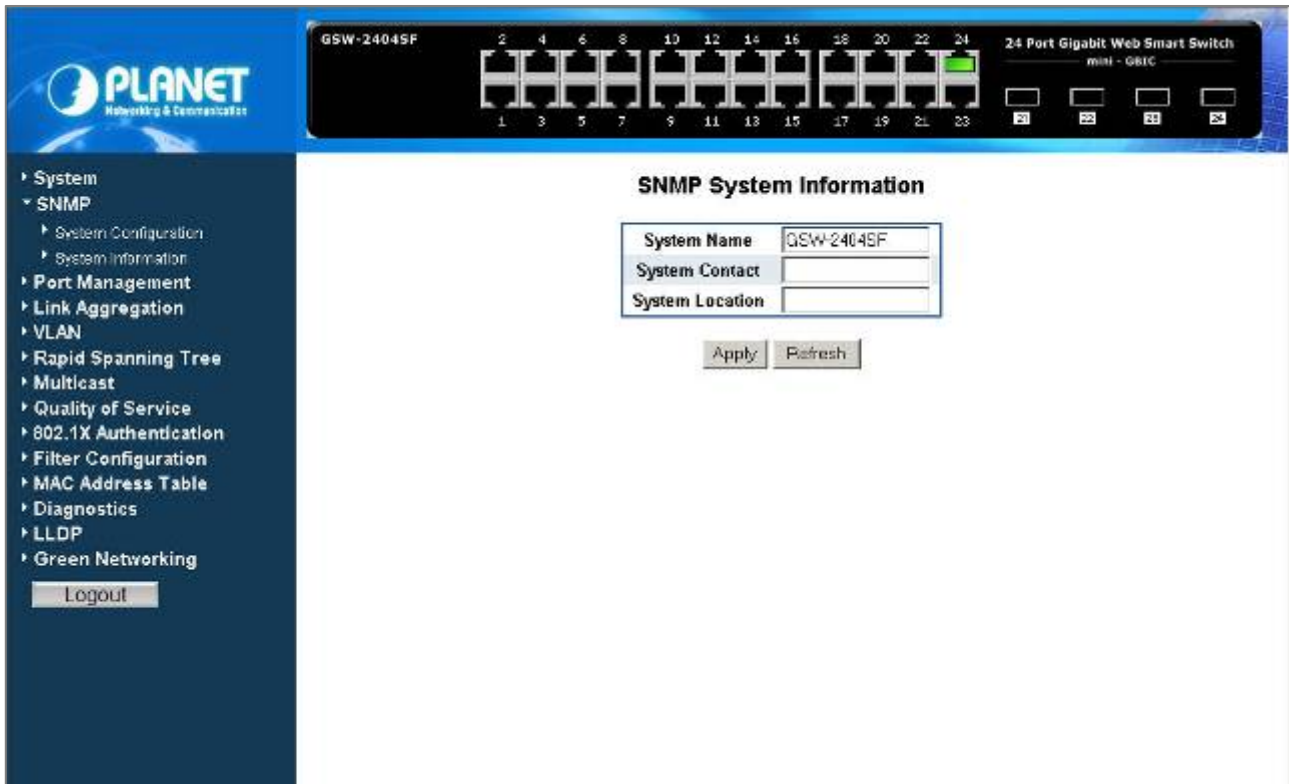
Figure 4-28 SNMP System Information screen

The page includes the following configurable data; see the **table 4-4** description of the System Information.

Item	Description
System Name	Defines the user-defined device name. Up to 16 characters is allowed.
System Contact	Defines the user-defined device contact. Up to 8 characters is allowed.
System Location	Defines the user-defined device location. Up to 8 characters is allowed.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh System Information screen of Web Smart Gigabit Switch.

Table 4-4 Description of the SNMP System Information

4.4 Port Management

4.4.1 Port Configuration

The Port Configuration page display per port link status / speed duplex mode, speed duplex mode configuration / Flow control / In-band & out-band bandwidth control / port description and Frame Length. The screen in Figure 4-29 appears.
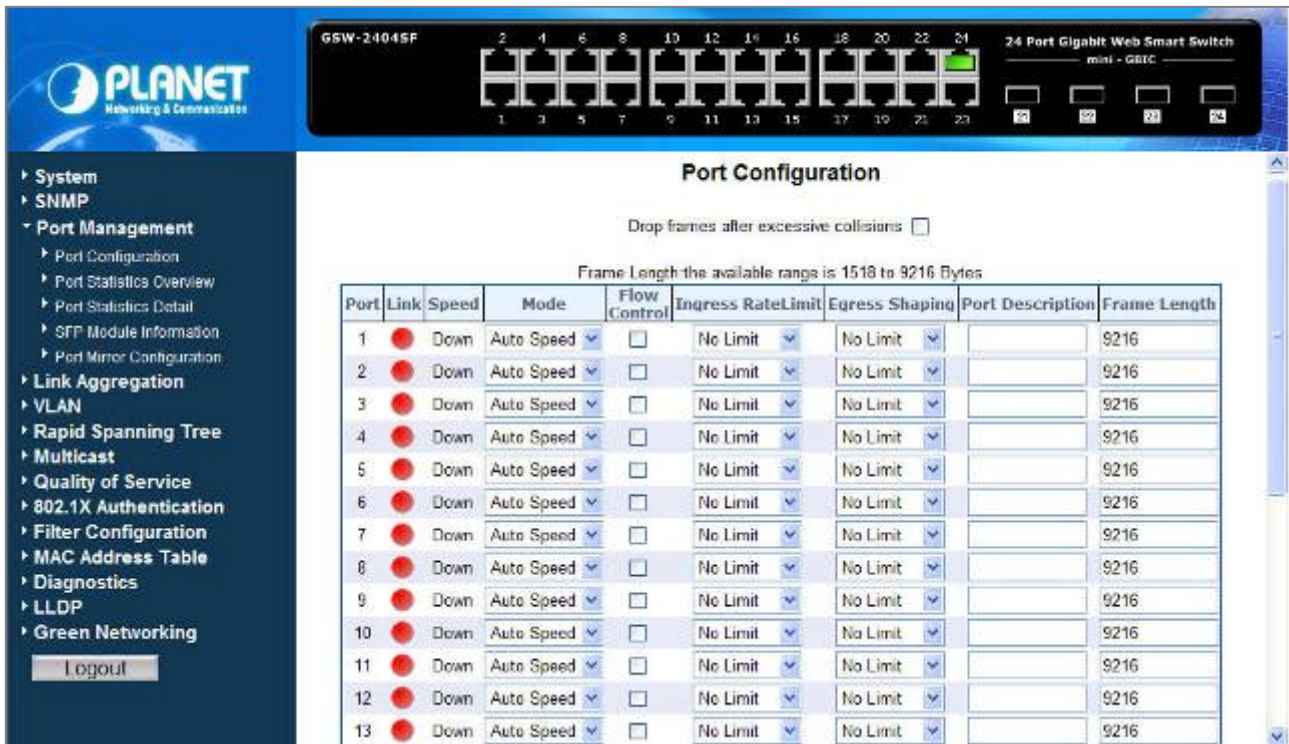
Figure 4-29 Port Configuration screen

The page includes the following configurable data; see the **table 4-5** description of the Port Configuration.

Item	Description
Port	Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF).
Link	Indicate current link status of each port.
Speed	Indicate current link speed duplex mode of each port.
Mode	Allow configuring the port speed and operation mode. Draw the menu bar to select the mode. • **Auto Speed** - Setup Auto negotiation. • **10 half** - Force sets 10Mbps Half-Duplex mode. • **10 Full** - Force sets 10Mbps Full-Duplex mode. • **100 half** - Force sets 100Mbps Half-Duplex mode. • **100 full** - Force sets 100Mbps Full-Duplex mode. • **1000 full** - Force sets 10000Mbps Full-Duplex mode. • **Disable** - Shutdown the port manually.
Flow Control	Allow **Enable** or **Disable** flow control for selected port.

	• **Enable** – 802.3x flow control is enabled on Full-Duplex mode or Backpressure is enabled on Half-Duplex mode. • **Disable** – No flow control or backpressure function on no matter Full-Duplex or Half-Duplex mode
Ingress Rate Limit	The value of inbound traffic limitation in kilobit-per-second (kbps). Per port in step of 128 kbps. Default : **No Limit** The range between 128 Kbps to 3968 kbps.
Egress Shaping	The value of outbound traffic limitation in kilobit-per-second (kbps). Per port in step of 128 kbps. Default : **No Limit** The range between 128 Kbps to 3968 kbps.
Port Description	Make a brief description for the port to help network manager identify the device connected to it. Maximum Length : **8** characters For example, label it as "***IP Phone***" if an IP Phone is connected to this port.
Frame Length	The value of Frame Length of per port can support. Default: **9216 Bytes** The range is 1518 Bytes to 9216 Bytes.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh Port Configuration screen of Web Smart Gigabit Switch.

Table 4-5 Description of the Port Configuration

4.4.2 Port Statistics Overview

The Port Statistics Overview page displays the status of packet count from each port. The Port Statistics Overview screen in Figure 4-30 appears.

Figure 4-30 Port Statistics Overview screen

The page includes the following configurable data; see the **table 4-6** description of the Port Statistics Overview.

• Item	Description
Auto Refresh	Disable or Enable the **Auto Refresh** function. While set to enable, the Port Statistics Overview table will refresh automatically every **30** seconds.
Port	The Port number. Press the port ID for detail packet information on the selected port.
Packets	
Receive	Number of total packets received on the selected port. Include the Unicast, broadcast and multicast packets.
Transmit	Number of total packets transmitted from the selected port. Include the Unicast , broadcast and multicast packets.
Bytes	
Receive	Number of total packets received on the selected port. Include the Unicast, broadcast and multicast packets. The unit is Bytes.
Transmit	Number of total packets transmitted from the selected port. Include the Unicast , broadcast and multicast packets. The unit is Bytes.
Error	
Receive	The number of **error** packets received on the selected port.

Transmit	The number of **error** packets transmitted from the selected port.
Broadcast	
Receive	Number of **Broadcast** packets received on the selected port.
Transmit	Number of **Broadcast** packets transmitted from the selected port.
Multicast	
Receive	Number of **Multicast** packets received on the selected port.
Transmit	Number of **Multicast** packets transmitted from the selected port.
Button	
Clear	Press this button to clear whole counter information from per port of Web Smart Gigabit Switch.
Refresh	Press this button for refresh Port Statistics Overview screen of Web Smart Gigabit Switch.

Table 4-6 Description of the Port Statistics Overview

4.4.3 Port Statistics Detail

The Port Statistics Detail page displays the status of packet count from each port. The Port Statistics Detail screen in appears.
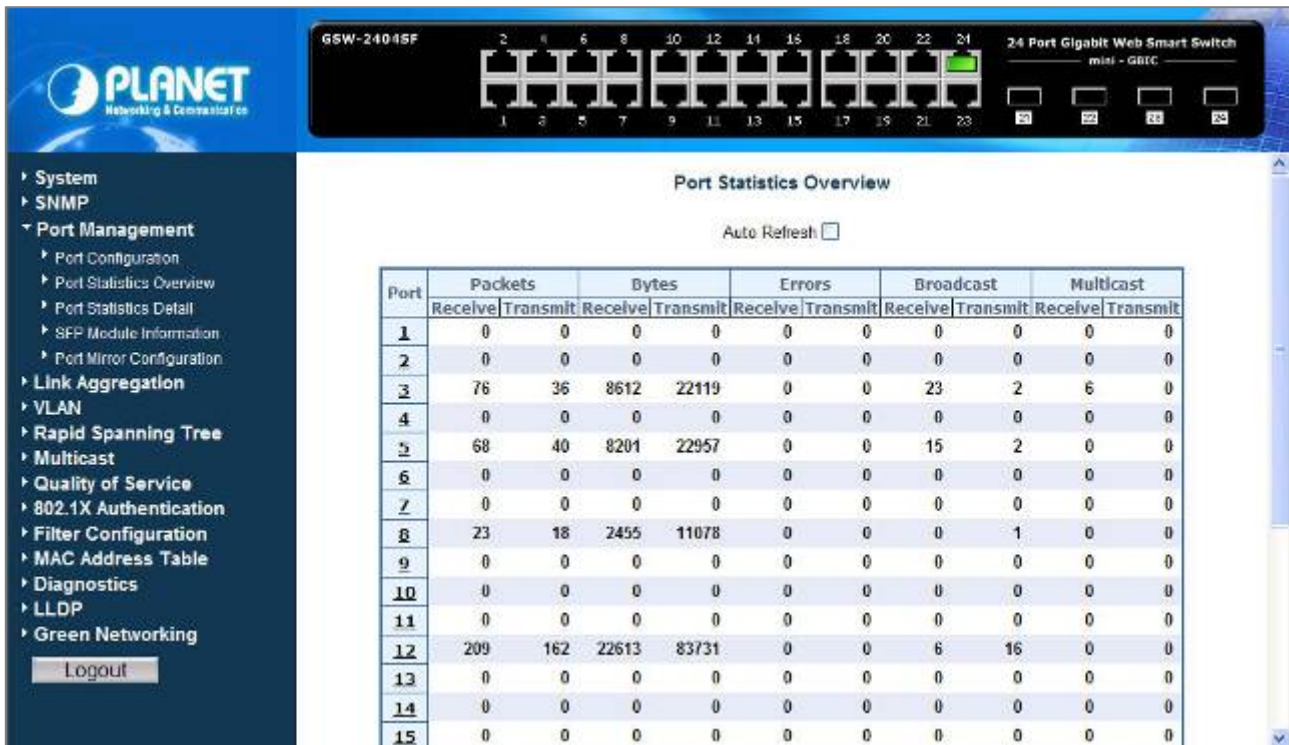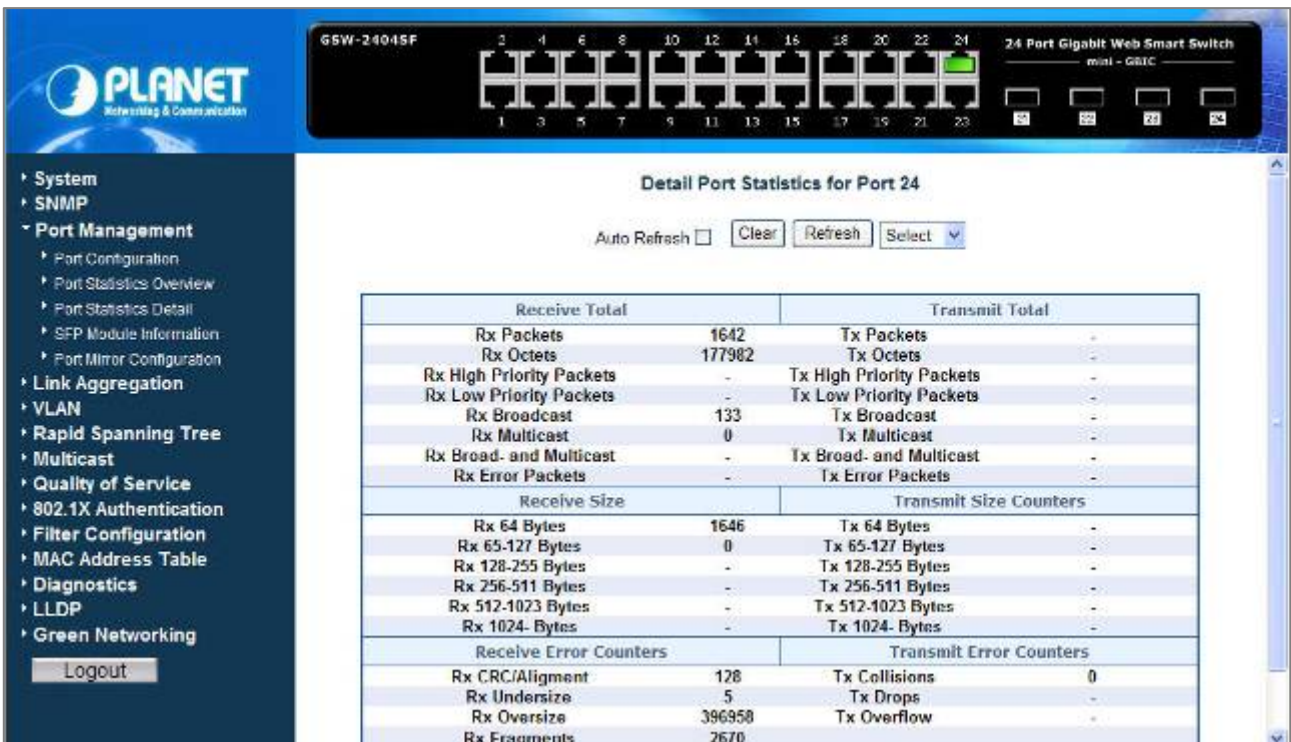

Figure 4-31 Port Statistics Detail screen

The page includes the following configurable data; see the **table 4-7** description of the Port Statistics Detail.

• Item	Description
Auto Refresh	Disable or Enable the **Auto Refresh** function. While set to enable, the Port Statistics Detail table will refresh automatically every **30** seconds.

Clear	Press this button to clear whole counter information from per port of Web Smart Gigabit Switch.
Refresh	Press this button for refresh Port Statistics Overview screen of Web Smart Gigabit Switch.
Select	Draw the menu bar to select the port (port 1 to port 16/24).
Receive Total	
Rx Packets	The number of packets received on the selected port.
Rx Octets	The number of total octets of data (including those in bad packets) received on the selected port.
Rx High Priority Packets	The number of high priority packets received on the selected port.
Rx Low Priority Packets	The number of low priority packets received on the selected port.
Rx Broadcast	The number of broadcast packets received on the selected port.
Rx Multicast	The number of multicast packets received on the selected port.
Rx Broad- and Multicast	The number of broadcast and multicast packets received on the selected port.
Rx Error Packets	The number of error packets received on the selected port.
•	
Transmit Total	
Tx Packets	The number of packets transmitted from the selected port.
Tx Octets	The number of total octets of data (including those in bad packets) transmitted from the selected port.
Tx High Priority Packets	The number of high priority packets transmitted from the selected port.
Tx Low Priority Packets	The number of low priority packets transmitted from the selected port.
Tx Broadcast	The number of broadcast packets transmitted from the selected port.
Tx Multicast	The number of multicast packets transmitted from the selected port.
Tx Broad- and Multicast	The number of broadcast and multicast packets transmitted from the selected port.
Tx Error Packets	The number of error packets transmitted from the selected port.
Receive Size	
Rx 64 Bytes	The number of **64 Bytes** packets received on the selected port.
Rx 65-127 Bytes	The number of **64-127 Bytes** packets received on the selected port.
Rx 128-255 Bytes	The number of **128-255 Bytes** packets received on the selected port.
Rx 256-511 Bytes	The number of **256-511 Bytes** packets received on the selected port.
Rx 512-1023 Bytes	The number of **512-1023 Bytes** packets received on the selected port.
Rx 1024- Bytes	The number of **1024 Bytes** packets received on the selected port.
Transmit Size Counters	
Tx 64 Bytes	The number of **64 Bytes** packets transmitted from the selected port.
Tx 65-127 Bytes	The number of **64-127 Bytes** packets transmitted from the selected port.

Tx 128-255 Bytes	The number of **128-255 Bytes** packets transmitted from the selected port.
Tx 256-511 Bytes	The number of **256-511 Bytes** packets transmitted from the selected port.
Tx 512-1023 Bytes	The number of **512-1023 Bytes** packets transmitted from the selected port.
Tx 1024- Bytes	The number of **1024 Bytes** packets transmitted from the selected port.
Receive Error Counters	
Rx CRC/Aligment	The number of **RX CRC/ Alignment** packets received on the selected port.
Rx Undersize	The number of **RX Undersize** packets received on the selected port.
Rx Oversize	The number of **RX Oversize** packets received on the selected port.
Rx Fragments	The number of **Rx Fragments** packets received on the selected port.
Rx Jabber	The number of **Rx Jabber** packets received on the selected port.
Rx Drops	The number of **Rx Drops** packets received on the selected port.
Transmit Error Counters	
Tx Collisions	The number of **Tx Collisions** transmitted from the selected port.
Tx Drops	The number of **Tx Drops** packets transmitted from the selected port.
Tx Overflow	The number of **Tx Overflow** packets transmitted from the selected port.

Table 4-7 Description of the Port Statistics Detail

4.4.4 SFP Module Information

The SFP Module Information page displays the mini-GBIC built-in information that installed into SFP slot. The SFP Module Information screen in Figure 4-32 appears.
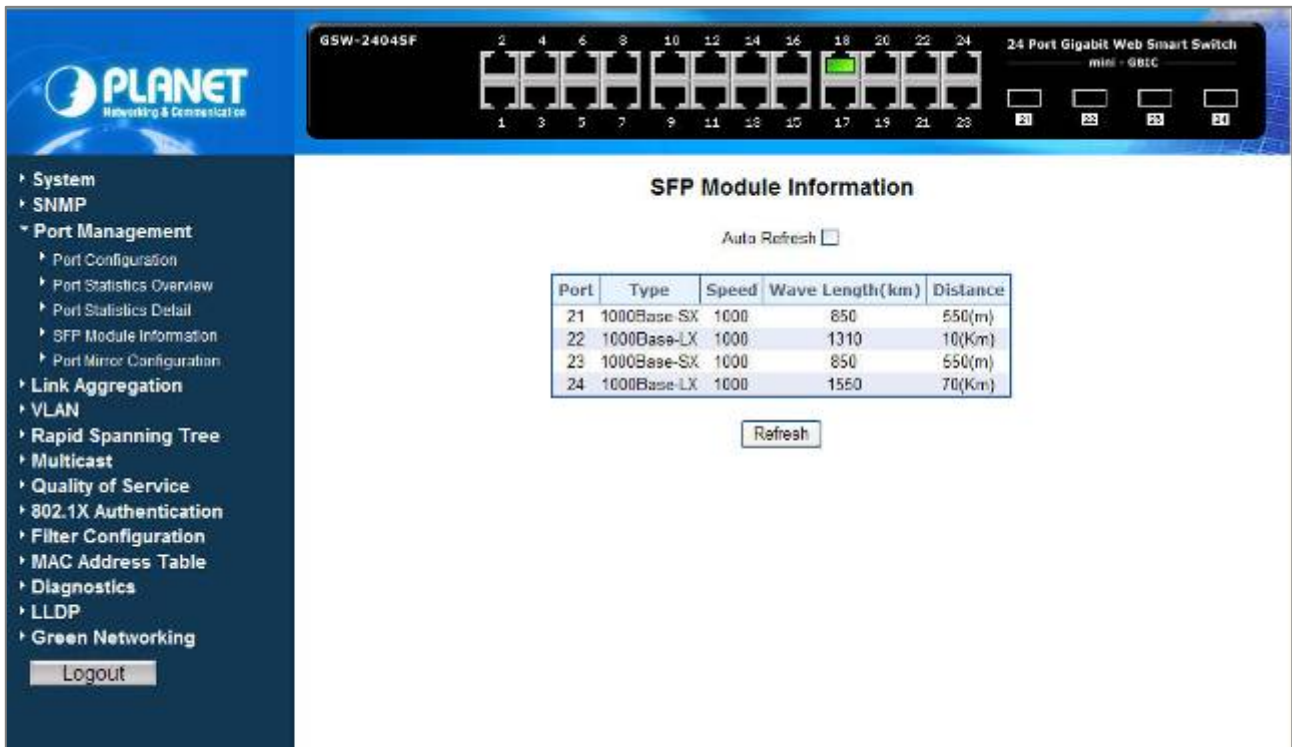
Figure 4-32 SFP Module Information screen

The page includes the following configurable data; see the **table 4-8** description of the SFP Module Information.

• Item	Description
Auto Refresh	Disable or Enable the **Auto Refresh** function. While set to enable, the Port Statistics Detail table will refresh automatically every **30** seconds.
Port	Indicate port 21 to port 24 (GSW-2404SF), port 15 to port 16 (GSW-1602SF).
Type	Display the Fiber type of mini-GBIC module that installed into SFP slot.
Speed	Display the Fiber operation speed of mini-GBIC module that installed into SFP slot.
Wavelength	Display the Fiber wavelength of mini-GBIC module that installed into SFP slot.
Distance	Display the Fiber transmit distance of mini-GBIC module that installed into SFP slot.
Refresh	Press this button for refresh SFP Module Information screen of Web Smart Gigabit Switch.

Table 4-8 Description of the SFP Module Information

4.4.5 Port Mirroring Configuration

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. The Port Mirroring Configuration screen in Figure 4-33 appears.
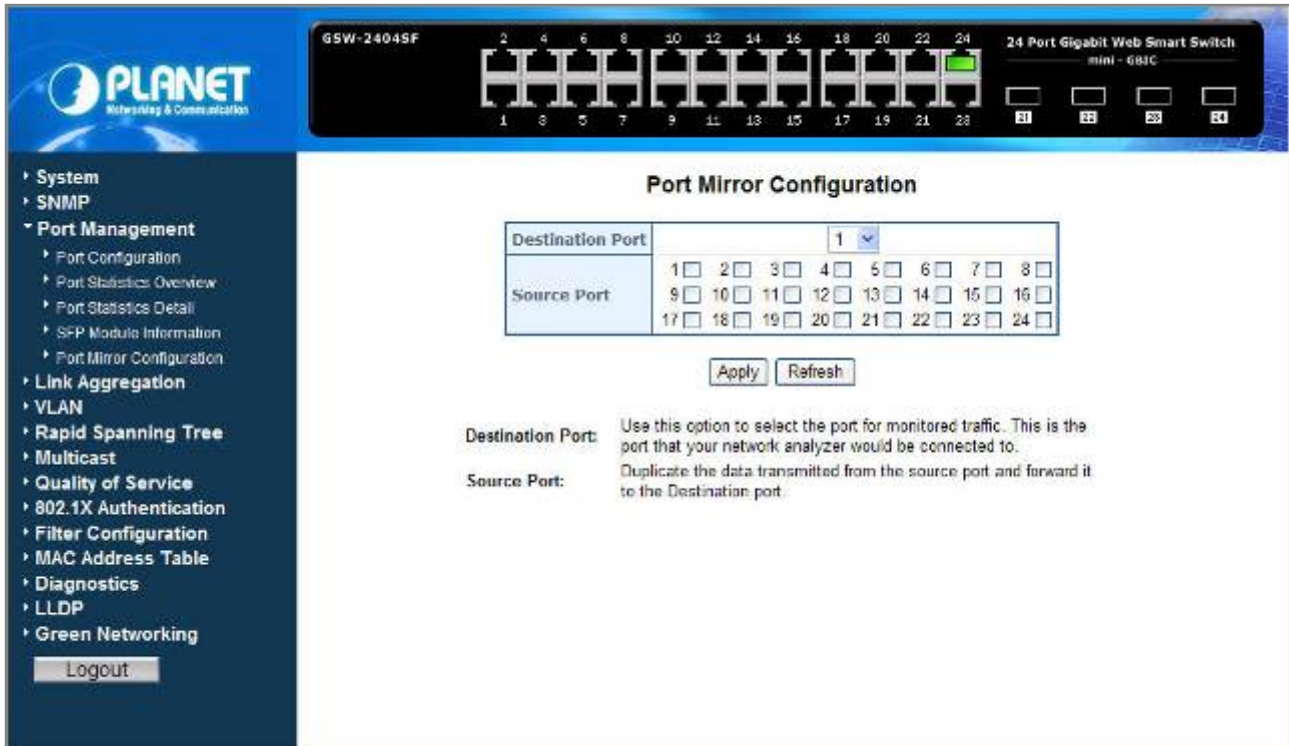
Figure 4-33 Port Mirroring Configuration screen

The page includes the following configurable data; see the **table 4-9** description of the Port Mirroring Configuration.

• Item	Description
Destination Port	Use this option to select the port for monitored traffic. This is the port that your network analyzer would be connected to – such as NAI **Sniffer Pro** or **Ethereal**.
Source Port	Duplicate the data transmitted from the source port and forward it to the Destination port.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh Port Mirroring Configuration screen of Web Smart Gigabit Switch.

Table 4-9 Description of the Port Mirroring Configuration

With the Chipset specification – the GSW-1602SF/GSW-2404SF port mirroring support **RX (Receive), TX (Transmit)** mode.

4.5 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 trounk 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.

4.5.1 Static Aggregation

This function provides to cascade two Switch devices with a double bandwidth (maximum up to 16/24Gbps in full duplex mode). The screen in Figure 4-34 appears.

- Eight Trunk Groups per system

- For GSW-1602SF, up to 8 ports per Trunk Group

- For GSW-2404SF, up to 12 ports per Trunk Group
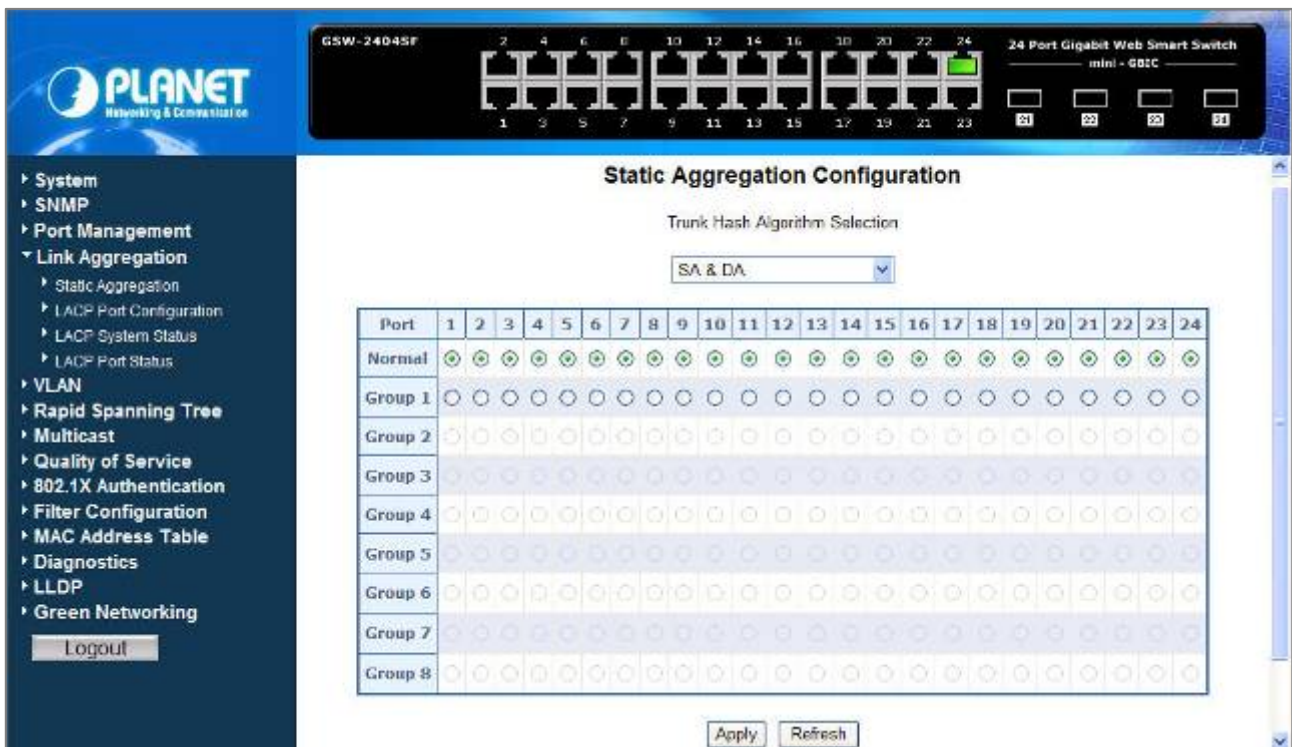
Figure 4-34 Static Aggregation Configuration screen

The page includes the following fields: **table 4-10** description of the Static Aggregation Configuration.

• Item	Description
Trunk Hash Algorithm Selection	Draw the menu bar to select the trunk hash algorithm • **Source MAC Address** • **Destination MAC Address** • **SA & DA** • **IP Address**
• **Port**	Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF).
• **Normal**	While a port is checked as **"Normal"**, the port is not joining to any Static Trunk Group.

• **Group 1-8**	Specify the Joined Trunk Group. There're maximum eight trunk groups per system. With different switch model, the maximum number of ports are as follow:
	
	  GSW-1602SF – Up to 8 ports per Trunk Group
	
	  GSW-2404SF – Up to 12 ports per Trunk Group
	
	  A port can be assigned to only one Trunk Group.

Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh Static Aggregation Configuration screen of Web Smart Gigabit Switch.

Table 4-10 Description of the Static Aggregation Configuration

4.5.2 LACP Port Configuration

Link Aggregation Control Protocol (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.

The **LACP** Port Configuration page contains fields for assigning **LACP** properties to individual ports. The screen in Figure 4-35 appears.
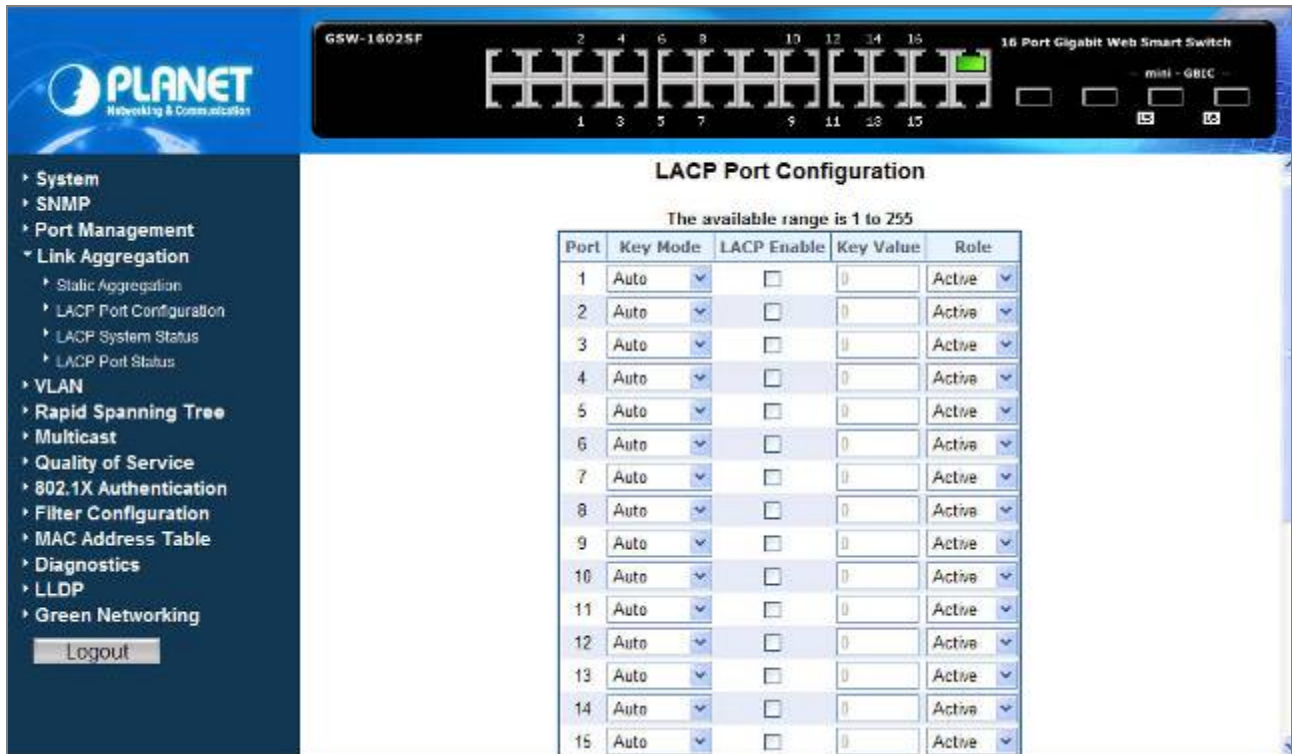

Figure 4-35 LACP Port Configuration

The page includes the following fields: **table 4-11** description of the LACP Port Configuration.

• Item	Description
Port	Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF).
Key Mode	Provide **"Auto"** or **"Customer"** for selection. Default is **"Auto"**.
LACP Enable	To Enable or disable the LCAP protocol on a selected port. Once the LACP protocol be enabled, the system will start transmit the LACP control packets and exchange with another LACP aware switch. If the linked switch didn't support LACP, then the aggregated link will not be established.
Key Value	Once set "**Customer"** in Key Mode, the Key Value will be filed in the LACP control packets. Ports with same key value will be set to the same LACP Group. If two ports are set with different key value, they will become two different LCAP groups. The key value will also be the identify ID to the linked LACP switch. The default setting is "**0**" and the available range is 1-255.
Role	Provide **"Active"** or **"Passive"** for selection. Default is **"Active"**.
Button	

Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh Static Aggregation Configuration screen of Web Smart Gigabit Switch.

Table 4-11 Description of the LACP Port Configuration.

When using a port link aggregation, note that:

- 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.

- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

4.5.3 LACP System Status

The LACP System Status page display the current LACP aggregation Groups and partner MAC Address status and etc.

The screen in Figure 4-36 appears.
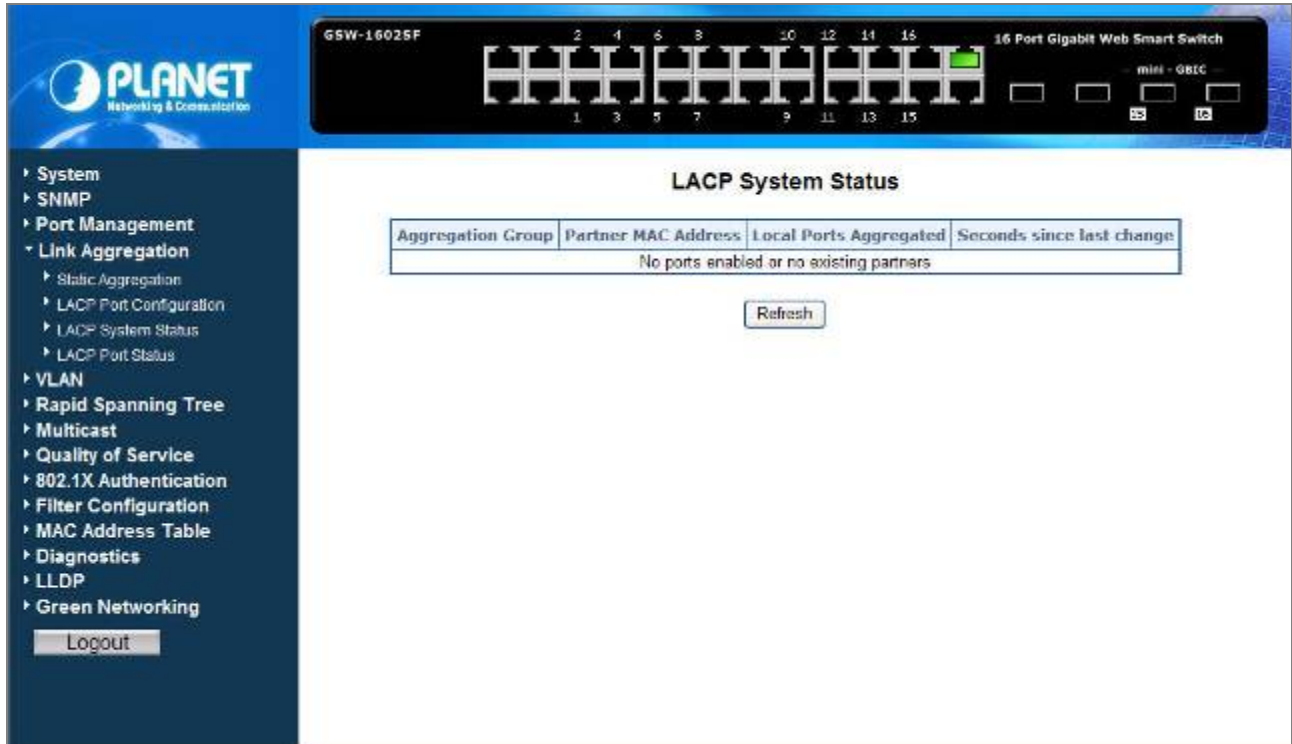
Figure 4-36 LACP System Status

The page includes the following fields: **table 4-12** description of the LACP System Status.

• Item	Description
Aggregation Group	The aggregation Group associated with this aggregation instance.
Partner MAC Address	The MAC Address of the aggregation partner.
Local ports Aggregated	Indicate which ports are parts of this aggregation for this Switch.
Seconds since last change	The time since this aggregation changed.
Button	
Refresh	Press this button for refresh LACP System Status screen of Web Smart Gigabit Switch.

Table 4-12 Description of the LACP System Status.

4.5.4 LACP Port Status

The LACP Port Status page lists the active LACP ports and the Partner Port number with the operational Port Key value.
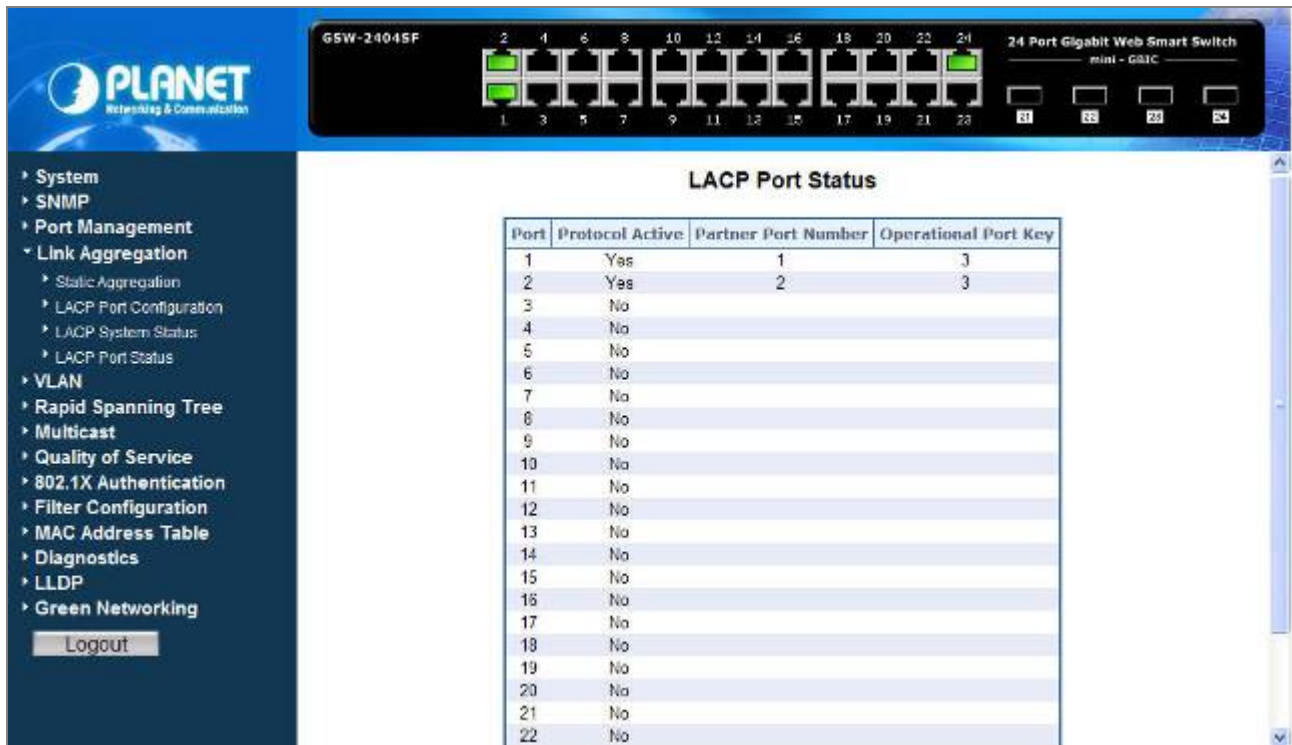
The screen in Figure 4-37 appears.

Figure 4-37 LACP Port Status

The page includes the following fields: **table 4-13** description of the LACP Port Status.

Item	Description
Port	Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF).
Protocol Active	Indicate the LCAP protocol is enable or not on the port. **Yes**- LACP is enabled and active on the port **No**- LACP is not enabled, or LACP is enabled but not active on the port. It's usually depends on the partner switch is LACP enabled or not.
Partner Port Number	The port number of the linked partner switch- if other switch has LACP enabled. Ex. Row of Port 7 with Partner Port Number value=15 The Port 7 of the switch is connecting to the Port 15 of the partner switch directly – both of the two switches are with LACP enabled.
Operational Port Key	The current operational key value of the partner port. Within the same LACP group, the port key value should be the same with the other LACP active ports.

Table 4-13 Description of the LACP Port Status

4.6 VLAN

■ VLAN Overview

A **Virtual LAN (VLAN)** is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

The Gigabit Ethernet Switch supports **IEEE 802.1Q (tagged-based)** and **Port-Base VLAN** setting in web management page. In the default configuration, VLAN support is **"802.1Q"**.

■ Port-based VLAN

Port-based VLAN limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLAN.NIC do not need to be able to identify 802.1Q tags in packet headers. NIC send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet is dropped by the Switch or delivered.

■ IEEE 802.1Q VLANs

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.
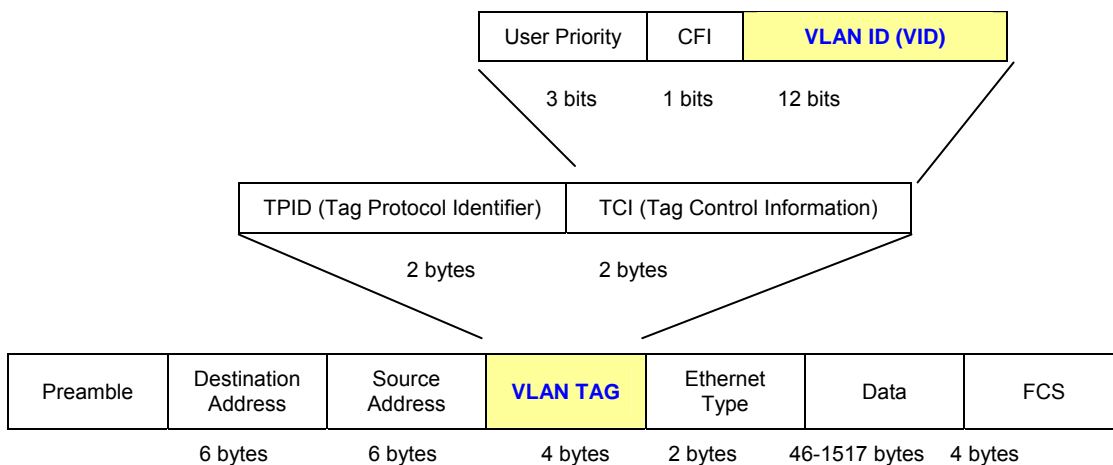
Some relevant terms:

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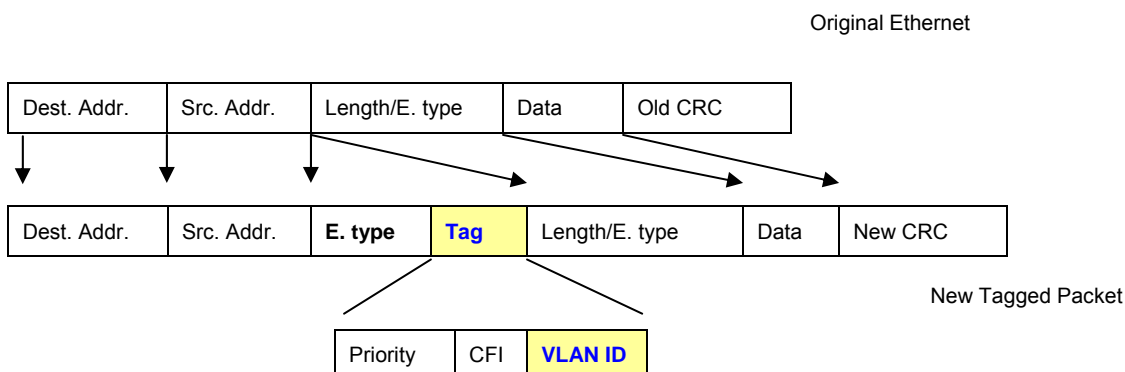
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

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	46-1517 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

Original Ethernet

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

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."

	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.
Note	2 The Switch supports Port-based VLAN and 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.

■ **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.

> 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.

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

The GSW-1602SF / GSW-2404SF Switch supports IEEE 802.1Q (tagged-based) and Port-Base VLAN setting in web management page. In the default configuration, VLAN support is **"802.1Q"**.

Port-based VLAN

Port-based VLAN limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLAN.NIC do not need to be able to identify 802.1Q tags in packet headers. NIC send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet is dropped by the Switch or delivered.

IEEE 802.1Q VLANs

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.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allow 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.

4.6.1 VLAN Basic Information

This function display current / basic information of VLAN. The screen in Figure 4-38 appears.
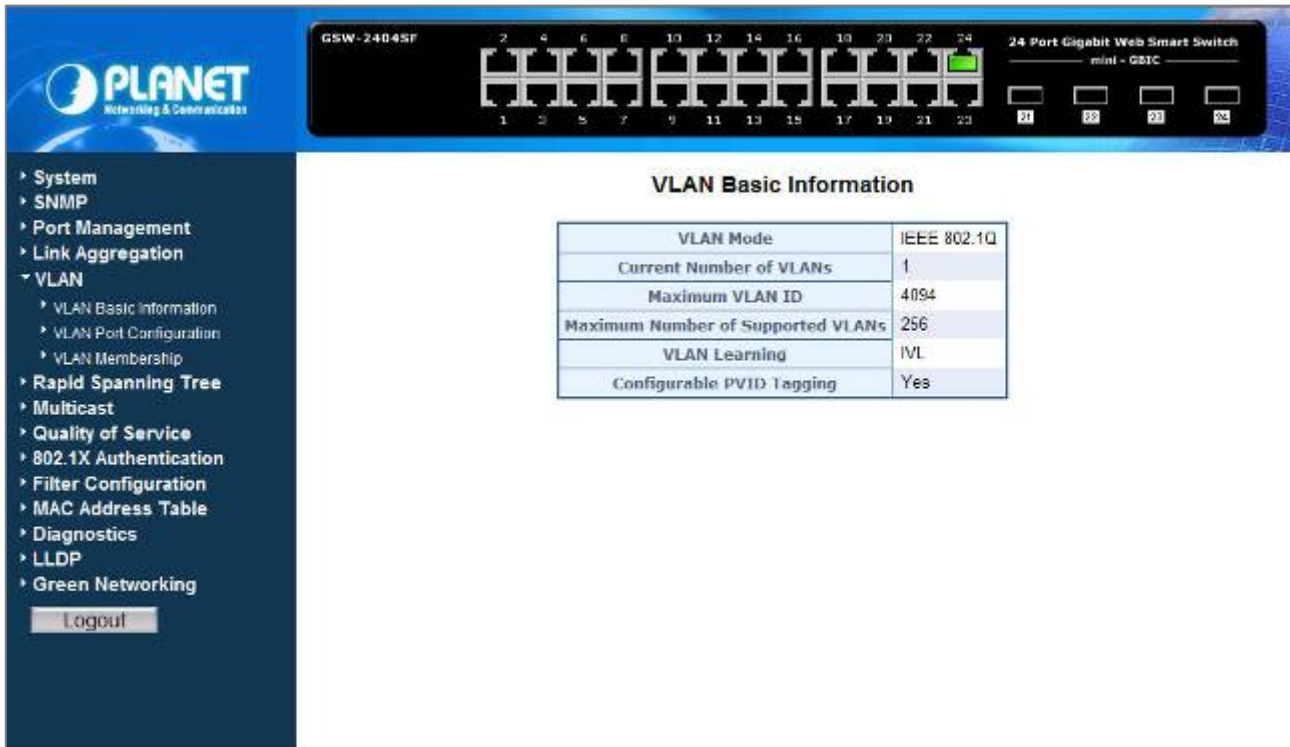
Figure 4-38 VLAN Basic Information

The page includes the following fields: **table 4-14** description of the VLAN Basic Information.

Item	Description
VLAN Mode	Indicate **"Port-Based VLAN"** or **"IEEE 802.1Q"** operation VLAN mode. Default mode is **IEEE 802.1Q**.
Current Number of VLANs	Indicate the current number of VLAN groups. Default mode is **1**.
Maximum VLAN ID	Indicate the maximum VLAN ID of VLAN function, the maximum VLAN ID is **4094**.
Maximum Number of Supported VLANs	Indicate the maximum number of VLAN groups support, the maximum value is **256**.
VLAN Learning	Indicate the method of VLAN Learning is **IVL** (Independent VLAN Learning).
Configurable PVID Tagging	Indicate per port support PVID Untagged and Tagging.

Table 4-14 Description of the VLAN Basic Information.

4.6.2 VLAN Port Configuration

The VLAN 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. The screen in Figure 4-39 appears.
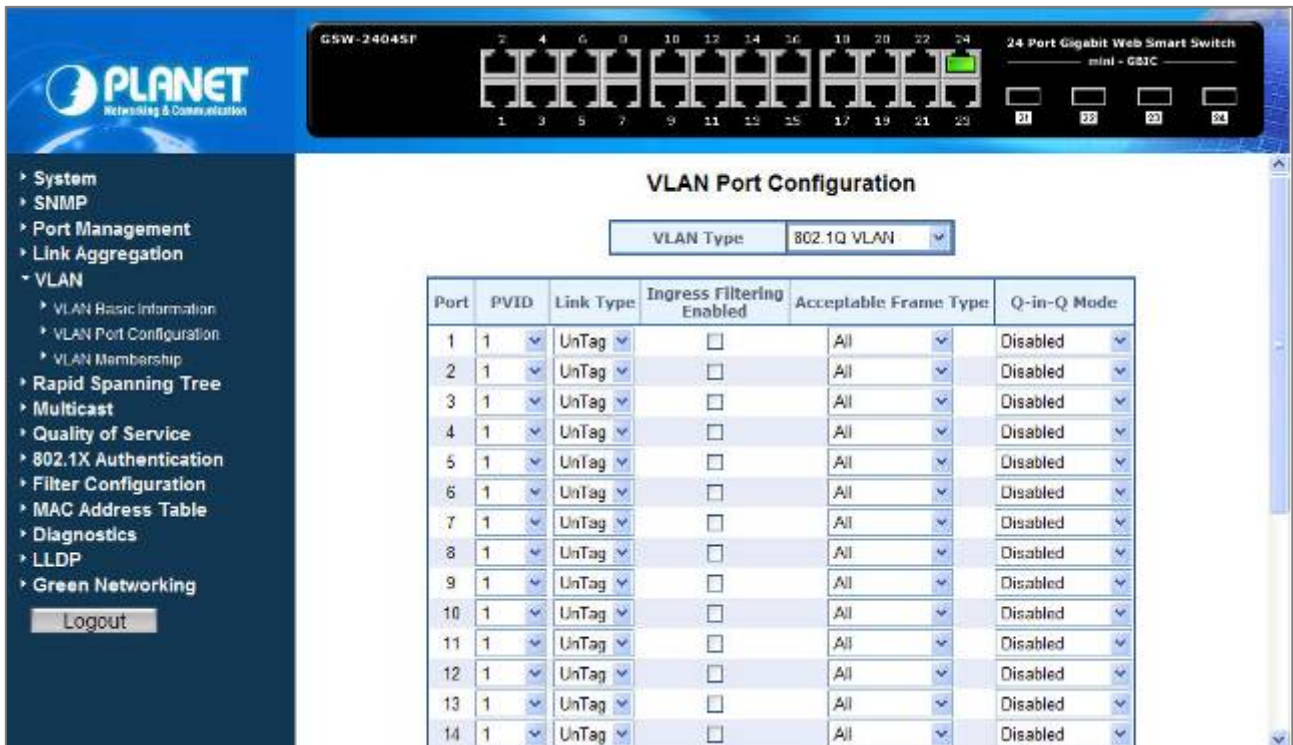

Figure 4-39 VLAN Port Configuration

The page includes the following fields: **table 4-15** description of the VLAN Port Configuration.

Item	Description
VLAN Type	There're two VLAN mode support – 802.1Q VLAN and Port-Based VLAN • **IEEE 802.1Q** – Packets income will be tagged with VID as the PVID setting. All ports on the Web Smart Gigabit Switch belong to default VLAN (VID 1). • **Port-Base** - Packets can only be broadcast among other members of the same VLAN group. Note all unselected ports are treated as belonging to the default system VLAN. If port-based VLAN are enabled, then VLAN-tagging feature is ignored. Default mode is **IEEE 802.1Q**.
Port	Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF).
PVID	Allow assign PVID for selected port. The range for the PVID is **1-4094.** 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.
Link Type	Allow 802.1Q Untagged or Tagged VLAN for selected port. When adding a VLAN to selected port, it tells the switch whether to keep or remove the tag from a frame on egress.

	Untag: outgoing frames without VLAN-Tagged.
	Tagged: outgoing frames with VLAN-Tagged.
Ingress Filtering Enable	**Enabled** - the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. **Disabled** - all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
Acceptable Frame Type	Specifies the types of frames that may be received on this port. The options are 'All' and 'Tagged only'. • **All**- untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. • **Tagged only** - untagged frames or priority tagged frames received on this port are discarded. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Q-In-Q Mode	Sets the Web Smart Gigabit Switch to **QinQ** mode, and allows the QinQ tunnel port to be configured. The default is for the Managed Switch to function in **Disable** mode.

Disable	The port operates in its normal VLAN mode. (**Default**.)
Customer Port:	Configures IEEE 802.1Q tunneling (QinQ) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
MAN Port:	Configures IEEE 802.1Q tunneling (QinQ) for an uplink port to another device within the service provider network.

Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Cancel	Press this button for ignore current configuration of Web Smart Gigabit Switch.

Table 4-15 Description of the VLAN Port Configuration.

4.6.3 VLAN Membership

This function group individual ports into a small "**Virtual**" network of their own to be independent of the other ports. The screen in Figure 4-40 appears.
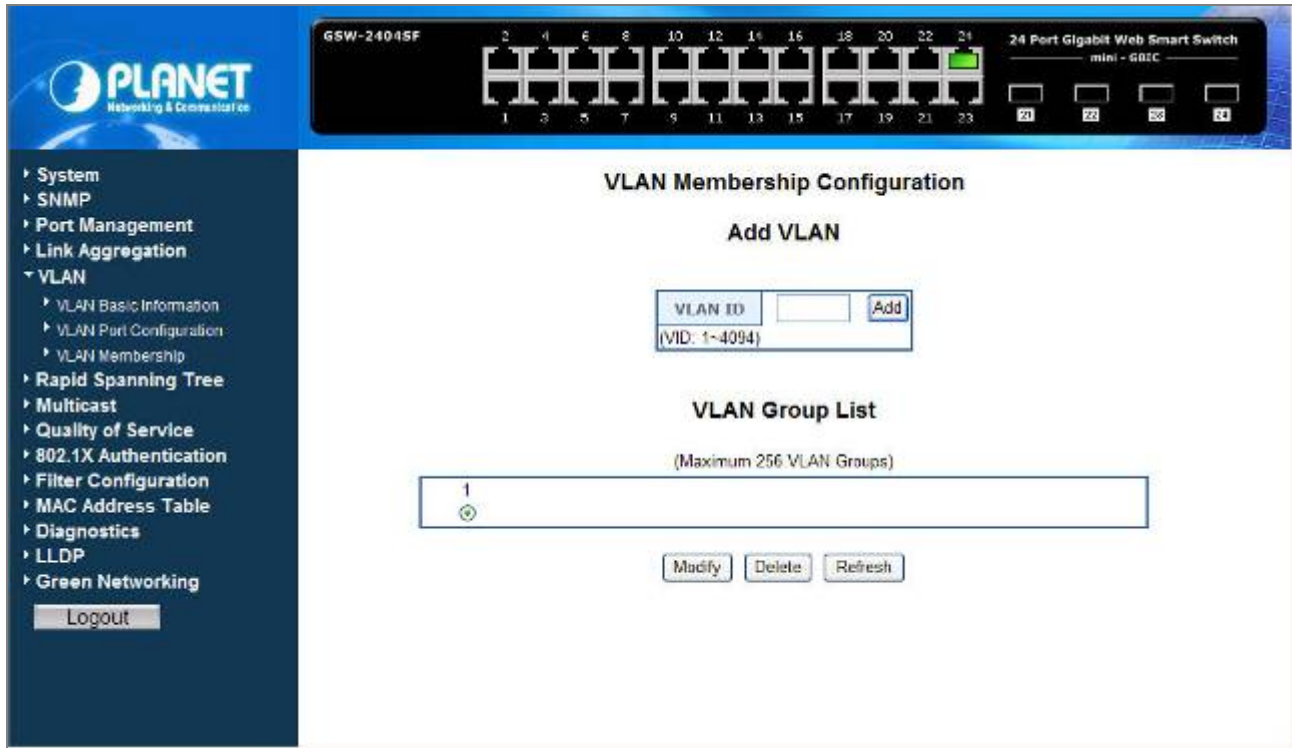

Figure 4-40 VLAN Membership

The page includes the following items: **table 4-16** description of the VLAN Membership.

Item	Description
VLAN ID	Specify the VLAN Identifier for the new VLAN. (You can only enter data in this field when you are creating a new VLAN.) The range of the VLAN ID is (**1 to 4094**).
Add	To add a new VLAN Group with the specify VLAN ID. Once the Add button be pressed. The page will be redirect to have the VLAN member setup page.
Modify	To modify an existence VLAN Group- adds new member ports or remove ports from the selected VLAN Group.
Delete	Delete the selected VLAN Group.
Refresh	Refresh the VLAN Configuration screen

Table 4-16 Description of the VLAN Membership

4.6.3.1 Add a VLAN Group

The PLANET Web Smart Gigabit Switch supports up to **256** active VLAN groups and the range for the VLAN ID is **1-4094**.

1. To add a VLAN group, filed in the **VLAN ID** (from 1-4094) and please press *"Add"* button, the new VLAN Setup screen will pop out.
2. Checked the Member box to select the members for the VLAN group.
3. After setup completed, please press **"Apply"** to take affect.

The above screen appears in Figure 4-41 and Figure 4-42.

Figure 4-41 Add a VLAN screen

Figure 4-42 VLAN Member Setup screen

4.6.3.2 Modify the VLAN Group Member

Once you want to modify the existence VLAN Group member or delete a existence VLAN Group. Refer to the following steps.

1. To modify the members of an existence VLAN Group, check the VLAN Group ID and press "**Modify**" button. the ID VLAN Member Setup screen will pop out.

2. To add / remove a port from specific VLAN group, just check / cancel the Member check Box and press "**Apply**" to take affect.

3. To delete an existence VLAN Group, check the VLAN Group ID and press "**Delete**" button.
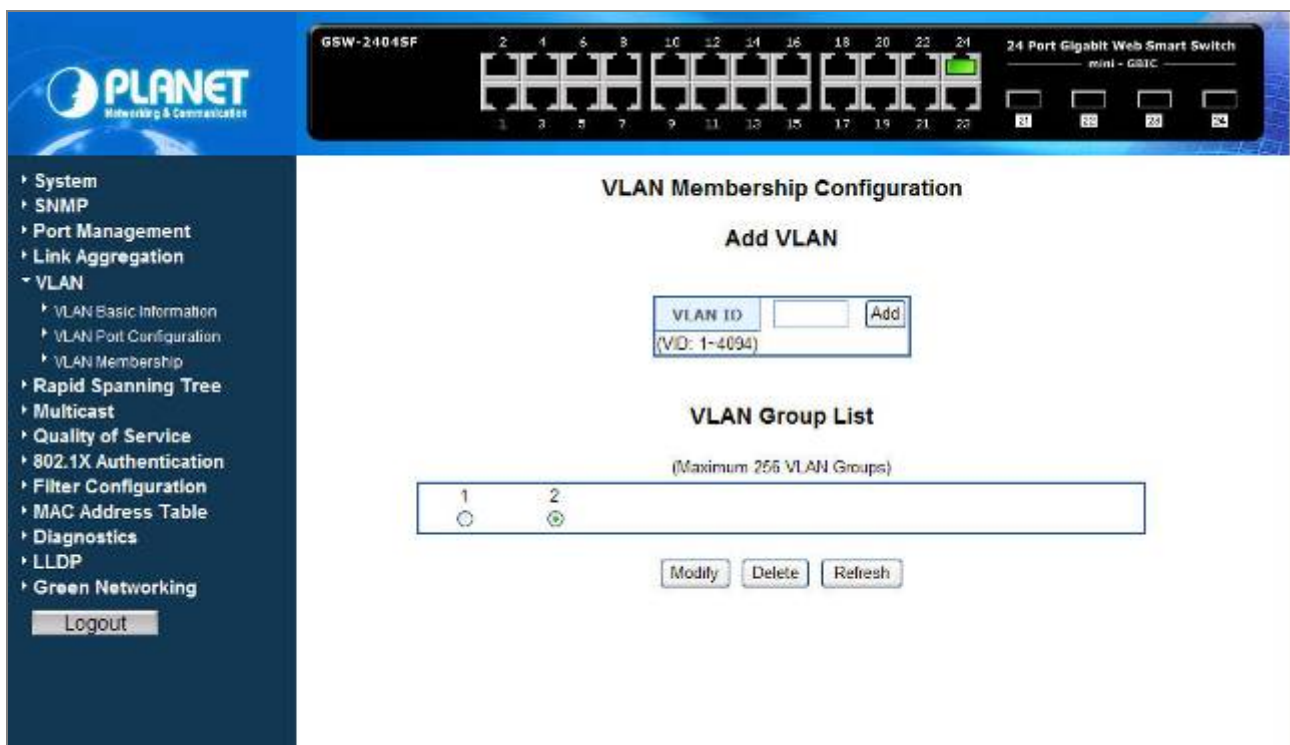
As show in Figure 4-43 appears.

Figure 4-43 VLAN Group – member modify and delete VLAN Group screen

Once the VLAN Group be deleted, the Ports with the PVID set to this VLAN Group have to re-configure the PVID. Or the PVID will be set to **"None"**.

4.6.4 VLAN setting example:

4.6.4.1 Two separate 802.1Q VLAN

The diagram shows how the Web Smart Gigabit Switch handle Tagged and Untagged traffic flow for two VLANs. VLAN

Group 2 and VLAN Group 3 are separated VLAN. Each VLAN isolate network traffic so only members of the VLAN receive

traffic from the same VLAN members. The screen in Figure 4-44 appears and **table 4-17** describes the port configuration of

switch.

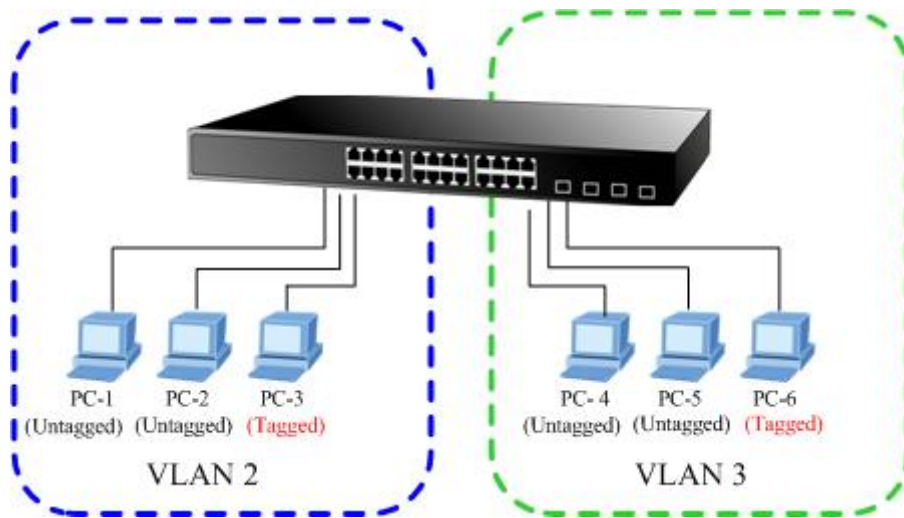**Figure 4-44** two separate VLAN diagram

VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 1	1	Port-7~Port-24	N/A
VLAN Group 2	2	Port-1,Port-2	Port-3
VLAN Group 3	3	Port-4,Port-5	Port-6

Table 4-17 VLAN and Port Configuration

The scenario described as follow:

■ **Untagged packet entering VLAN 2**

1. While **[PC-1]** transmit an **untagged** packet enters **Port-1**, the 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**

5.   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**.

6.   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 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**.

> At this example, VLAN Group 1 just set as default VLAN, but only focus on VLAN 2 and VLAN 3 traffic flow
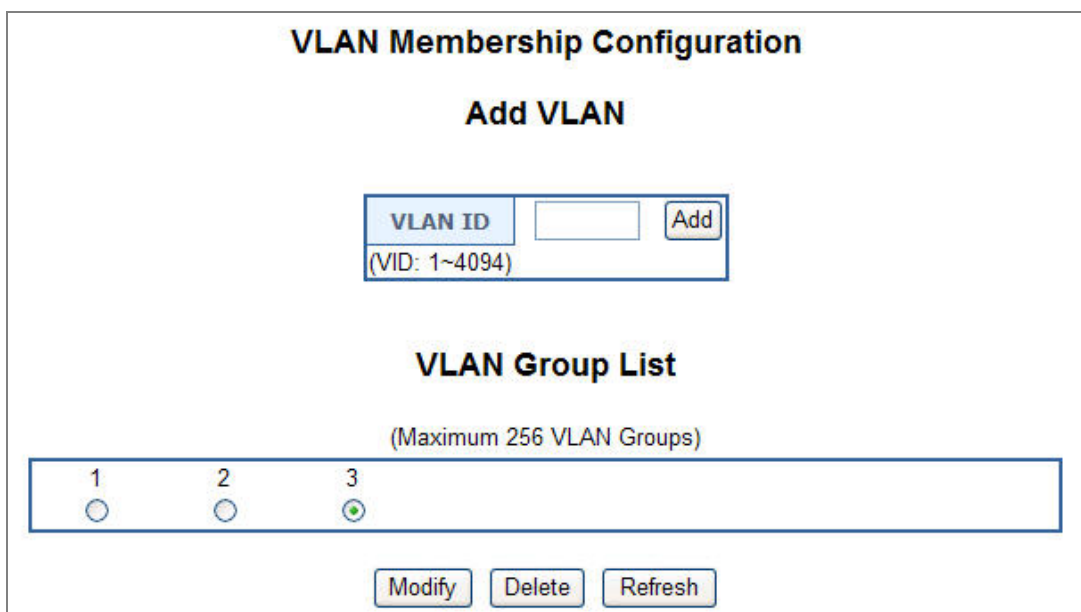
Setup steps

1.   Create VLAN Group

Set VLAN Group 1 = Default-VLAN with VID (VLAN ID) =1

Add two VLANs – VLAN 2 and VLAN 3

   VLAN Group 2 with VID=*2*

   VLAN Group 3 with VID=*3*

Figure 4-45 Add new VLAN Group screen

2. Assign VLAN Member :

VLAN 2 : Port-1,Port-2 and Port-3

VLAN 3 : Port-4, Port-5 and Port-6

VLAN 1 : All other ports – Port-7~Port-24

Figure 4-46 Assign VLAN members for VLAN 2 and VLAN 3

Remember to remove the Port 1 – Port 6 from VLAN 1 membership, since the Port 1 – Port 6 had be assigned to VLAN 2 and VLAN 3.

VLAN Member Setup

VLAN ID: 1			
Port	Member	Port	Member
Port 1	☐	Port 13	☑
Port 2	☐	Port 14	☑
Port 3	☐	Port 15	☑
Port 4	☐	Port 16	☑
Port 5	☐	Port 17	☑
Port 6	☐	Port 18	☑
Port 7	☑	Port 19	☑
Port 8	☑	Port 20	☑
Port 9	☑	Port 21	☑
Port 10	☑	Port 22	☑
Port 11	☑	Port 23	☑
Port 12	☑	Port 24	☑

Apply   Refresh

Figure 4-47 Remove specify ports from VLAN 1 member

> **Note**
> It's import to remove the VLAN members from VLAN 1 configuration. Or the ports would become overlap setting. (About the overlapped VLAN configuration, see next VLAN configure sample)

3. **Assign PVID for each port:**

Port-1,Port-2 and Port-3 : PVID=*2*

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

Port-7~Port-24 : PVID=*1*

4. **Enable VLAN Tag for specific ports**

Link Type : *Port-3* (VLAN-2) and *Port-6* (VLAN-3)

The Per Port VLAN configuration in Figure 4-48 appears.

Figure 4-48 Port 1-Port 6 VLAN Configuration

4.6.4.2 Two VLANs with overlap area

Follow the example of 4.6.4.1. There're two exist separate VLANs – VLAN 2 and VLAN 3, and the PCs of each VLANs are not able to access each other of different VLANs. But they all need to access with the same server. The screen in Figure 4-49 appears. This section will show you how to configure the port for the server – that could be accessed by both VLAN 2 and VLAN 3.
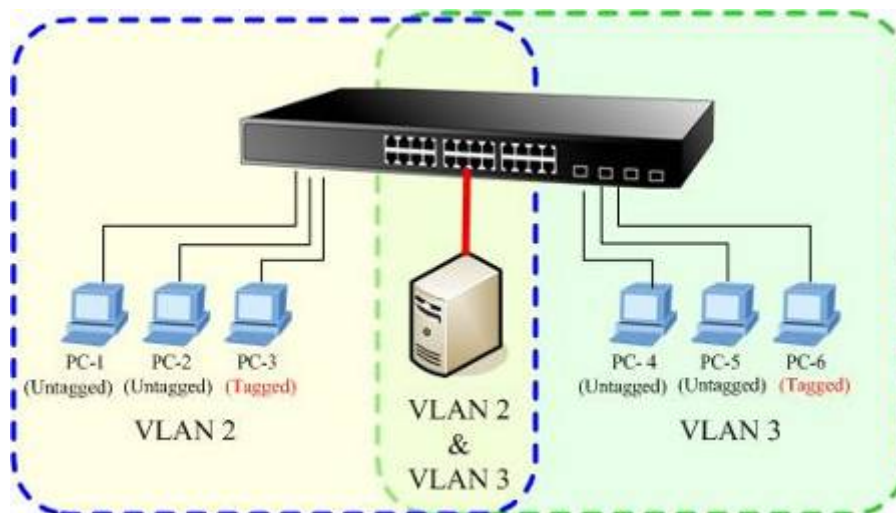
Figure 4-49 A Server connect to the VLAN overlap area

1. Specify **Port-7** on the device to connect to the server.

2. Assign **Port-7** to both **VLAN 2** and **VLAN 3** at the VLAN Member configuration page. The screen in Figure 4-50 appears.

Figure 4-50 VLAN overlap port setting

3. Define a **VLAN 1** as a **"Public Area"** that overlapping with both **VLAN 2 members** and **VLAN 3 members**.

Figure 4-51 VLAN 1 – The public area member assign

4. Setup **Port-7** with "**PVID=1**" at VLAN Per Port Configuration page. The screen in Figure 4-52 appears.

VLAN Port Configuration

| | VLAN Type | 802.1Q VLAN |

Port	PVID	Link Type	Ingress Filtering Enabled	Acceptable Frame Type	Q-in-Q Mode
1	2	UnTag	☐	All	Disabled
2	2	UnTag	☐	All	Disabled
3	2	Tag	☐	All	Disabled
4	3	UnTag	☐	All	Disabled
5	3	UnTag	☐	All	Disabled
6	3	Tag	☐	All	Disabled
7	1	UnTag	☐	All	Disabled
8	1	UnTag	☐	All	Disabled

Figure 4-52 Setup Port-7 with PVID-1

That is, although the VLAN 2 members: Port-1 to Port-3 and VLAN 3 members: Port-4 to Port-6 also belongs to VLAN 1. But with different PVID settings, packets form VLAN 2 or VLAN 3 is not able to access to the other VLAN.

4.6.4.3 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 4-53 appears.
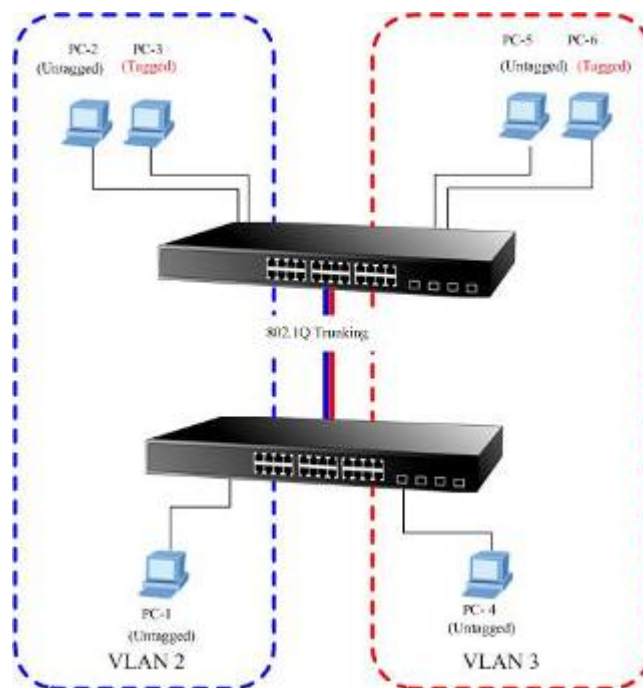
Figure 4-53 802.1Q Trunking with other VLAN aware device

About the VLAN ports connect to the hosts, please refer to 4.5.4.1 and 4.5.4.2 examples. The following steps will focus on the VLAN **Trunk port** configuration.

1. Specify **Port-8** to be the 802.1Q VLAN **Trunk port**, and the Trunking port must be a **Tagged** port while egress. The Port-8 configuration as the following screen in Figure 4-54.

Figure 4-54 The configuration of VLAN Trunk port

2. Assign the VLAN Trunk Port to be the member of each VLAN – which wants to be aggregated. At this sample, add **Port-8** to be **VLAN 2** and **VLAN 3** member port.

Figure 4-55 Add VLAN Trunk port to each VLAN

3. Repeat Step 1 and 2, setup the VLAN Trunk port at the partner switch.

4. To add more VLANs to join the VLAN trunk, repeat Step 2 to assign the Trunk port to the VLANs.

4.7 Rapid Spanning Tree

4.7.1 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 Managed Industrial Switch include these versions:

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

Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops.

Rapid Spanning Tree Protocol (RSTP) - While Classic Spanning Tree guarantees preventing L2 forwarding loops in a general network topology, convergence can take up to 30-60 seconds. The convergence time is considered too long for many applications. When network topology allows, faster convergence may be possible. The **Rapid Spanning Tree Protocol (RSTP)** detects and uses of network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.

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 por tidentifier

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
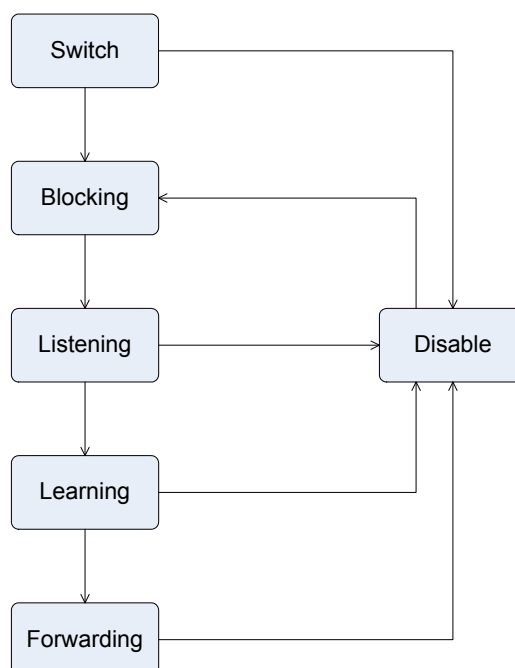
STP Figure STP Port State Transitions

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.

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 except by setting priority below)**	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	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 Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.
Note	

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

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

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.
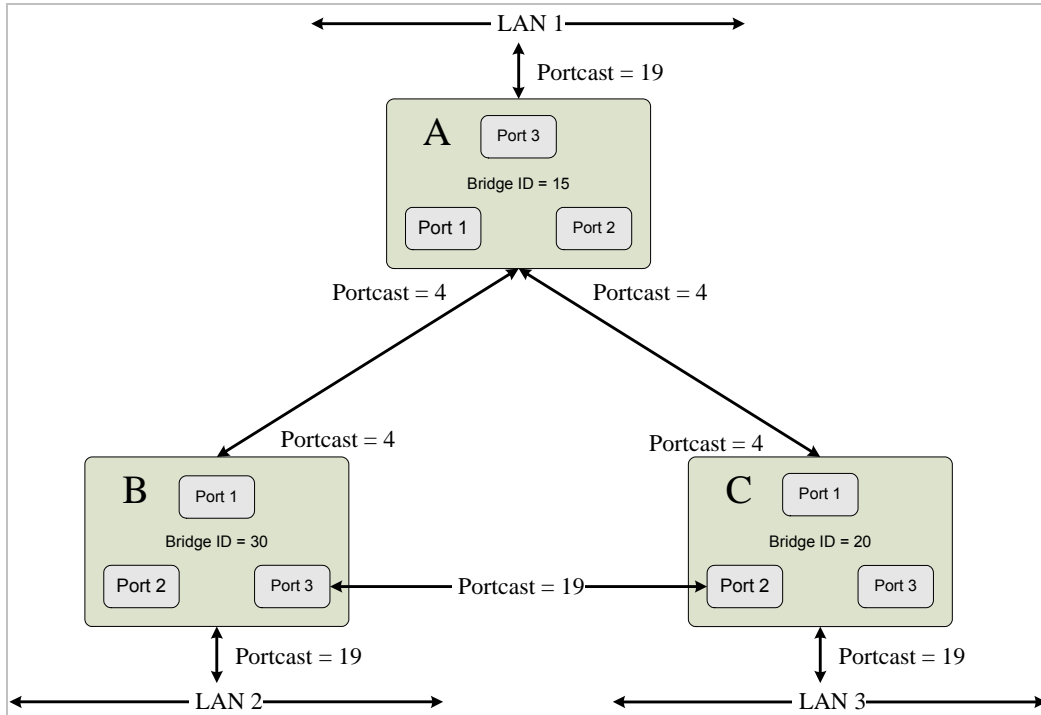
STP Figure Before Applying the STA Rules

In this example, only the default STP values are used.
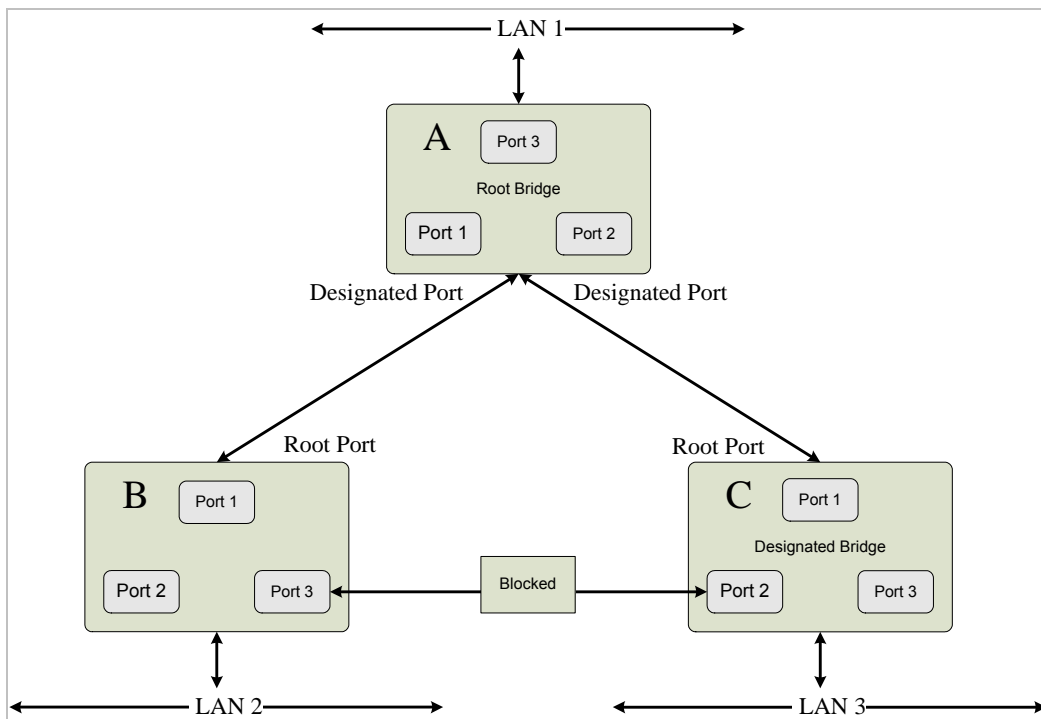
STP Figure After Applying the STA Rules

4.7.2 RSTP System Configuration

This page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the switch. The Web Smart Gigabit 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.

> **Note**
> The GSW-1602SF/GSW-2404SF implement the Rapid Spanning Protocol as the default spanning tree protocol. While select "Compatibles" mode, the system use the **RSTP** (802.1w) to compatible and co work with another **STP** (802.1d)'s BPDU control packets.

This page is to enable/disable the Spanning Tree protocol. The Web Smart Gigabit Switch support IEEE 802.1D Spanning Tree (**STP**), IEEE 802.1w Rapid Spanning Tree (**RSTP**). The screen in Figure 4-56 appears.
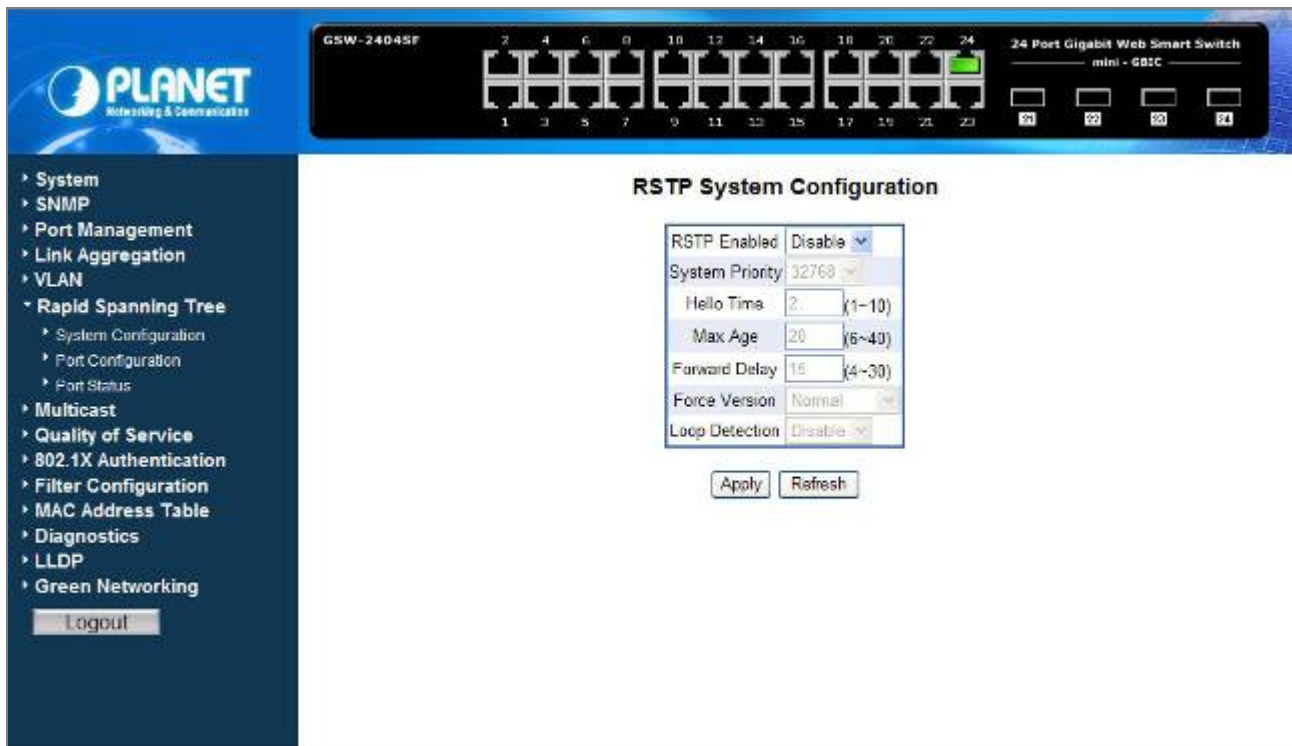
Figure 4-56 Rapid Spanning Tree System Configuration

4.7.3 RSTP System Configuration

The **"RSTP System Configuration"** table allows configuring the spanning tree parameters.

Figure 4-57 RSTP System Configuration

The page includes the following fields: **table 4-18** description of the RSTP System Configuration.

Item	Description
RSTP Enabled	**Enabled** –Enabled the **RSTP**. **Disabled** -Disable the **RSTP**. Default is **Disable**.
System Priority	Specifies the bridge priority value. When switches or bridges are running **STP**, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the Root Bridge. The bridge priority value is provided in increments of 4096 (4K increments). For example, 0, 4096, 8192, etc. The default value is **32768**.
Hello Time	Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a root bridge waits between configuration messages. Value Range : 1-10 The default is **2** seconds.
Max Age	Specifies the device Maximum Age Time. The Maximum Age Time indicates the amount of time in seconds a bridge waits before sending configuration messages. Value Range : 6-40 The default max age is **20** seconds.
Forward Delay	Specifies the device forward delay time. The Forward Delay Time indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. Value Range : 4-30 The default is **15** seconds.
Force Version	Specifies the Force Protocol Version parameter for the switch. The options are Normal and Compatible

	Normal – Rapid STP (802.1w): Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.
	Compatible – Classis STP (802.1d): Provides a single path between end stations, avoiding and eliminating loops.
Loop Detection	Enable or disable the loop detection.

Table 4-18 Description of the RSTP System Configuration

> **Note**
> - **Max Age -**. The value lies between 6 and 40, with the value being less than or equal to "(2 * Bridge Forward Delay) - 1" and greater than or equal to "**2 * (Bridge Hello Time +1)**". The default value is 20.
> - **Hello Time -** The value being less than or equal to "**(Bridge Max Age / 2) - 1**". The default hello time value is 2.
> - **Forward Delay-** Bridge Forward Delay must be greater or equal to "**(Bridge Max Age / 2) + 1**". The time range is from 4 seconds to 30 seconds. The default value is 15.

4.7.4 Port Configuration

The RSTP Port Configuration page contains fields for assigning RSTP properties to individual ports. The screen in Figure 4-58 appears.
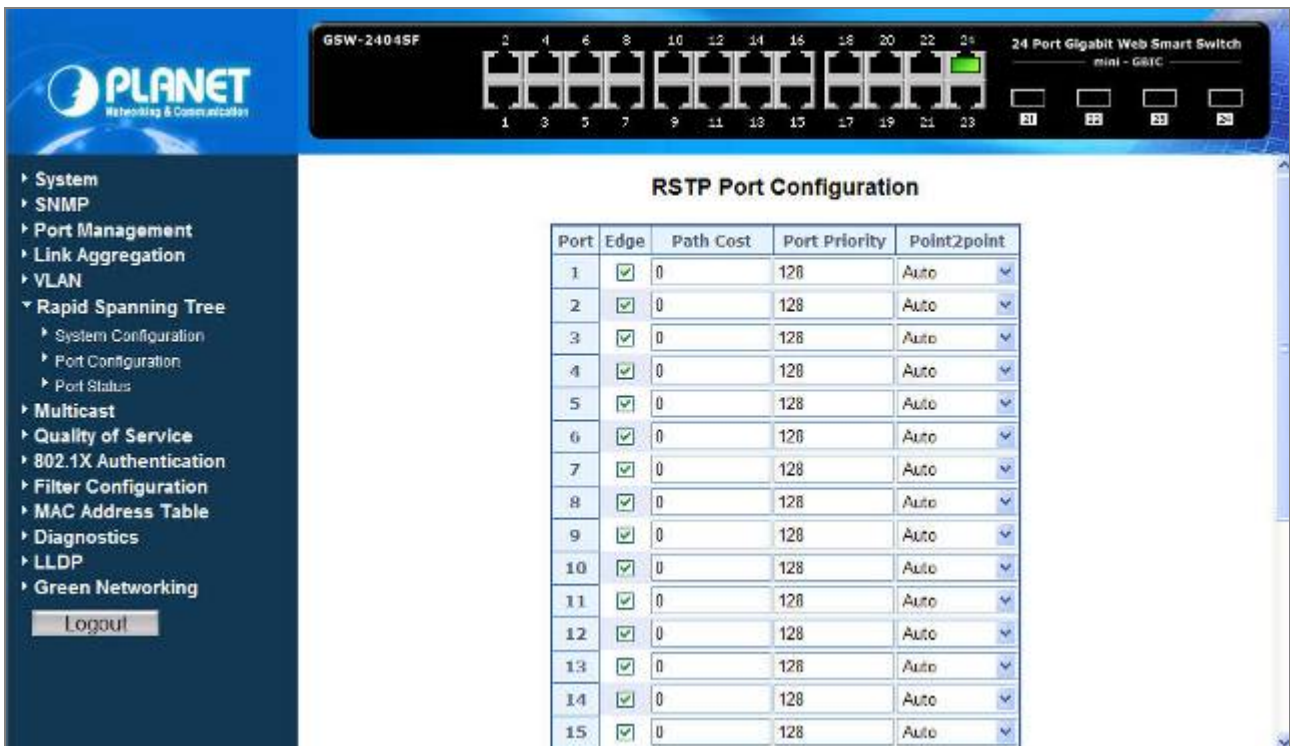
Figure 4-58 RSTP Port Configuration

The page includes the following fields: **table 4-19** description of the RSTP Port Configuration.

Item	Description
Port	Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF).
Edge	Enable or disable the function.
Path Cost	The port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted. Value Range : 1 to 200000000. Default Path Cost -- The default path cost of the port is automatically set by the port speed and the default path cost method. The default values for path costs are: - Ethernet - 2000000 - Fast Ethernet - 200000 - Gigabit Ethernet - 20000
Port Priority	The value of the port priority. The default value is **"128"**.
Point2Point	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. Transitions to the forwarding state are faster for point-to-point LANs than for shared media. (This applies to physical ports only. Aggregations are always *forced Point2Point*). The available options are shown as below: **Force True** **Force False** **Auto (Default value)**
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh RSTP Port Configuration screen of Web Smart Gigabit Switch.

Table 4-19 Description of the RSTP Port Configuration

4.7.5 Port Status

The RSTP Port Status page display the current STP bridge , roor bridge and per port stp status. The **"RSTP VLAN Bridge Overview"** and **"RSTP Port Status"** screen is displayed as in Figure 4-59.
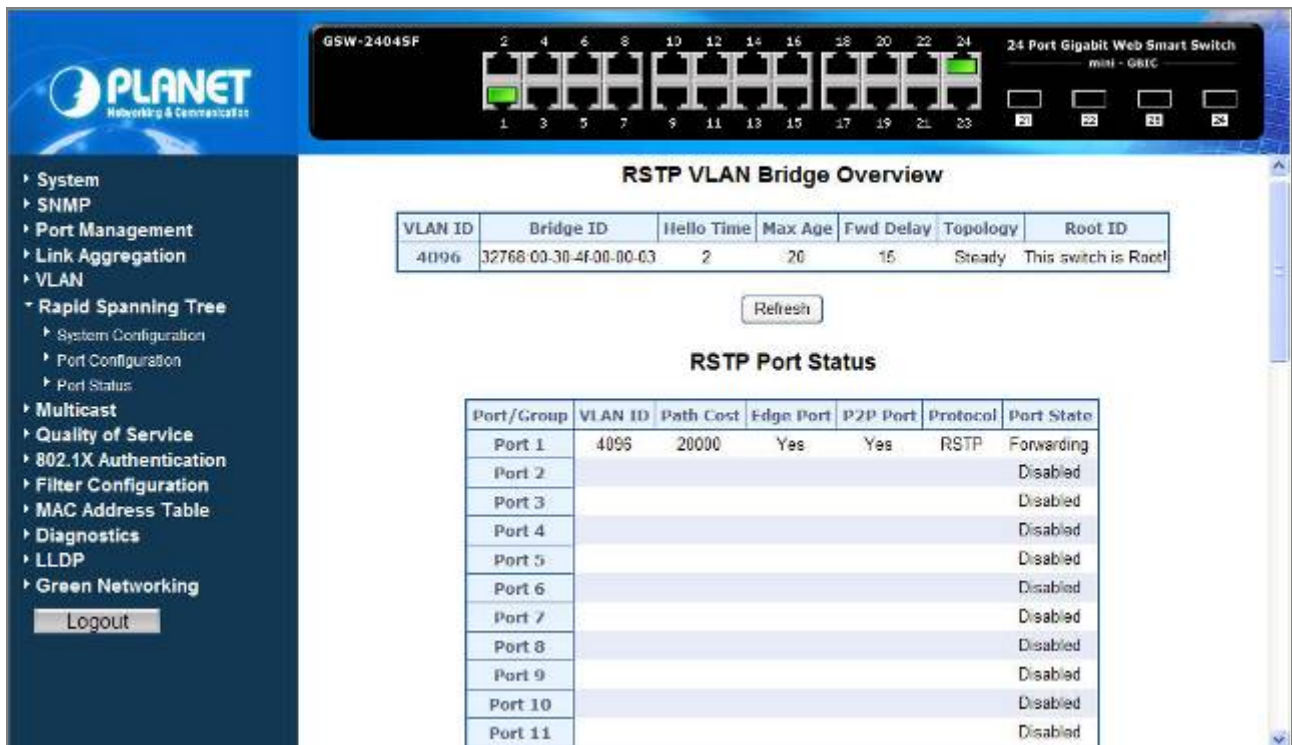
Figure 4-59 RSTP Port Status

■ **RSTP VLAN Bridge Overview**

The information of the RSTP Root shows in the Bridge overview table. The screen in Figure 4-60 appears.

Figure 4-60 RSTP VLAN Bridge Overview

The page includes the following fields: **table 4-20** description of the RSTP VLAN Bridge Overview.

• Item	Description
VLAN ID	Identifies VLANs associated with the Rapid Spanning Tree.
Bridge ID	Identifies the Bridge priority and MAC address.
Hello Time	Minimum time between transmissions of Configuration BPDUs.

Max Age	Path Cost to the Designated Root for the spanning tree.
Forward Delay	Derived value of the Root Port Bridge Forward Delay parameter.
Topology	Specifies the Tolology change status of the current operation. If no topology change happened, the table show "**Steady**".
Root ID	Identifies the Root Bridge priority and MAC address.
Refresh	Press this button for refresh RSTP VLAN Bridge Overview screen of Web Smart Gigabit Switch.

Table 4-20 Description of the RSTP VLAN Bridge Overview

■   **RSTP Port Status**

The information of the RSTP per Port and Trunk group shows in the RSTP Port Status table. The screen in Figure 4-61 appears.

Figure 4-61 RSTP Port Status screen

The page includes the following fields: **table 4-21** description of the RSTP Port status.

Item	Description
Port/Group	Port or Link Aggregation group on which Rapid STP is enabled
VLAN ID	Port or Link Aggregation interfaces associated with VLANs associated with the Rapid Spanning Tree.

Path Cost	Cost of the port participating in the RSTP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Edge Port	Indicates whether the port is enabled as an edge port. It takes the value "Yes" or "No".
P2p Port	The Point-to-Point operating state. This is the actual device port link type.
Protocol	Indicates the current spanning protocol on the ports.
Port State	The current port STP state. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are: • **Disabled --** The port link is currently down. • **Blocking --** The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled. • **Listening --** The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses. • **Learning --** The port is currently in the learning mode. The port cannot forward traffic however it can learn new MAC addresses. • **Forwarding --** The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.

Table 4-21 Description of the RSTP Port Status

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

■   **RSTP Port Statistics**

The information of the RSTP per Port and Trunk group shows in the RSTP Port Status table. The screen in Figure 4-62 appears.
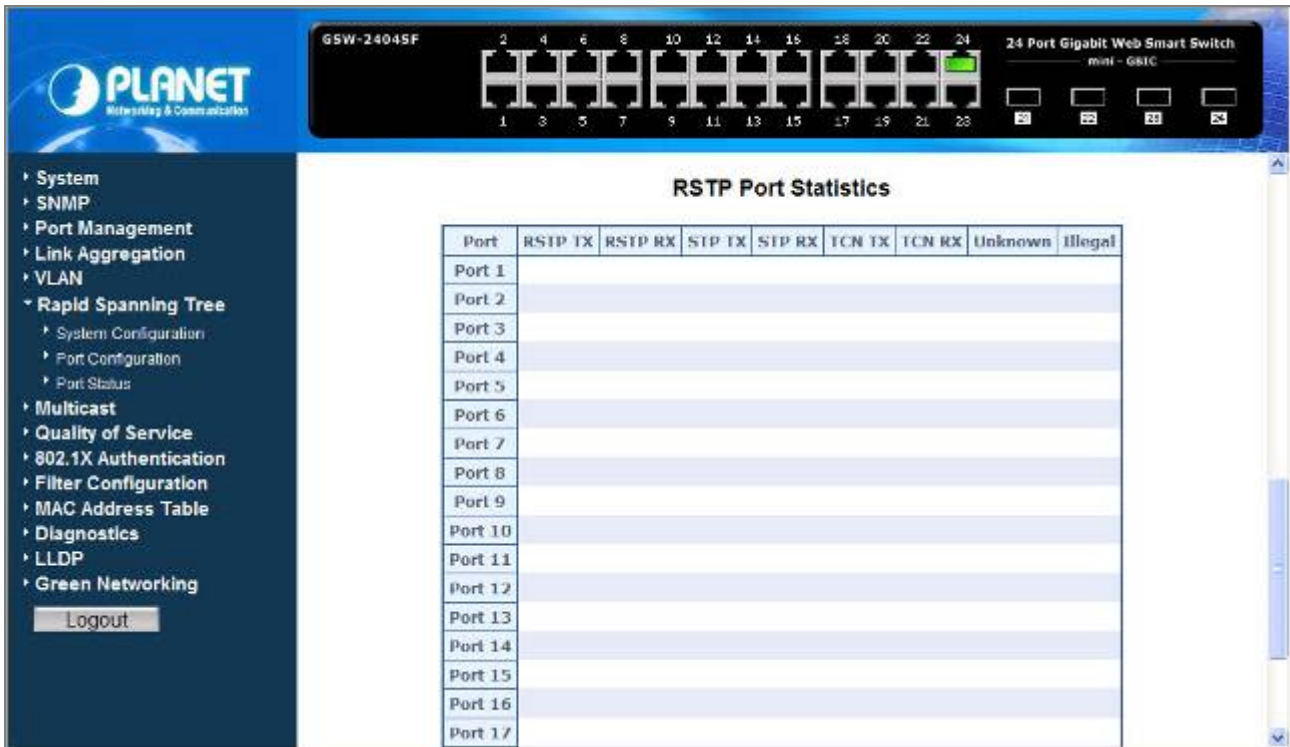
Figure 4-62 RSTP Port Statistics screen

The page includes the following fields: **table 4-22** description of the RSTP Port Statistics.

Item	Description
Port	Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF).
RSTP TX	The number of RSTP Configuration BPDU's transmitted on the port.
RSTP RX	The number of RSTP Configuration BPDU's received on the port.
STP TX	The number of legacy STP Configuration BPDU's transmitted on the port.
STP RX	The number of legacy STP Configuration BPDU's received on the port.
TCN TX	The number of (legacy) Topology Change Notification BPDU's transmitted on the port.
TCN RX	The number of (legacy) Topology Change Notification BPDU's received on the port.
Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Table 4-22 Description of the RSTP Port Statistics

4.8 Multicast

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 4-63 Multicast Service
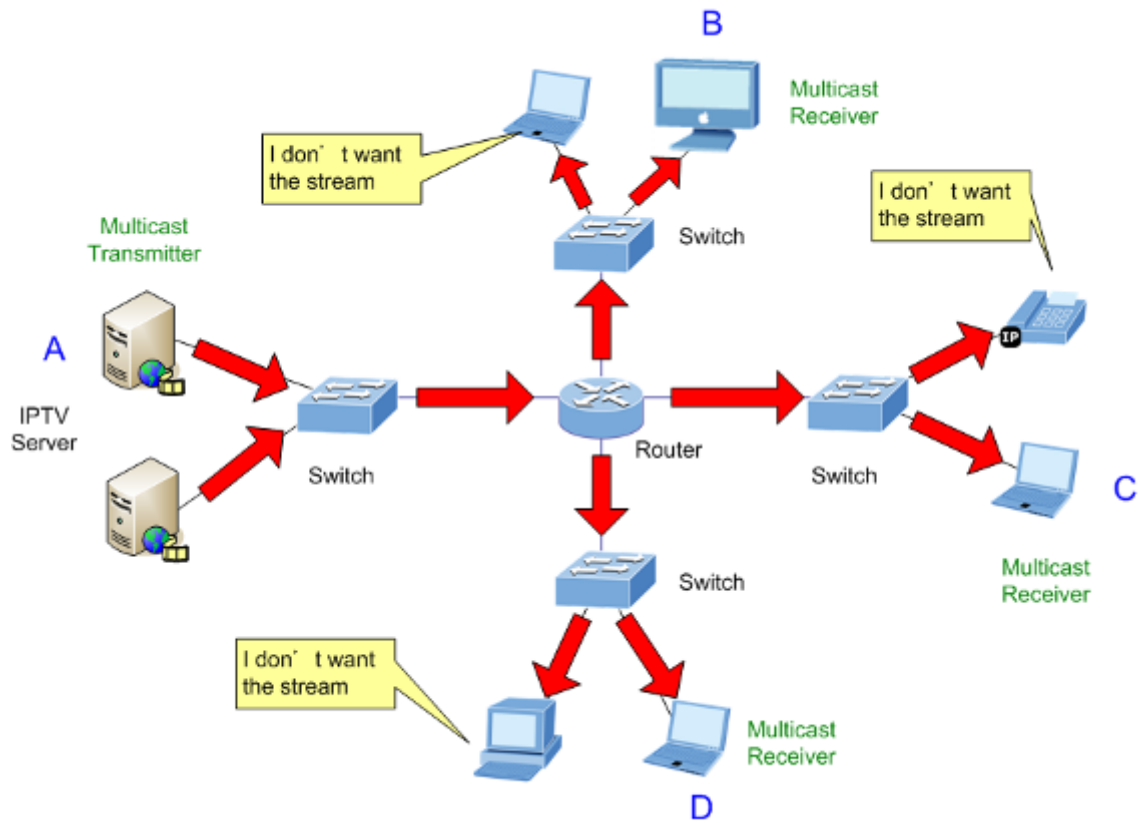
Figure 4-64 Multicast flooding
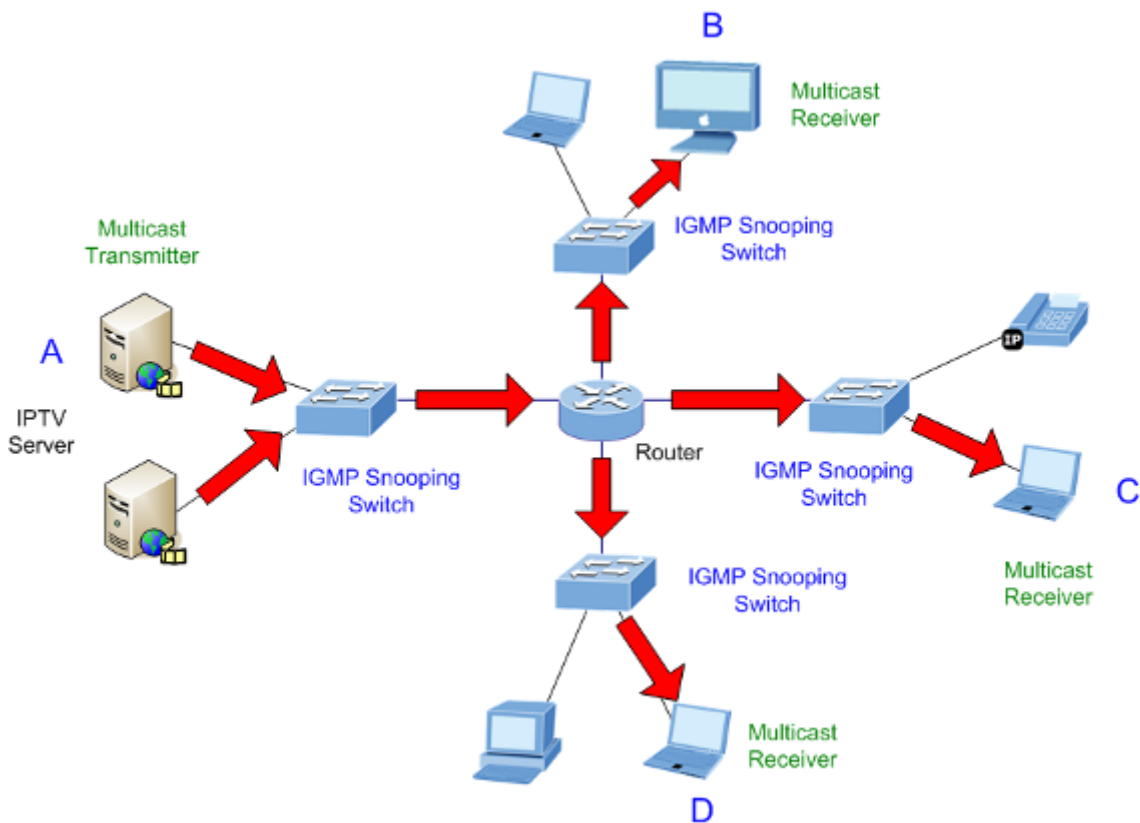
Figure 4-65 IGMP Snooping multicast stream control

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)
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 4-66 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.

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

4.8.1 IGMP Snooping Configuration

The IGMP Snooping Configuration allow administrator to configure the parameters for IGMP Snooping, which is used to build forwarding lists for multicast traffic. The screen in Figure 4-67 appears.
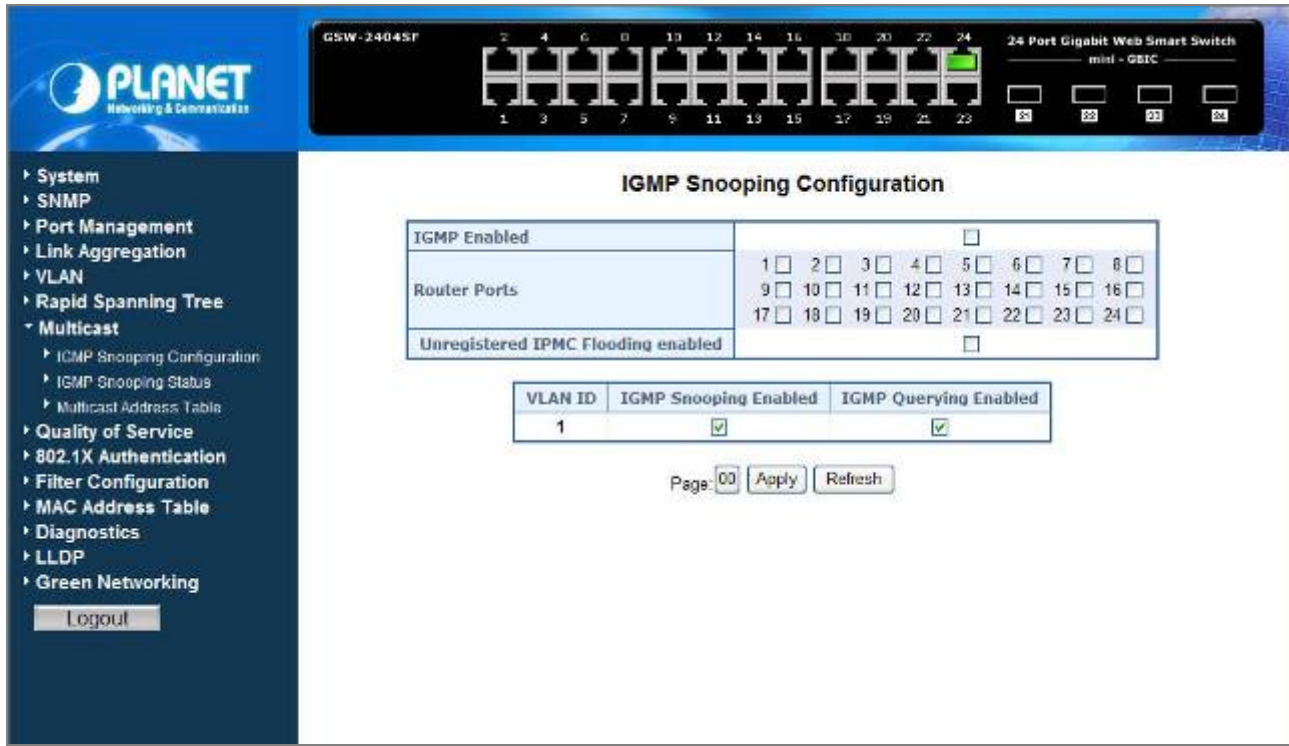
Figure 4-67 IGMP Snooping Configuration and Status

The page includes the following fields: **table 4-23** description of the **IGMP** Snooping Configuration.

Item	Description
IGMP Enable	Enables or disables IGMP global function on the device. Default mode is **Disable**.
Router Ports	The Router Ports check box fields for attaching ports to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port .
Unregistered IPMC Flooding Enable	The function is to set **"Enable"** or **"Disable"** to allow the unregistered IP Multicast Group streams to flood to all ports of this switch. The unregistered IP Multicast means that the received Multicast Group address not listed in the Multicast Group Table of the switch. Enabled is the default value. The switch forwards all the multicast steams to all the host or linked switch.
VLAN ID	Identifies a VLAN and contains information about the Multicast group configuration. Add a new VLAN group and the Table will add the VLAN entry automatically.

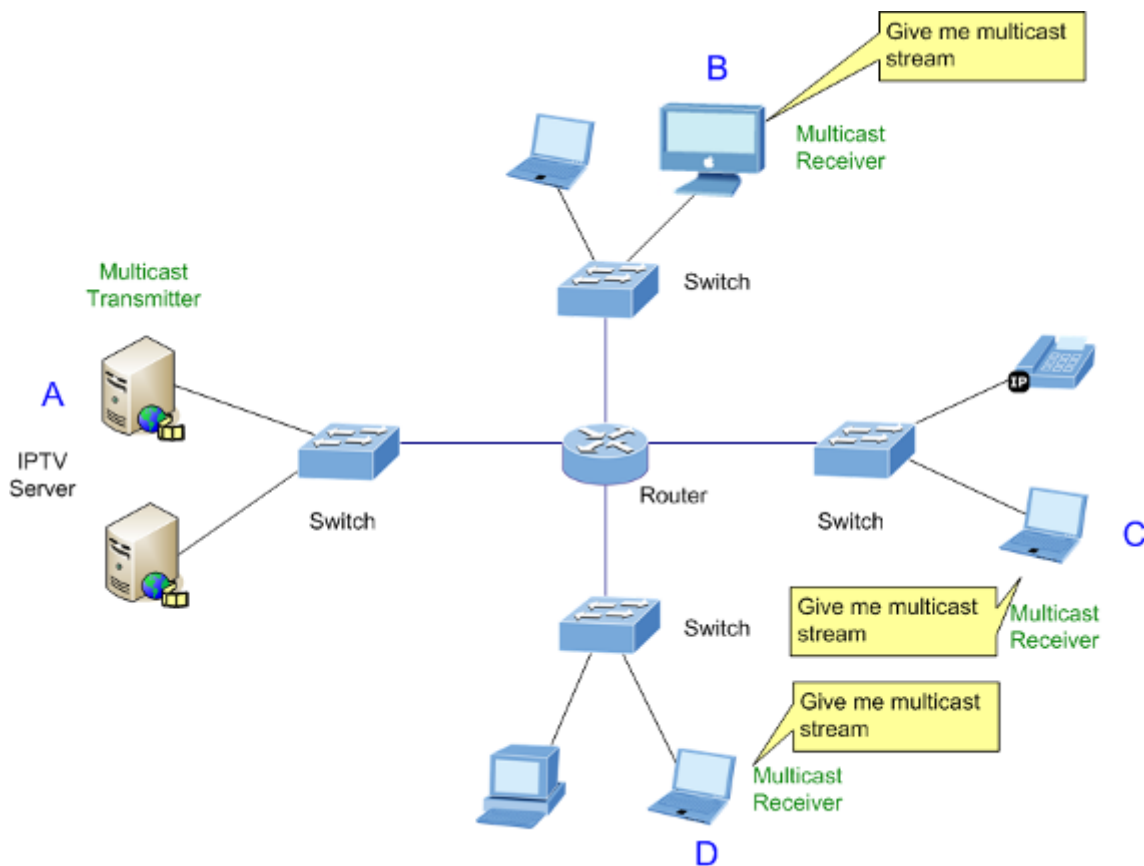|	
IGMP Snooping Enabled	Enables or disables IGMP snooping on the VLAN. Ports be assign to the VLAN will be applied to filter the Multicast stream. Default mode is **Enable**.
IGMP Querying Enabled	Enables or disables IGMP Query mode on the VLAN. The Query mode is used to periodically check the multicast 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. Default mode is **Enable**.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh IGMP Snooping Configuration screen of Web Smart Gigabit Switch.

Table 4-23 Description of the IGMP Snooping Configuration

Add a new VLAN group, the VLAN ID will be added to the table automatically with both **"IGMP Snooping Enabled"** and **"IGMP Querying Enabled"**

4.8.2 IGMP Snooping Status

The IGMP Snooping Status display the current IGMP Status and the statistics of received Query / report packets. The **"IGMP Snooping Status"** screen is displayed as in Figure 4-68.
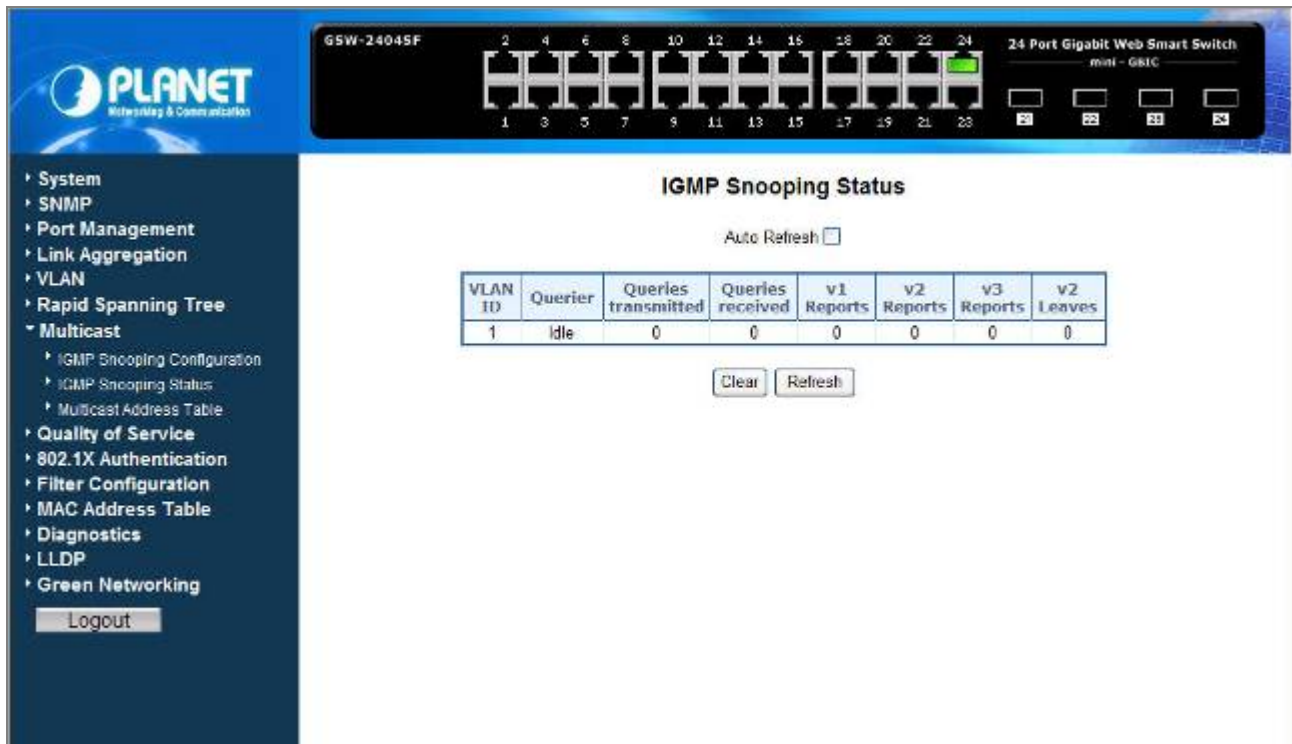
Figure 4-68 IGMP Snooping Status

The page includes the following fields: **table 4-24** description of the **IGMP** Snooping Status.

Item	Description
Auto Refresh	Disable or Enable the **Auto Refresh** function. While set to enable, the IGMP Snooping Status l will refresh automatically every **30** seconds.
VLAN ID	Identifies a VLAN and contains information about the Multicast group configuration.
Querier	Display the current status of IGMP Querier on the device. **Active** – The IGMP Query function had been enabled on the device and played as a main Querier within a subnet domain. Within a network domain, there will be only one IGMP Querier. While two or more Querier exist, only one Querier operation by election. The Querier will transmit a IGMP Query packet about every 125 secs. **Idle** – The IGMP Querier function had be enabled but might be at the initiation status, or there're already other Querier exist.
• **Queries transmitted**	Statistics of IGMP Query packets transmitted from the VLAN. Only the "IGMP Querying

	Enabled" be checked, the counter is active.
• **Queries received**	Statistics of IGMP Query packets received at the VLAN –from another switches or routers.
• **V1 Reports**	Statistics of IGMP V1 report packets received at the VLAN. (Packets with content type = **0x12** ; The Membership Report (version 1))
• **V2 Reports**	Statistics of IGMP V2 report packets received at the VLAN. (Packets with content type = **0x16** ; The Membership Report (version 2))
• **V3 Reports**	Statistics of IGMP V3 report packets received at the VLAN.
• **V2 Leaves**	Statistics of IGMP V2 leave packets received at the VLAN. (Packets with content type = **0x17** ; Leave a Group (version 2))
Button	
Clear	Press this button for clear IGMP Snooping Status counter values of Web Smart Gigabit Switch.
Refresh	Press this button for refresh IGMP Snooping Status screen of Web Smart Gigabit Switch.

Table 4-24 Description of the **IGMP** Snooping Status

4.8.3 Multicast Address Table

The Multicast Address Table displays the ports attached to the Multicast service group in the Ports tables. The Port a tables also reflect the manner in which the port joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. The Bridge Multicast Group page permits new Multicast service groups to be created. The Bridge Multicast Group page also assigns ports to a specific Multicast service address group. The Multicast Address Table screen is displayed as in Figure 4-69.
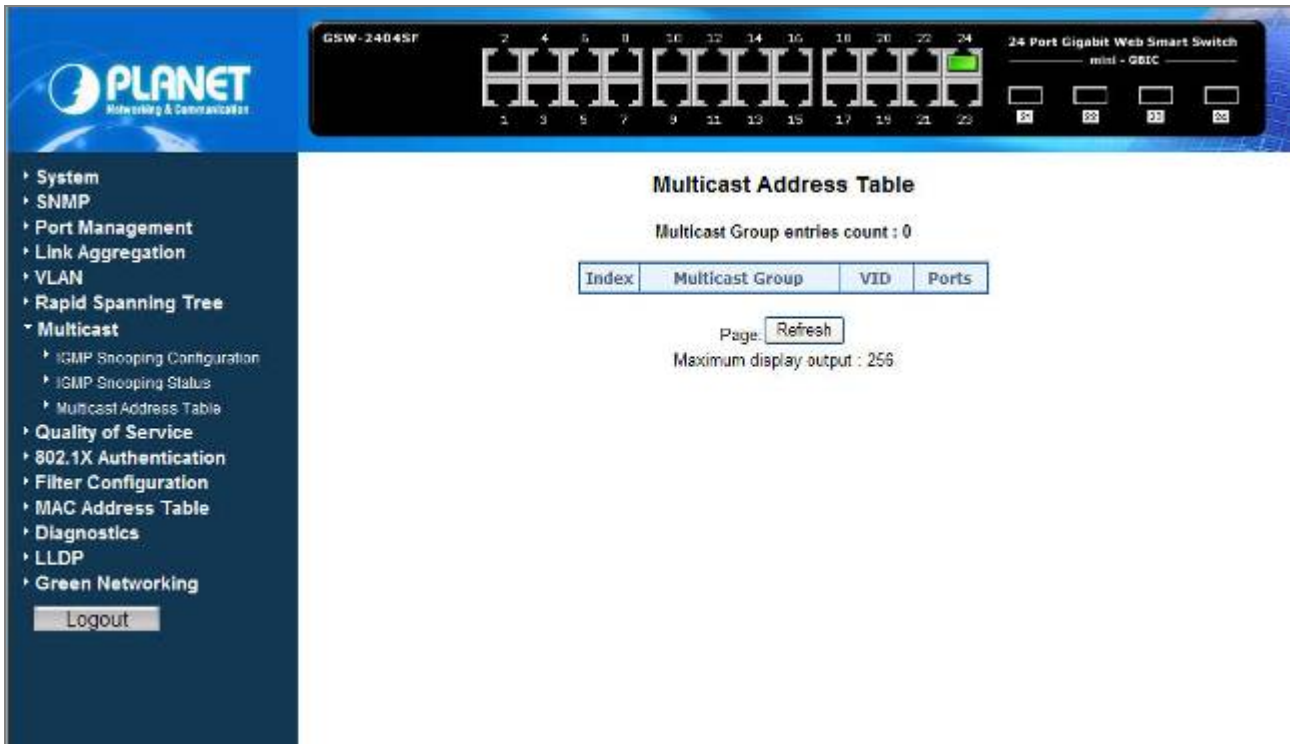
Figure 4-69 The Multicast Address Table

The page includes the following fields: **table 4-25** description of the Multicast Address Table.

Item	Description
Index	The total count of the current Multicast Group entries of the Web Smart Gigabit Switch.
Multicast Group	Identifies the Multicast group MAC address/IP address
VID	Identifies a VLAN and contains information about the Multicast group address.
Ports	Identifies assigned ports to a specific Multicast service address group- By received Join or leave packets.
Button	
Refresh	Press this button for refresh Multicast Address Table screen of Web Smart Gigabit Switch.

Table 4-25 Description of the Multicast Address Table

The Multicast Address Table display 256 Multicast Address groups maximum.

4.9 Quality of Service

4.9.1 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:

- 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.

The **QoS Configuration** page contains fields for enabling or disabling QoS. In addition, the 802.1p mode or DSCP mode can be selected. Both the two mode rely on predefined fields within the packet to determine the output queue.

- ■ **QoS Disabled** - Disables managing network traffic using Quality of Service.

- ■ **802.1p** Mode –The output queue assignment is determined by the IEEE802.1p VLAN priority tag.

- ■ **DSCP** Mode - The output queue assignment is determined by the DSCP field.

> **Note**
> The GSW-1602SF/GSW-2404SF support QoS **Strict** mode only, the strict mode is to specifies if traffic scheduling is based strictly on the queue priority.

4.9.2 QoS Configuration

The **QoS Configuration** page contains fields for enabling or disabling QoS. In addition, the **802.1p** mode or **DSCP** mode can be selected. Both the two mode rely on predefined fields within the packet to determine the output queue. The QoS Configuration page in Figure 4-70 appears.
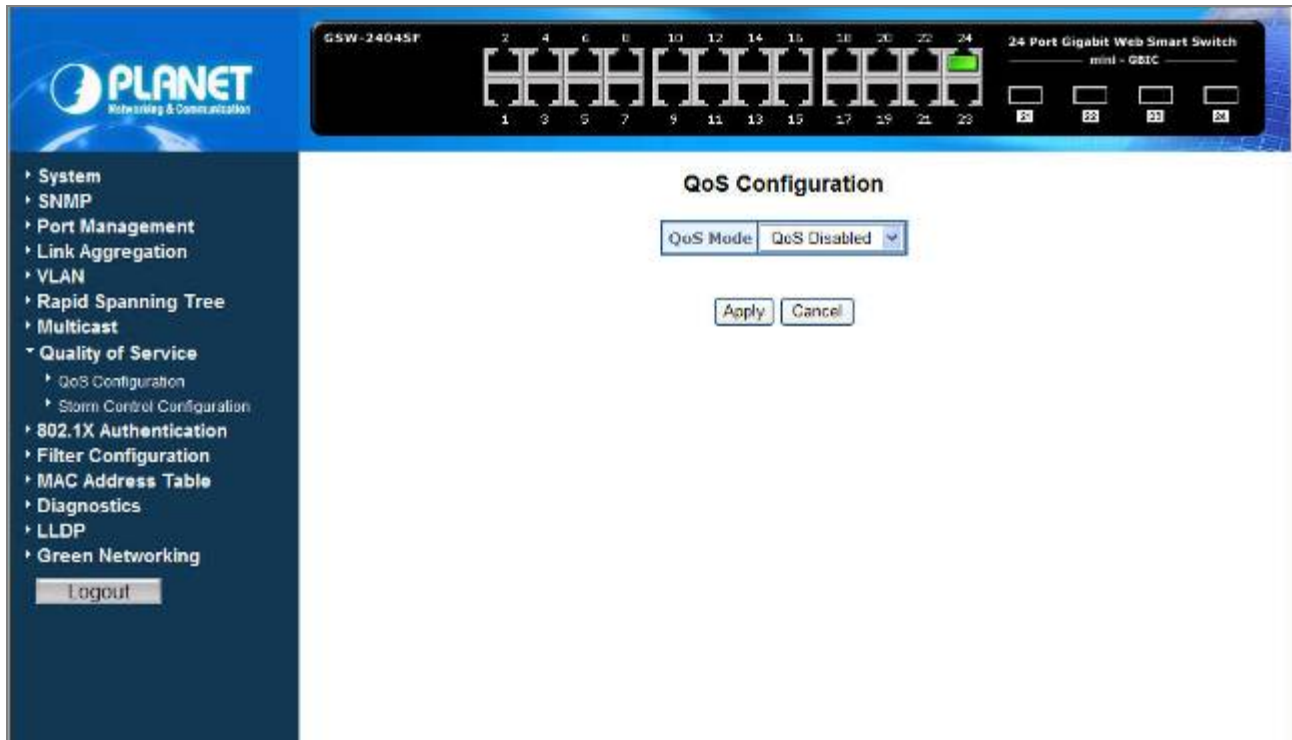
Figure 4-70 QoS Configuration screen

The page includes the following fields:

Item	Description
Queue Mode	This indicates that traffic scheduling for the selected queue is based **strictly** or **WRR (Weight Round Robin)** on the queue priority.
QoS Mode	Configure the QoS mode for the switch: ■ **QoS Disabled** - Disables managing network traffic using Quality of Service. ■ **802.1p** Mode –The output queue assignment is determined by the IEEE802.1p VLAN priority tag. ■ **DSCP** Mode - The output queue assignment is determined by the DSCP field.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Cancel	Press this button for ignore current configuration of Web Smart Gigabit Switch.

4.9.3 802.1p QoS Mode

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. When 802.1p Tag Priority is applied, the Web Smart Switch recognizes 802.1Q VLAN tag packets and extracts the VLAN tagged packets with User Priority value.

802.1Q Tag and 802.1p priority

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	46-1517 bytes	4 bytes
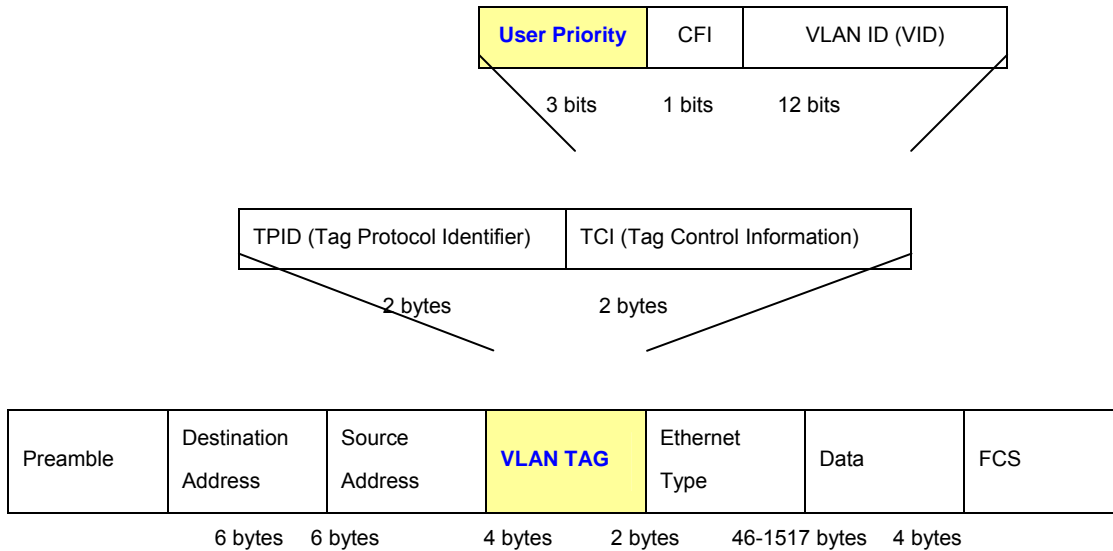
The IEEE 802.1p Priority specification uses 8 priority levels to classify data packets. The screen in Figure 4-71 and Figure 4-72 appears.
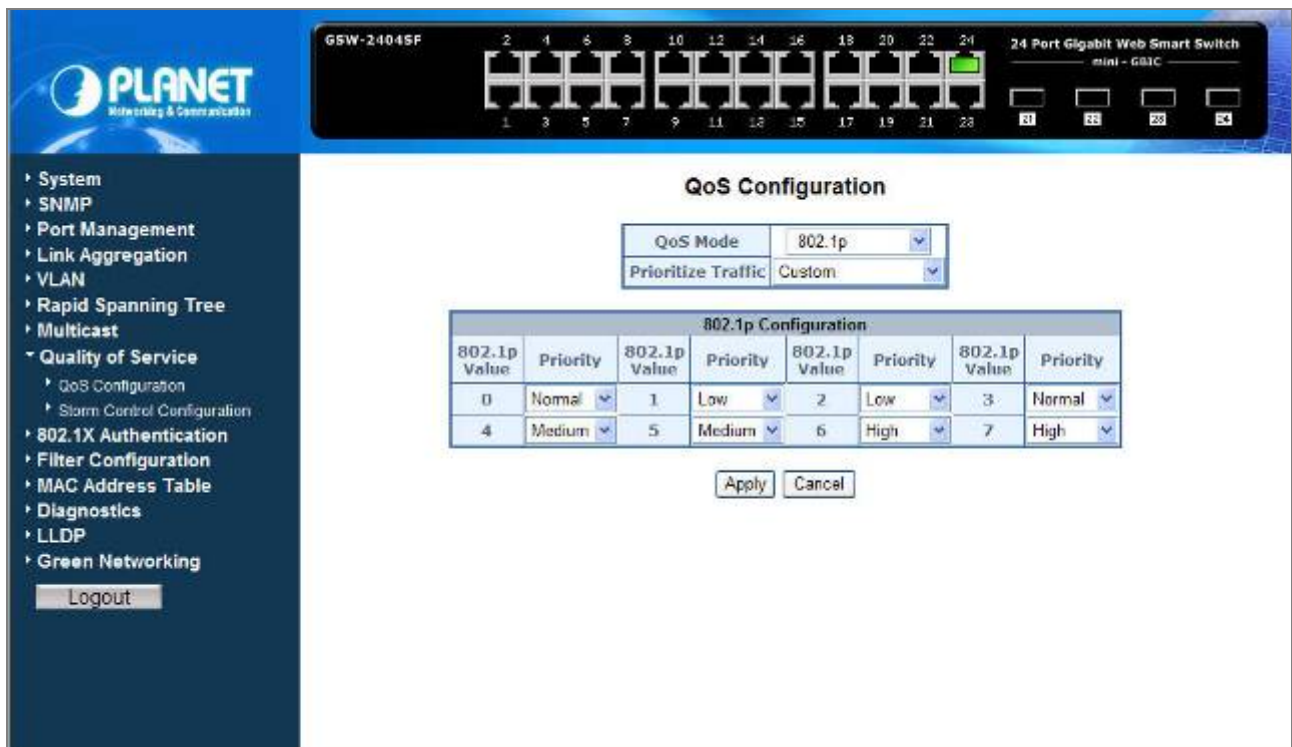
Figure 4-71 802.1p QoS Configuration screen

QoS Configuration

| QoS Mode | 802.1p |
| Prioritize Traffic | Custom |

Custom
All Low Priority
All Normal Priority
All Medium Priority
All High Priority

Figure 4-72 Prioritize Traffic screen

The page includes the following fields: **table 4-26** Description of the QoS Configuration.

Item	Description
Prioritize Traffic	The draw menu allows customization of 802.1p to Traffic classifiers. Total 5 selections for the Prioritize Traffic. • **Custom –** Manual mapping the 802.1p priority to the 4-level queues. Setup at the next table. • **All Low Priority** - mapping all 802.1p tagged packets to **Queue 0** • **All Normal Priority** - mapping all 802.1p tagged packets to **Queue 1** • **All Medium Priority** - mapping all 802.1p tagged packets to **Queue 2** • **All High Priority** - mapping all 802.1p tagged packets to **Queue 3**
802.1p Value	Specifies the CoS priority tag values, where zero is the lowest and 7 is the highest.
Priority	The traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported as follow : • **Low** = Queue 0 • **Normal** = Queue 1 • **Medium** = Queue 2 • **High** = Queue 3
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Cancel	Press this button for ignore current configuration of Web Smart Gigabit Switch.

Table 4-26 Description of the QoS Configuration

4.9.4 DSCP QoS Mode

DiffServ Code Point (DSCP) － is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.

The **DSCP Configuration** page provides fields for defining output queue to specific DSCP fields.
Select the QoS mode to DSCP, the DSCP to queue mapping configuration page appears, as the Figure 4-73 shows.
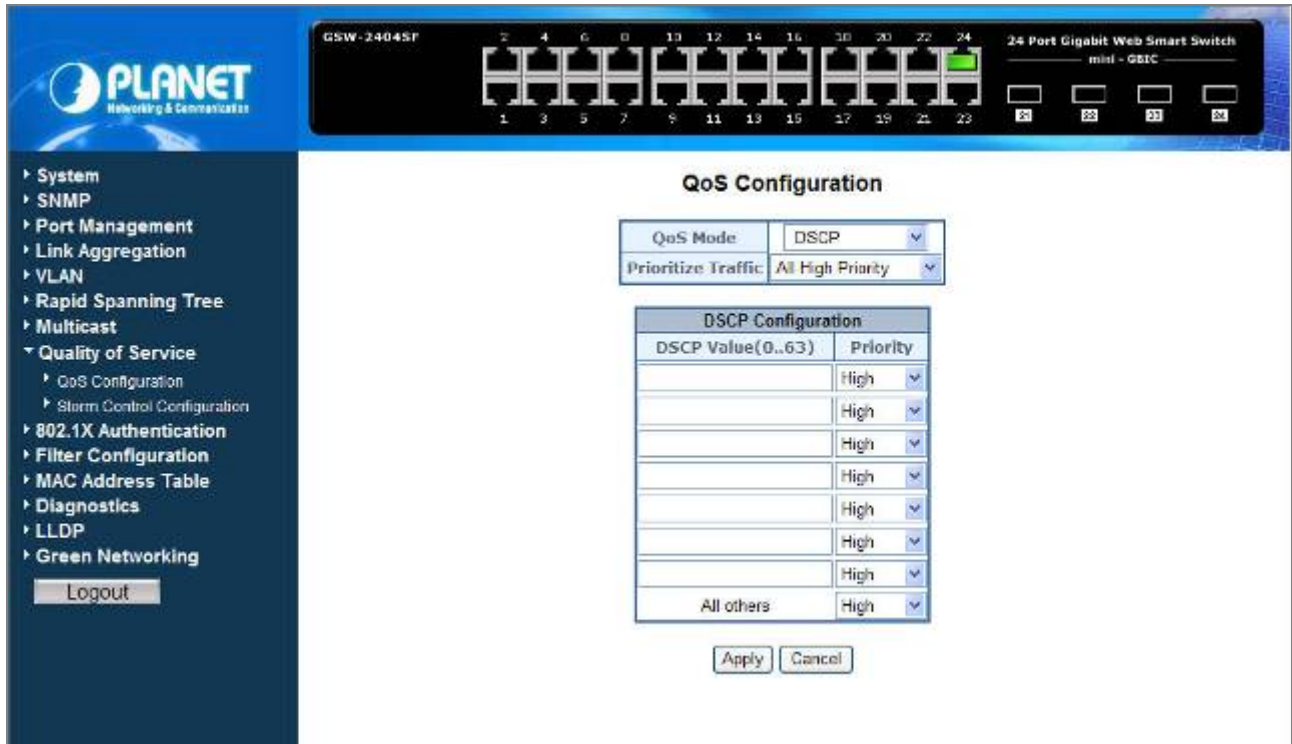
Figure 4-73 DSCP QoS Configuration screen

The page includes the following fields: **table 4-27** Description of the DSCP QoS Configuration.

Item	Description
Prioritize Traffic	The draw menu allows customization of DSCP to Traffic classifiers. Total 5 selections for the Prioritize Traffic. • **Custom –** Manual mapping the DSCP to the 4-level queues. Setup at the next table. • **All Low Priority** - mapping all IP DCSP header packets to **Queue 0** • **All Normal Priority** - mapping all IP DCSP header packets to **Queue 1** • **All Medium Priority** - mapping all IP DCSP header packets to **Queue 2** • **All High Priority** - mapping all IP DCSP header packets to **Queue 3**
DSCP Value (0..63)	The values of the IP DSCP header field within the incoming packet.
Priority	The traffic forwarding queue to which the DSCP is mapped. Four traffic priority queues are supported.

	The queue to which packets with the specific DSCP value is assigned. The values are low,Normal,Medium and High. • **Low** = Queue 0 • **Normal** = Queue 1 • **Medium** = Queue 2 • **High** = Queue 3
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Cancel	Press this button for ignore current configuration of Web Smart Gigabit Switch.

Table 4-27 Description of the DSCP QoS Configuration

4.9.5 Storm Control Configuration

This function provide various type of storm control of the device, such as ICMP Rate , Learn Frames Rate, Broadcast Rate, Multicast Rate and Flooded unicast Rate. The Storm Control screen in Figure 4-74 appears.
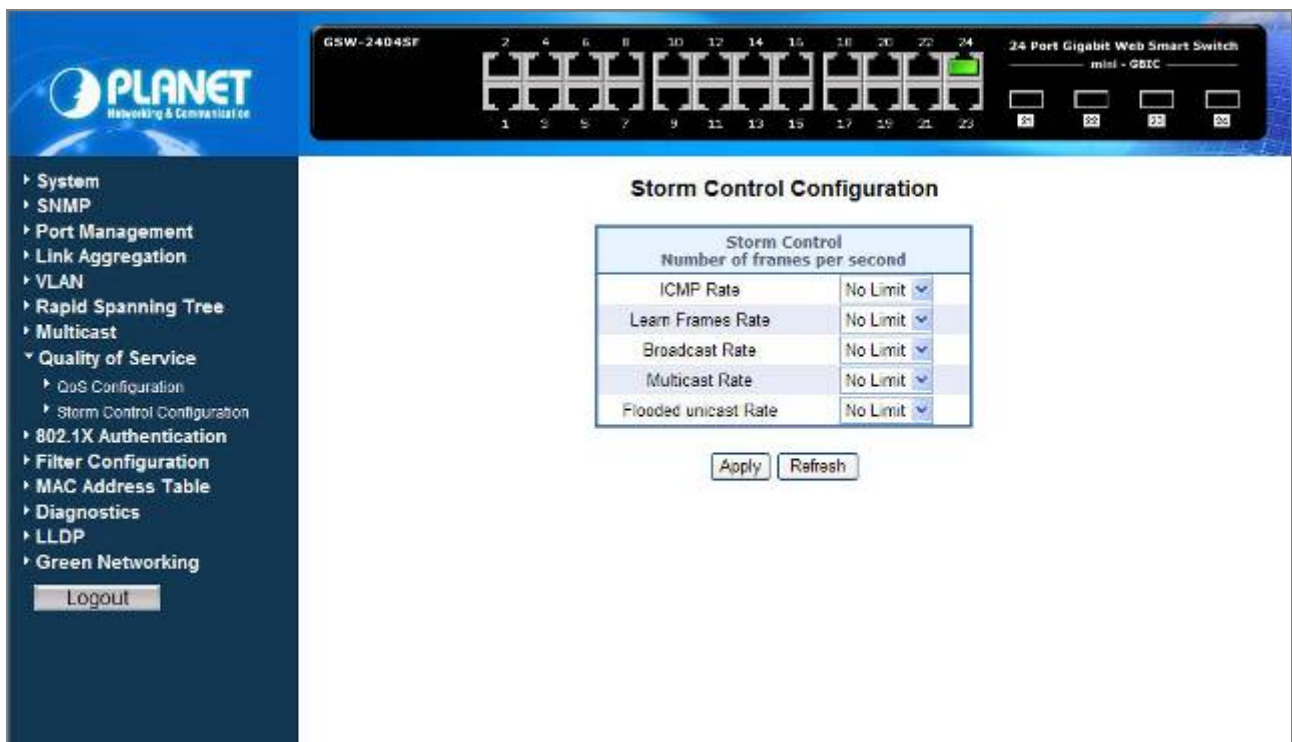
Figure 4-74 Storm Control Configuration

The page includes the following configurable data **table 4-28** description of the Storm Control.

Item	Description
ICMP Rate	This function allows to filter the ICMP storm traffic, the available options are 1K/2K/4K/8K/16K/32K/64K/128K/256K/512K/1024K/2048K/4096K/8192K/1638K4/32768K and **"No Limit"(Default mode)**.
Learn Frames Rate	This function allows to filter the learn frames storm traffic, the available options are 1K/2K/4K/8K/16K/32K/64K/128K/256K/512K/1024K/2048K/4096K/8192K/1638K4/32768K and **"No Limit"(Default mode)**.
Broadcast Rate	This function allows to filter the broadcast storm traffic, the available options are 1K/2K/4K/8K/16K/32K/64K/128K/256K/512K/1024K/2048K/4096K/8192K/1638K4/32768K and **"No Limit"(Default mode)**.
Multicast Rate	This function allows to filter the multicast storm traffic, the available options are 1K/2K/4K/8K/16K/32K/64K/128K/256K/512K/1024K/2048K/4096K/8192K/1638K4/32768K and **"No Limit"(Default mode)**.
Flooded unicast Rate	This function allows to filter the flooded unicast storm traffic, the available options are 1K/2K/4K/8K/16K/32K/64K/128K/256K/512K/1024K/2048K/4096K/8192K/1638K4/32768K and**"No Limit"(Default mode)**.

Table 4-28 Description of the Storm Control Configuration

4.10 802.1X Authentication

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

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

The PLANET GSW-1602SF / GSW-2404SF supports IEEE 802.1X Port-base network access control and RADIUS server authentication to enhance the host link more security. An 802.1X Infrastructure is composed of three major components: Authenticator, Authentication server, and Supplicant.

Authentication server – (RADIUS Server): An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator.

Authenticator-(GSW-1602SF / GSW-2404SF): An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.

Supplicant-(A Host Client): An entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link.

The instructions are divided into three parts:
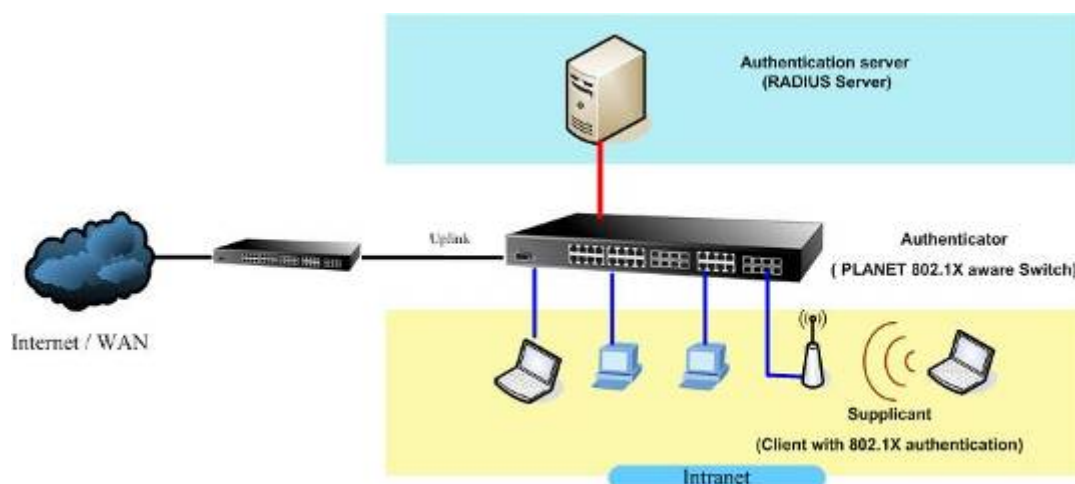
The above graph shows the network topology of the solution we are going to introduce. As illustrated, a group of clients is trying to build a network with GSW-1602SF / GSW-2404SF in order to have access to both Internet and Intranet. With 802.1X authentication, each of these clients would have to be authenticated by RADIUS server. If the client is authorized, GSW-1602SF / GSW-2404SF would be notified to open up a communication port to be used for the client. There are 2 Extensive Authentication Protocol (EAP) methods supported: (1) MD5 and (2) TLS.

MD5 authentication is simply a validation of existing user account and password that is stored in a database of RADIUS server. Therefore, clients will be prompted for account/password validation to build the link. TLS authentication is a more complicated authentication, which is using certificate that is issued by RADIUS server for authentication. TLS authentication is a more secure authentication, since not only RADIUS server authenticates the client, but also the client can validate RADIUS server by the certificate that it issues. The TLS authentication request from clients and reply by Radius Server and GSW-1602SF / GSW-2404SF can be briefed as follows:
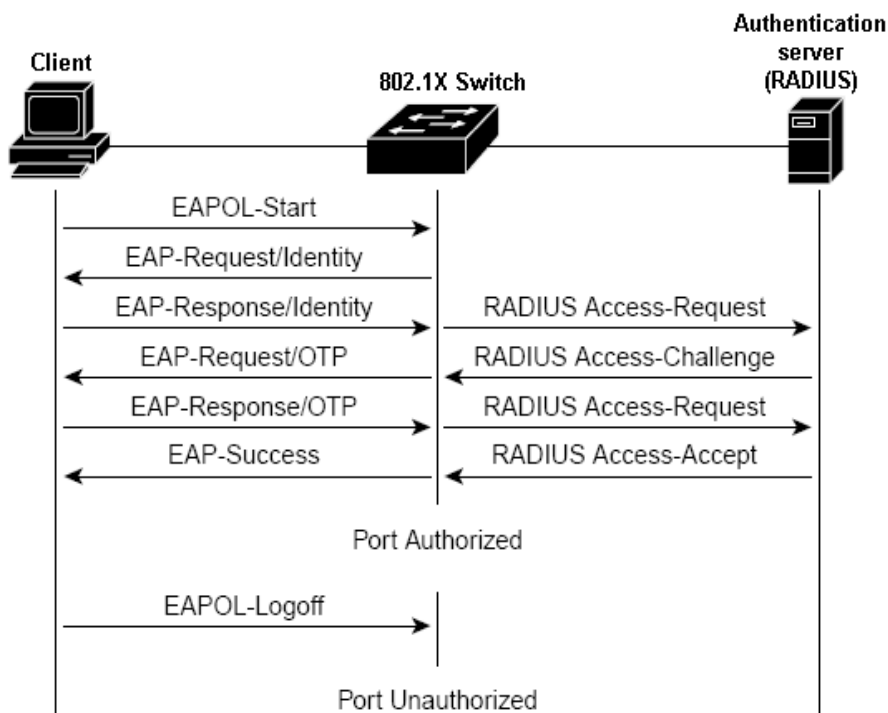
1. The client sends an EAP start message to Web Smart Gigabit Switch.

2. Web Smart Gigabit Switch replies with an EAP Request ID message.

3. The client sends its Network Access Identifier (NAI) – its user name – to Web Smart Gigabit Switch in an EAP Respond message.

4. Web Smart Gigabit Switch forwards the NAI to the RADIUS server with a RADIUS Access Request message.

5. The RADIUS server responds to the client with its digital certificate.

6. The client validates the digital certificate, and replies its own digital certificate to the RADIUS server.

7. The RADIUS server validates client's digital certificate.

8. The client and RADIUS server derive encryption keys.

9. The RADIUS server sends Web Smart Gigabit Switch a RADIUS ACCEPT message.

10. Web Smart Gigabit Switch sends the client an EAP Success message along with the broadcast key and key length.

This section is to control the access of the Web Smart Gigabit Switch, includes the user access and management control.

The 802.1X Authentication page contains links to the following topics:

- **802.1X System Configuration**

- **802.1X Port Configuration**

4.10.1 802.1X System Configuration

This page is to configure the RADIUS server connection features. The screen in Figure 4-75 appears.
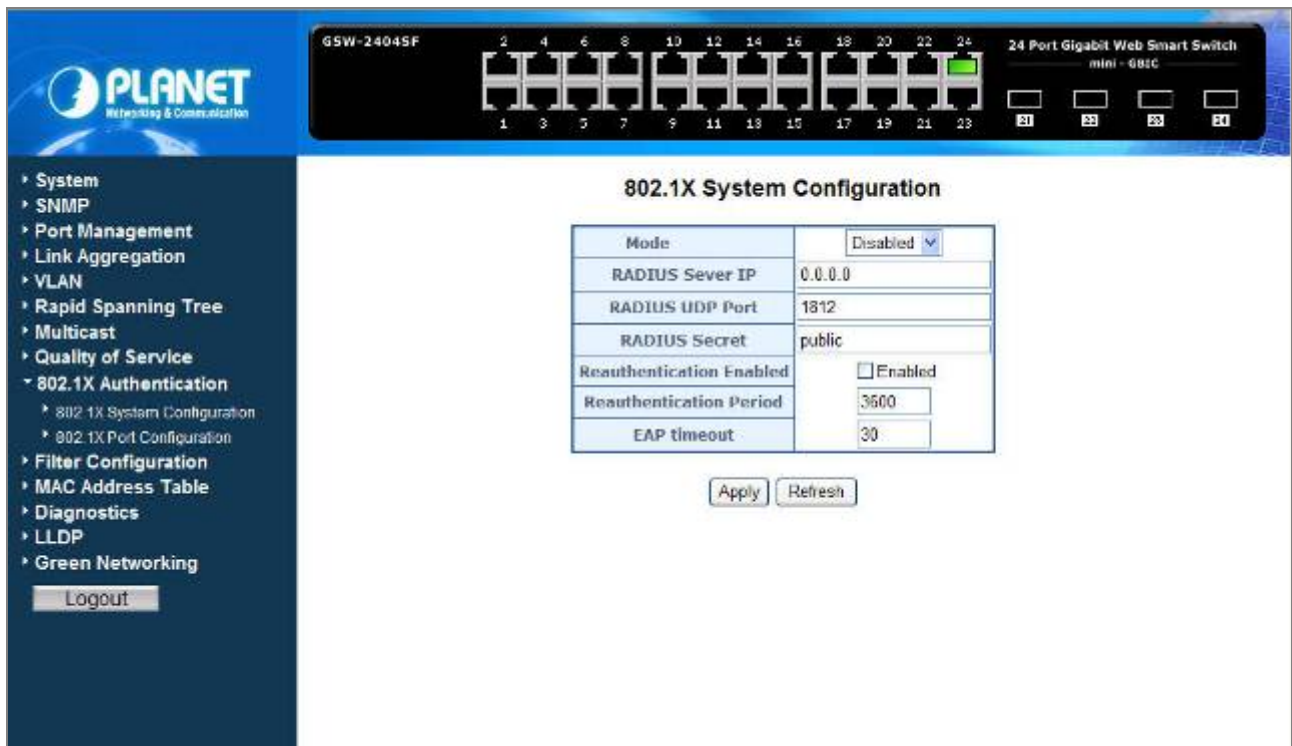
Figure 4-75 802.1X System Configuration

Table 4-29 Description of the 802.1X System Configuration.

Item	Description
Mode	To Enable / Disable the port access control administrative mode This selector lists the two options for administrative mode: **Enabled** and **Disabled**. The default mode is **Disabled**.
RADIUS Server IP	The IP address of the RADIUS server being added.
RADIUS UDP Port	The UDP port used by this server. The valid range is 0 - 65535. The default UDP Port No. is **1812**
RADIUS Secret	Indicates if the shared secret for this server has been configured.

Reauthentication Enabled	This select field allows the user to enable or disable reauthentication of the supplicant for the specified port. If "Enabled" be checked, reauthentication will occur. Otherwise, reauthentication will not be allowed. Changing the selection will not change the configuration until the Apply button is pressed. The default value is **not "Enabled"** .
Reauthentication Period [1-3600 seconds]	This input field allows the user to enter the reauthentication period for the selected port. The reauthentication period is the value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauthentication period must be a value in the range of 1 and 65535. Changing the value will not change the configuration until the Apply button is pressed. The default value is **3600**.
EAP Timeout [1-255 seconds]	This input field allows the user to enter the EAP timeout for the selected port. The EAP timeout is the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The EAP timeout must be a value in the range of 1 and 255. The default value is **30**.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh 802.1X System Configuration screen of Web Smart Gigabit Switch.

Table 4-29 Description of the 802.1X Configuration

Setup the RADIUS server and assign the client IP address to the Web Smart Gigabit Switch. In this case, field in the default IP Address of the Web Smart Gigabit Switch with 192.168.0.100. And also make sure the shared secret key is as same as the one you had set at the switch RADIUS server – 12345678 at this case.
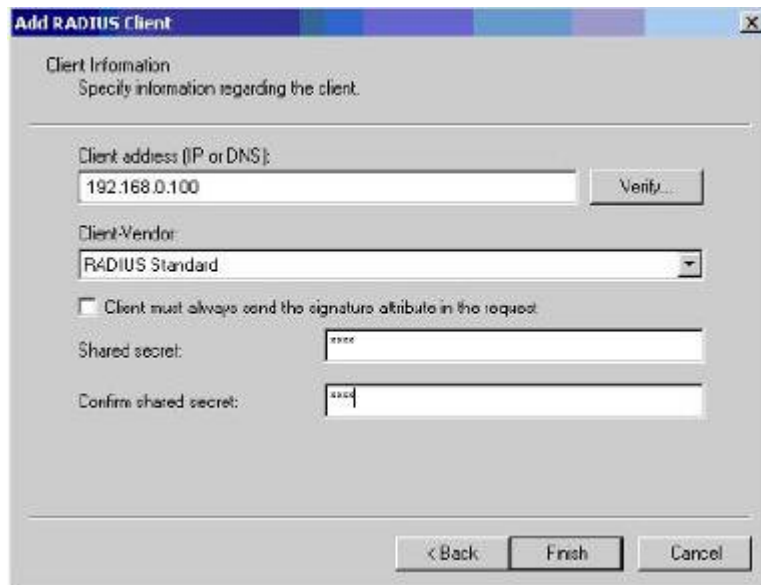
Figure 4-76 RADIUS Server configuration

4.10.2 802.1X Port Configuration

This table is to configure the per port network access control setting. By drawing and select the menu bar to define the port control type. The screen in Figure 4-77 and Figure 4-78 appears.
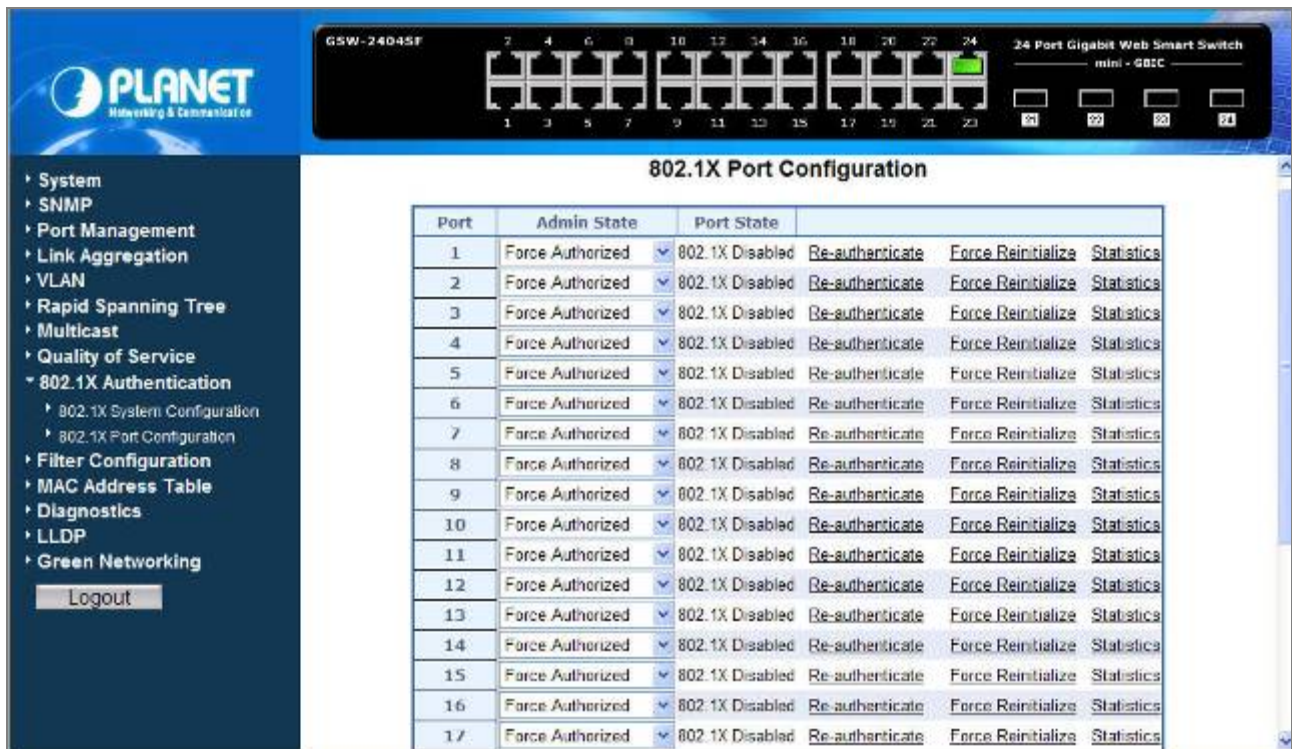
Figure 4-77 802.1X Port Configuration
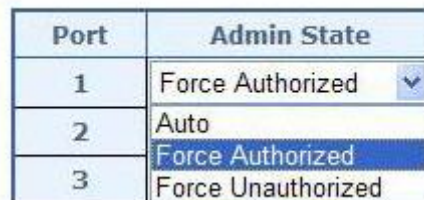
Figure 4-78 802.1X Network access control mode selection

The Network Access Control port configuration table includes the following fields: **Table 4-30** Description of the 802.1X Port Configuration.

Item	Description
Port	Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF). Selects the port to be configured. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port.
Admin State	This selector lists the options for control mode. The control mode is only set if the link status of the port is link up. The options are: • **Auto:** The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

	• **Force authorized:** The authenticator PAE unconditionally sets the controlled port to be authorized.
	• **Force unauthorized:** The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized
Port State	This field indicates the configured control mode for the port.
Re-authenticate	This button begins the re-authentication sequence on the selected port. This button is only selectable if the control mode is **'auto'**. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.
Force Reinitialize	This button begins the re-initialization sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.
Statistics	This button redirect to the **"802.1X Statistics"** page on the selected port.
Re-authenticate All	This button begins the re-authentication sequence on all ports.
Force Reinitialize All	This button begins the re-initialization sequence on all ports.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh 802.1X System Configuration screen of Web Smart Gigabit Switch.

Table 4-30 Description of the 802.1X Port Configuration

4.11 Filter Configuration

The GSW-1602SF / GSW2404SFsupport per-Port IP Filter function to management the IP traffic flow. With the IP Filter configuration, administrator can block the specify source IP Address range. The screen in Figure 4-79 appears.
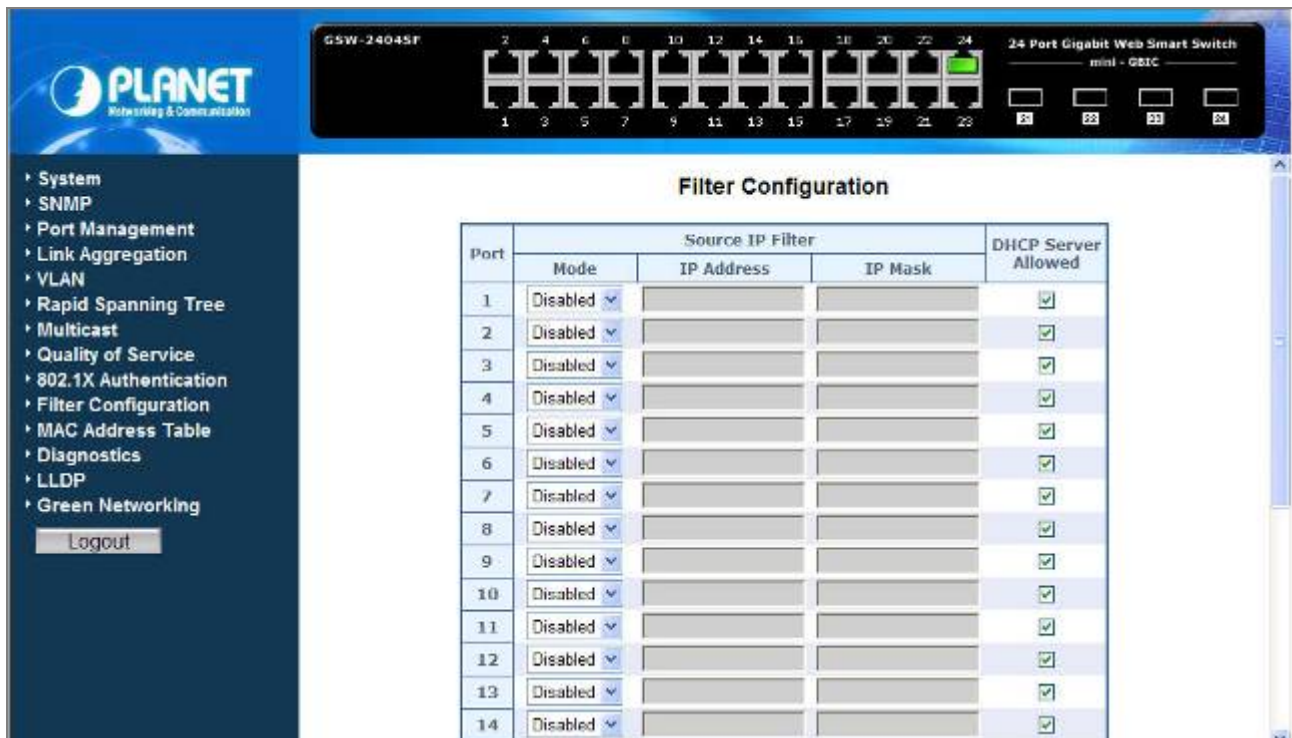
Figure 4-79 Filter Configuration

The Filter Configuration page includes the following fields: **Table 4-31** Description of the Filter Configuration.

Item	Description
Port	Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF) for the IP Filter setting.
Mode	To "**Enabled**" or "**Disabled**" the IP Filter on the selected port. If "**Enabled**" be selected, the next two fields are allowed to be configured. Press "**Apply**" to active the IP Filter setting on the port.
IP Address	This input field allows the user to enter the "**Source IP network address**" to be filtered on the selected port. This field has to co-work with the "**IP Mask**" filed.
IP Mask	This input field allows the user to enter the "**IP Mask**" of the Source IP address to be filtered on the selected port.
DHCP Server Allowed	To allow the ICMP DHCP request and reply packets be pass through the port even the IP address of the DHCP server inside the range of the Filter list.

Table 4-31 Description of the Filter Configuration

4.12 MAC Addresses Table

4.12.1 Aging Time Configuration

This function provides MAC Address Table refresh aging time setting, the screen in Figure 4-80 appears.
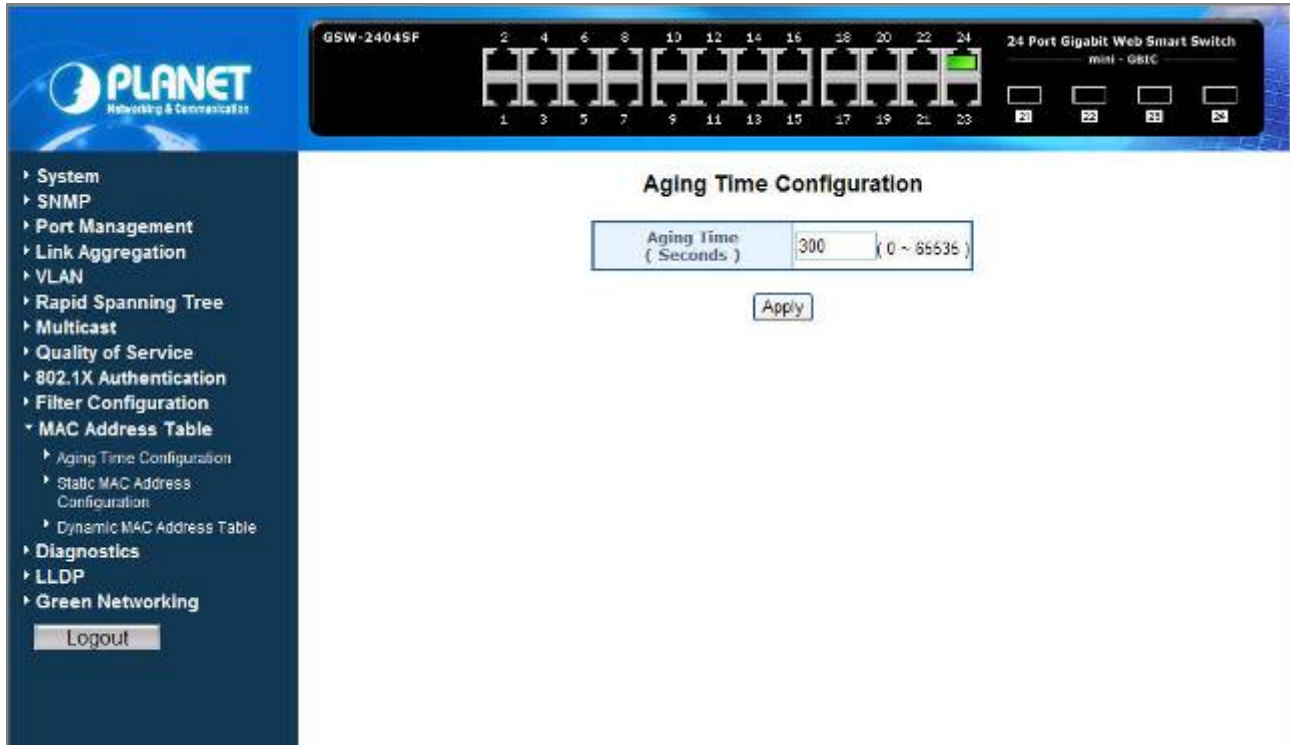
Figure 4-80 Aging Time Configuration

■   **Ageing Timeout Configuration (seconds)**

The MAC Address database contains static entries, which are never aged out, and dynamically learned entries, which are removed if they are not updated within a given time. You specify that time by entering a value for the Address Ageing Timeout. You may enter any number of seconds between **0 and 65535**.

IEEE 802.1D recommends a default of **300** seconds, which is the factory default.

The Aging Time Configuration includes the following fields: **Table 4-32** Description of the Aging Time Configuration.

Item	Description
Aging Time (Seconds)	Allow assign an aging time for MAC Address table refresh of Web Smart Gigabit Switch, the available range is 0-65535 seconds. Default mode is **300** seconds.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.

Table 4-32 Description of the Aging Time Configuration

4.12.2 Static MAC Address Configuration

The Static MAC Address page contains a list of static MAC addresses. Static Address can be added and removed from the page. In addition, several MAC Addresses can be defined for a single port. The screen in appears.
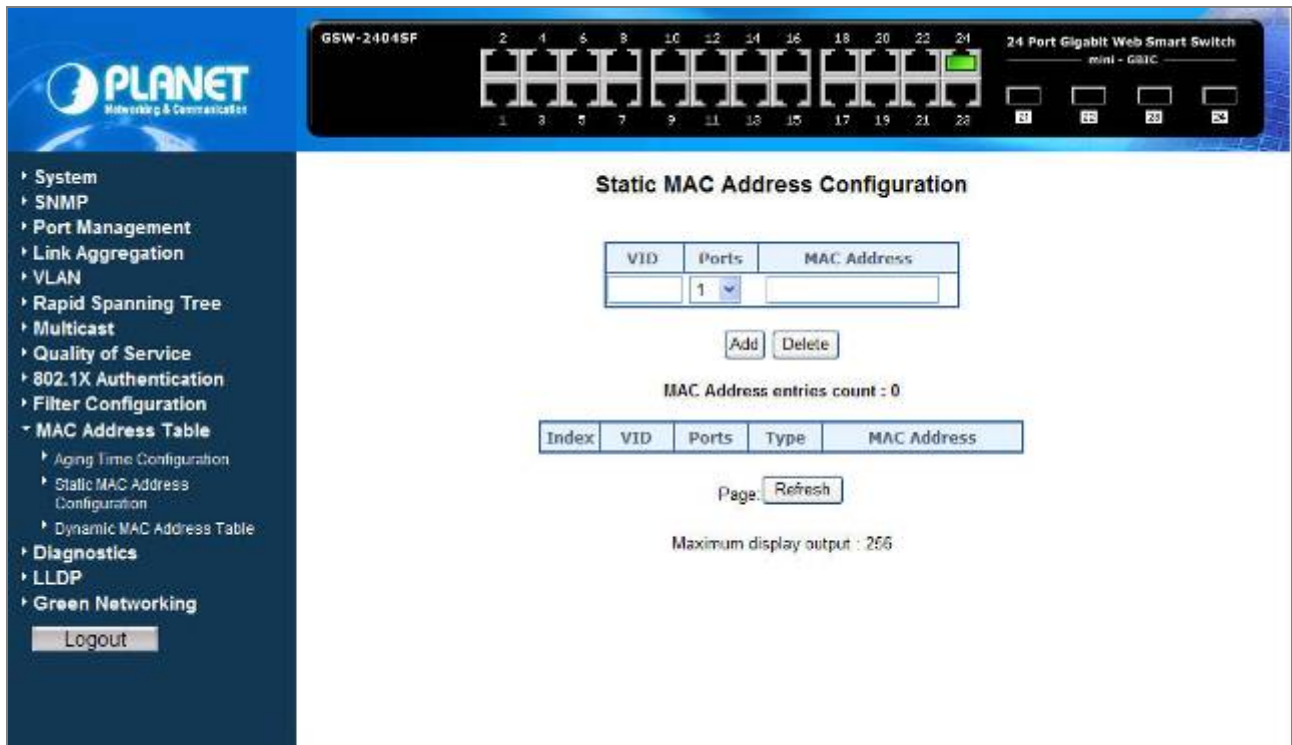
Figure-4-81 Static MAC Address Configuration

The configable filelds includes the following items: **Table 4-33** Description of the Static MAC Address Configuration.

Item	Description
VID	The VLAN ID attached to the MAC Address
Ports	Specifies the port numbers for which the table is queried. Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF).
MAC-Address	Input the MAC address entry be manualed bind to the specify port.
Button	
Add	Press this button for add specific MAC Address to one specific port.
Delete	Press this button for delete specific MAC Address from one specific port.

Table 4-33 Description of the Static MAC Address Configuration

The MAC Address entries count table includes the following fields: **Table 4-34** Description of the MAC Address entries count.

Item	Description
VID	The VLAN ID attached to the MAC Address
Ports	Specifies the port numbers for which the table is queried.
Type	**Static -** Static addresses are manually configured. Packets received with the destinated MAC

	address mathch the port static MAC setting will be forward to the specify port.
MAC-Address	The MAC address listed in the current static address list.
Button	
Refresh	Press this button for refresh MAC Address entries count table screen of Web Smart Gigabit Switch.

Table 4-**34** Description of the MAC Address entries count table

4.12.3 Dynamic MAC Address Table

This function display information about entries in the MAC Address database. These entries are used by the transparent bridging function to determine how to forward a received frame. The screen in appears.
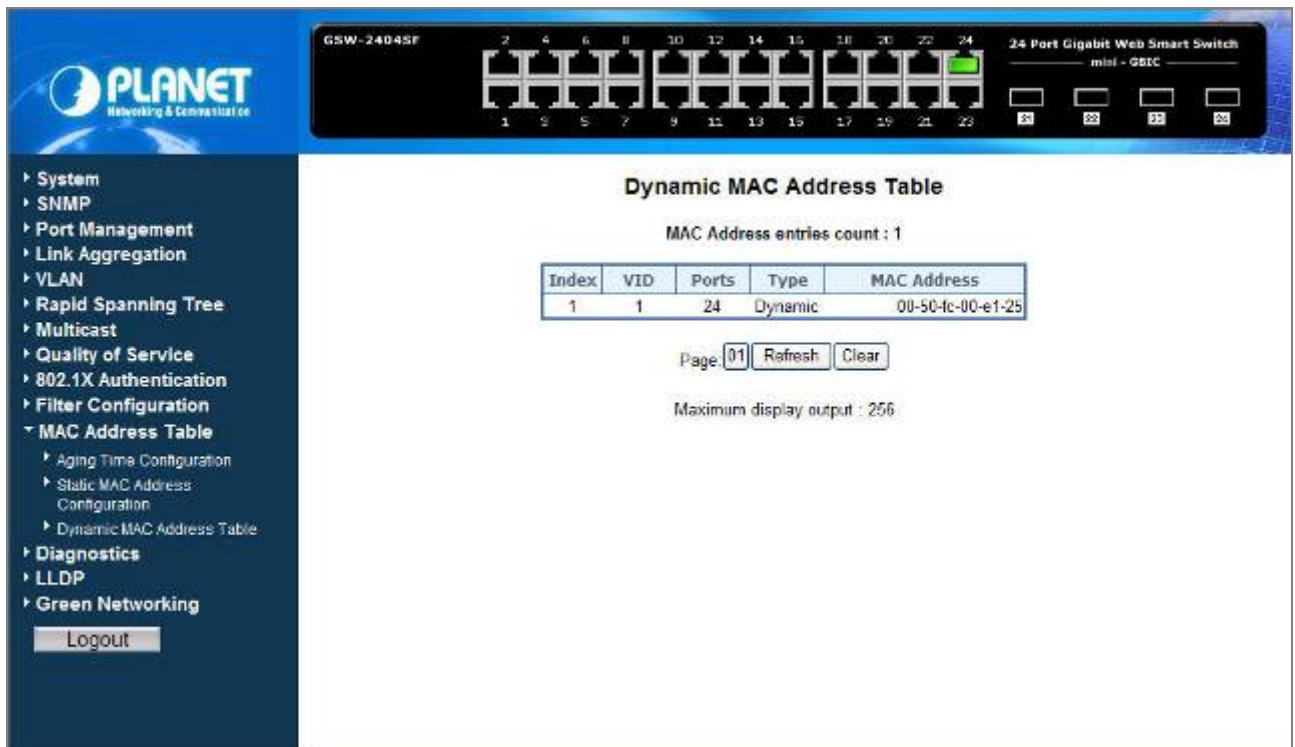
Figure 4-82 Dynamic MAC Address Table

■ **Dynamic MAC Address Table**

The Dynamic MAC Address Table includes the following fields: **Table 4-35** Description of the Dynamic Address Table.

Item	Description
MAC Address entries count	The count of the MAC Address
VID	The VLAN ID for which the table is queried.
Ports	Specifies the port numbers for which the table is queried.

Type	The MAC Address type for which the table is queried. There're two possible type-
	• **Dynamic** - Addresses are associated with ports by learning the ports from the frame source address
	• **Static -** Static addresses are manually configured. Packets received with the destinated MAC address mathch the port static MAC setting will be forward to the specify port.
MAC-Address	Specifies the MAC address for which the table is queried.

Table 4-35 Description of the Dynamic MAC Address Table

> **Note**: Although the MAC Address Table of GSW-Series Web-Smart switches are up to 8K .entries. To reduce the Web-Page memory loading, the maximum MAC lists are limited to **256** entries.

4.13 Diagnostics

4.13.1 Ping Parameters

Use this screen to tell the Web Smart Gigabit Switch to send a Ping request to a specified IP address. You can use this function to check whether the Web Smart Gigabit Switch can communicate with a particular IP station. Once you click the Apply button, the switch will send **n** pings and the results will be displayed below the configurable data. The screen in Figure 4-83 appears.
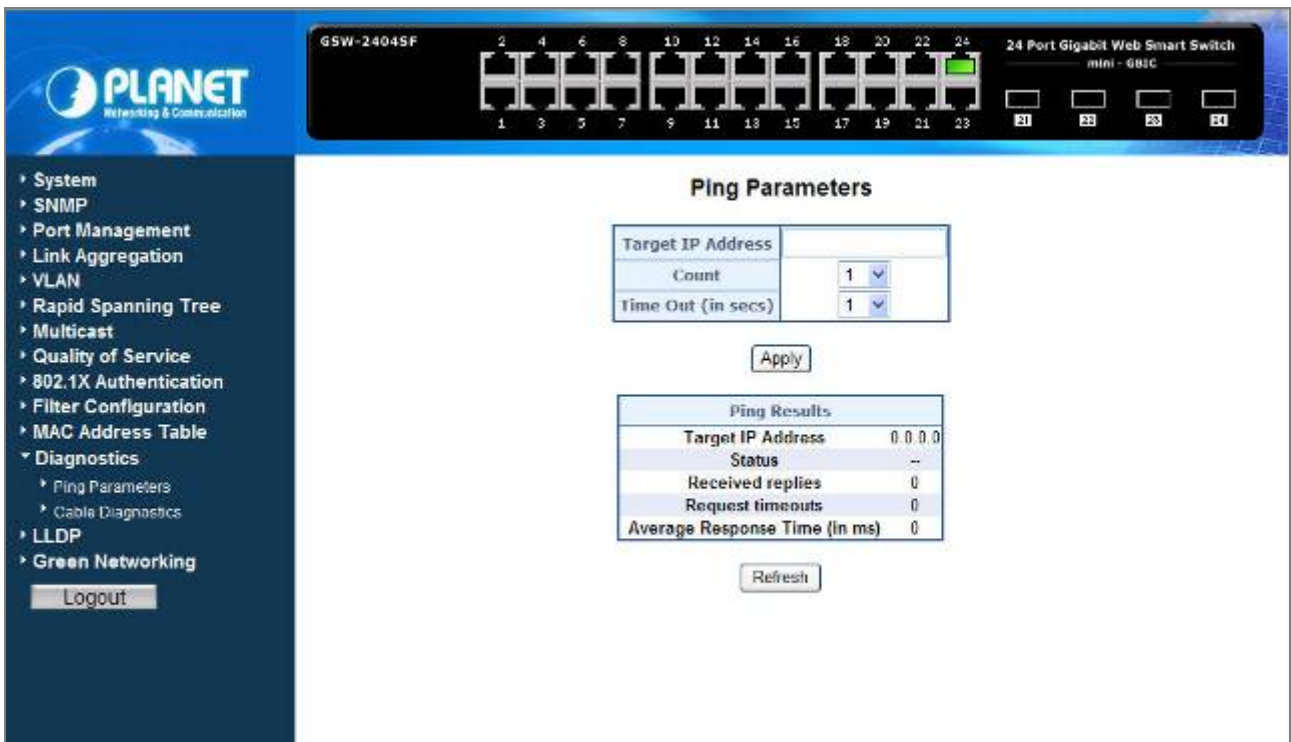
Figure 4-83 Ping Parameters screen

The Ping Parameters includes the following fields: **Table 4-36** Description of the Ping Parameters.

Item	Description
Target IP Address	Enter the IP address of the station you want the Web Smart Gigabit Switch to ping. The initial value is blank. The IP Address you enter is not retained across a power cycle.
Count	Number of echo requests to send
Time Out (in secs)	Timeout in milliseconds to wait for each reply.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.

Table 4-36 Description of the Ping Parameters

After field the parameter and press "**Apply**" to execute the Ping function. The Ping result shows at the next table. As the screen in Figure 4-84 appears.

Figure 4-84 Ping Result screen

Be sure the target IP Address is within the same network subnet of the Web Smart Gigabit Switch, or you had setup the correct gateway IP address.

4.13.2 Cable Diagnostics

The Cable Diagnostics page contains fields for performing tests on copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on the Cat5 twisted-pair cabling. There might be two statuses as follow:

■ If the link is established on the twisted-pair interface in 1000BASE-T mode, the Cable Diagnostics can run without disruption of the link or of any data transfer.

■ If the link is established in 100BASE-TX or 10BASE-T, the Cable Diagnostics cause the link to drop while the diagnostics are running.

After the diagnostics are finished, the link is reestablished. And the following functions are available.

• Coupling between cable pairs.

- Cable pair termination
- Cable Length

Anomalous coupling between cable pairs can be caused by shorted wires, improper termination, or high crosstalk resulting from an incorrect wire map. These conditions can all prevent the PLANET Switch from establishing a link. The screen in Figure 4-85 appears.
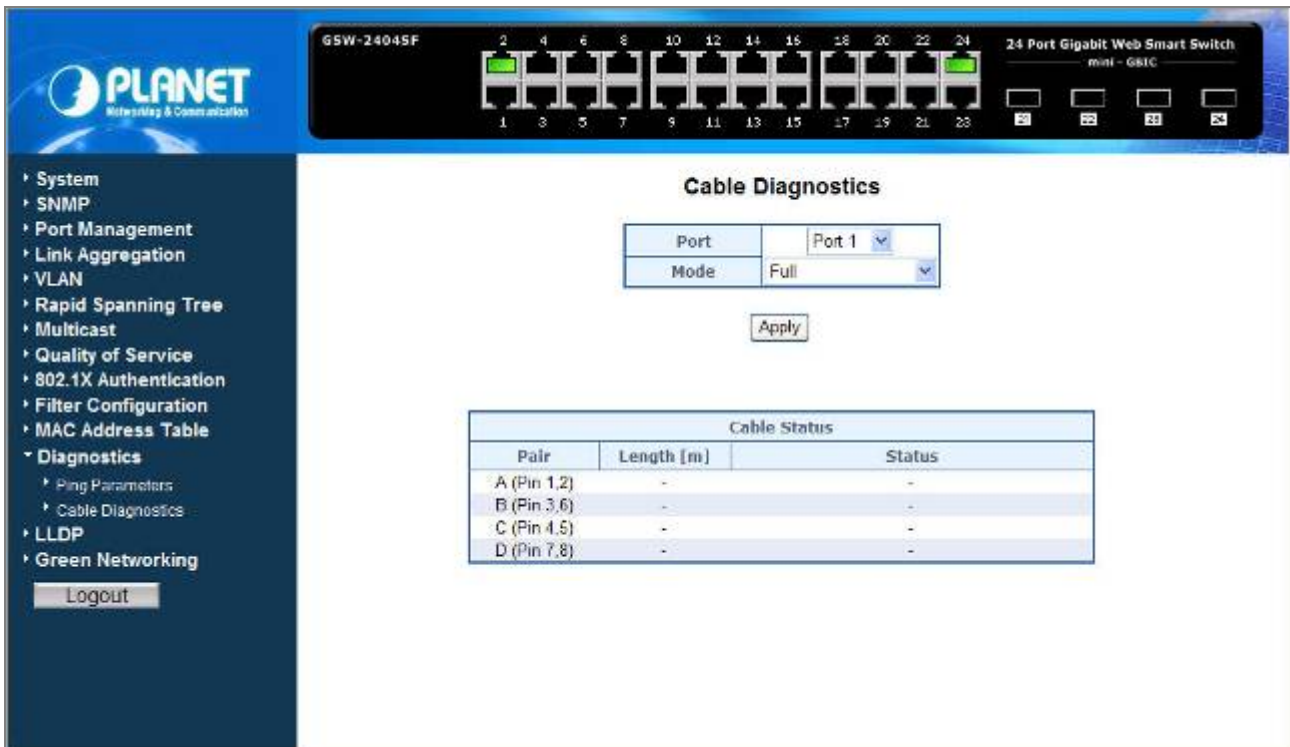
Figure 4-85 Cable Diagnostics

The Cable Diagnostics includes the following fields: **Table 4-37** Description of the Cable Diagnostics.

Item	Description
Port	Specifies the port numbers for which to run the cable diagnostics.
Mode	There're three cable test mode for selection: **Full** – test full pairs **Anomaly** – test with only anomaly pairs **Anomaly w/o X-pair** - test anomaly pairs but without X-pair
Button	
Apply	Press this button for start the cable diagnostics process.

Table 4-37 Description of the Cable Diagnostics

The Cable Status includes the following items: **Table 4-38** Description of the Cable Status.

Item	Description
• **Pair**	The twist pair of the UTP cable. The pair groups as follow: **A (Pin 1,2)** **B (Pin 3,6)** **C (Pin 4,5)** **D (Pin 7,8)**
• **Length[m]**	When properly terminated, Cable Diagnostics reports the approximate cable length in meters of each of the four cable pair A, B, C, and D.
• **Status**	The cable test results. Possible values are: • **Proper -** The cable passed the test. • **Open -** The cable is connected on only one side or there is no cable connected to the port • **Short -** A short has occurred in the cable. With 10/100BASE link, the status of Pair C and Pair D will be **"Short"**. • **Abnormal termination –** An improper termination be detected. Proper termination of Cat5 cable requires 100Ω differential impedance between the positive and negative cable terminals. IEEE STD 802.3 allows for a termination of as large as 115Ω or as small as 85Ω. If the termination falls out of this range, it is reported as falls an anomalous termination.

Table 4-38 Description of the Cable Status

	Be sure to running the Cable diagnostics with standard Cat 5e or Cat 6 UTP cable. With some of the UTP cables that not match the standard of Cat 5e, it might cause the 10/100Base-TX link down after the cable diagnostics.
Note	

4.14 LLDP

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.

4.14.1 LLDP Configuration

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Configuration screen in Figure 4-86 appears.
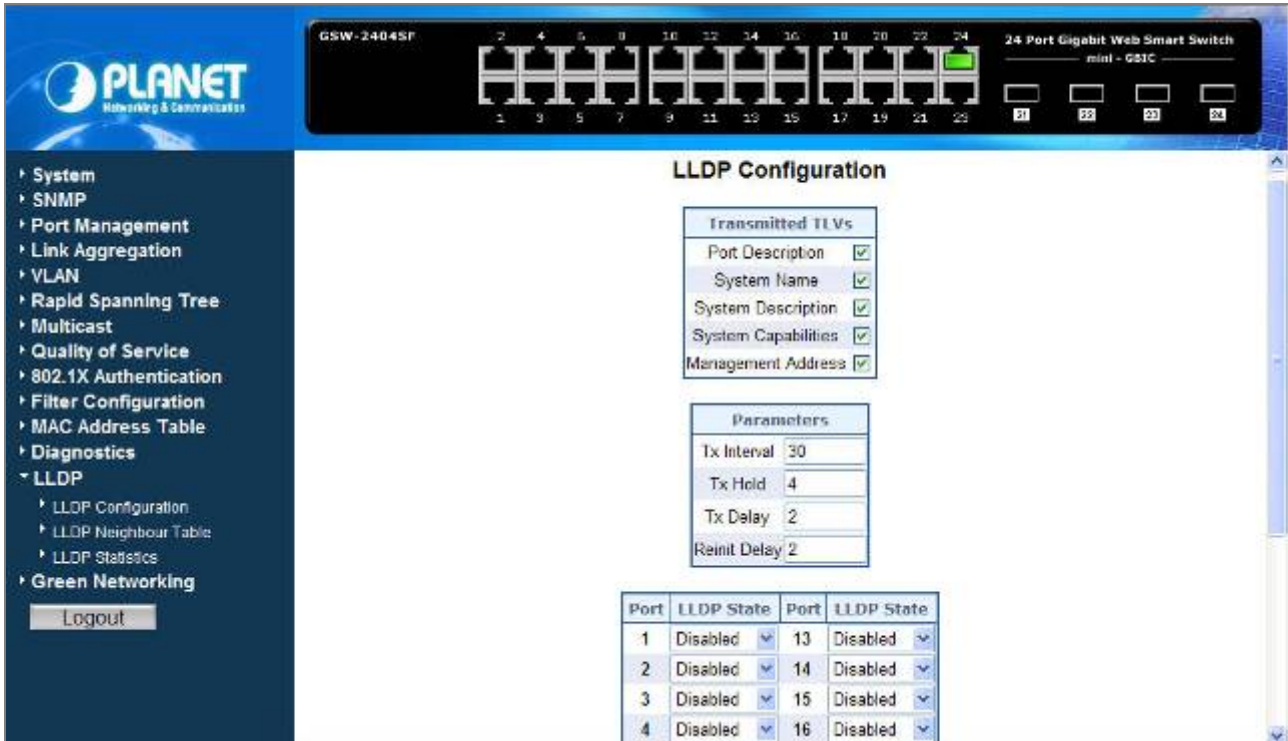
Figure 4-86 LLDP Configuration

■ **Transmitted TLVs Parameters**

■ The Transmitted TLVs Parameters includes the following items: **Table 4-39** Description of the Transmitted TLVs Parameters.

Object	Description
Port Description	Optional TLV: When checked the **"Port Description"** is included in LLDP information transmitted.
System Name	Optional TLV: When checked the **"System Name"** is included in LLDP information transmitted.
System Description	Optional TLV: When checked the **"System Description"** is included in LLDP information transmitted.
System Capabilities	Optional TLV: When checked the **"System Capability"** is included in LLDP information transmitted. The system capabilities identify the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.
Management Address	Optional TLV: When checked the **"Management Address"** is included in LLDP information transmitted. The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address.

Table 4-39 Description of the Transmitted TLVs Parameters

■   **Parameters**

■   The Parameters includes the following items: **Table 4-40** Description of the Parameters.

Object	Description
Tx Interval	The Web Smart Gigabit 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 **Tx 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)
Tx Hold	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to

	Tx Hold multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
Tx Delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval
Reinit 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.

Table 4-40 Parameters

■ **LLDP Port State**

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header. The LLDP State includes the following items: **Table 4-41** Description of the LLDP State.

Object	Description
• **Port**	The Web Smart Gigabit Switch port number of the logical LLDP port.
• **Mode**	Select LLDP mode. • **Disabled** The Web Smart Gigabit Switch will not send out LLDP information, and will drop LLDP information received from neighbors. • **Rx and Tx** The Web Smart Gigabit Switch will send out LLDP information, and will analyze LLDP information received from neighbors. • **Tx only** The Web Smart Gigabit Switch will drop LLDP information received from neighbors, but will send out LLDP information. • **Rx only** The Web Smart Gigabit Switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh LLDP State Configuration screen of Web Smart Gigabit Switch.

Table 4-41 LLDP State

4.14.2 LLDP Neighbour Table

This function provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP Neighbour Table screen in Figure 4-87 appears.
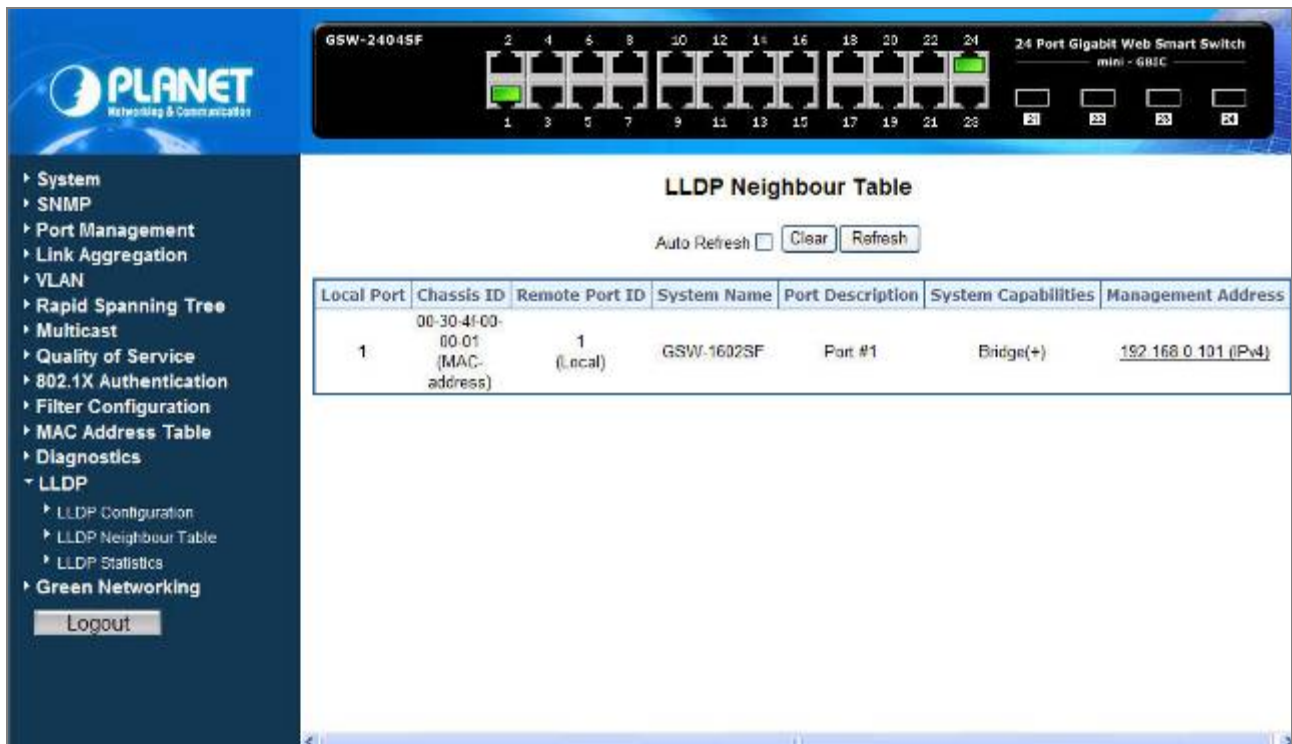
Figure 4-87 LLDP Neighbour Table

The columns hold the following information:

Object	Description
• **Local Port**	The port on which the LLDP frame was received.
• **Chassis ID**	The **Chassis ID** is the identification of the neighbor's LLDP frames.
• **Remote 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.
• **Port Description**	**Port Description** is the port description advertised by the neighbor unit.

• **System Capabilities**	**System Capabilities** describes the neighbor unit's capabilities. The possible capabilities are:
	
	    1. Other
	    2. Repeater
	    3. Bridge
	    4. WLAN Access Point
	    5. Router
	    6. Telephone
	    7. DOCSIS cable device
	    8. Station only
	    9. Reserved
	
	When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

• **Management Address**	**Management Address** is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.

Table 4-42 LLDP Neighbor Table

4.14.3 LLDP Statistics

This function provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected Switch. The LLDP Statistics screen in Figure 4-88 appears.
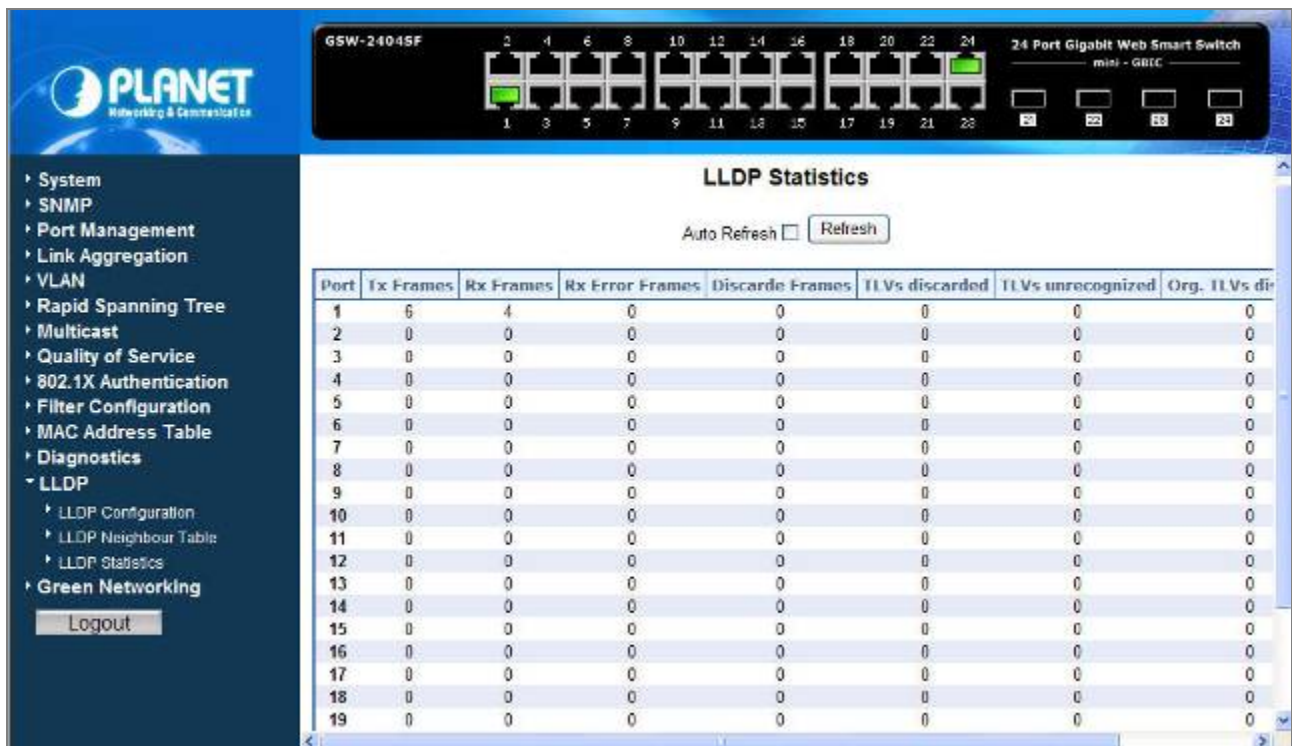
Figure 4-88 LLDP Statistics

LLDP Statistics

The displayed table contains a row for each port. The columns hold the following information:

Object	Description
Auto Refresh	Disable or Enable the **Auto Refresh** function. While set to enable, the Port Statistics Detail table will refresh automatically every **30** seconds.
Refresh Button	Press this button for refresh LLDP Statistics screen.
Port	The port on which LLDP frames are received or transmitted. Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF).
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors Frames	The number of received LLDP frames containing some kind of error.

Discarded Frames	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.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. TLVs Discarded	The number of organizationally TLVs received.
AgeOuts	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.

Table 4-43 LLDP Statistics

4.15 Green Networking

In line with the energy-saving trend worldwide, PLANET delivers the new generation green Switch- GSW-1602SF / GSW-2404SF Series Web Smart Gigabit Ethernet Switch. With both benefit of energy saving and gigabit performance, the new engine that provides power saving for less energy consumption but not reduce the Gigabit performance.

The GSW-1602SF / GSW-2404SF incorporate two advanced Green Networking technologies:

- **Hibernation Link Down power saving**

- **Intelligent scales power based on cable length**

The Hibernation Link Down power savings goes beyond IEEE specifications to automatically lower power for a given port when it is not linked. With the Hibernation Link Down power savings technology, the GSW-1602SF / GSW-2404SF will automatically adjusts power usage of the ports that are shutdown or not connected to network device. The other technology adopted, intelligent scales power, is an intelligent algorithm that actively determines the appropriate power level based on cable length. The Green Networking screen in Figure 4-89 appears.
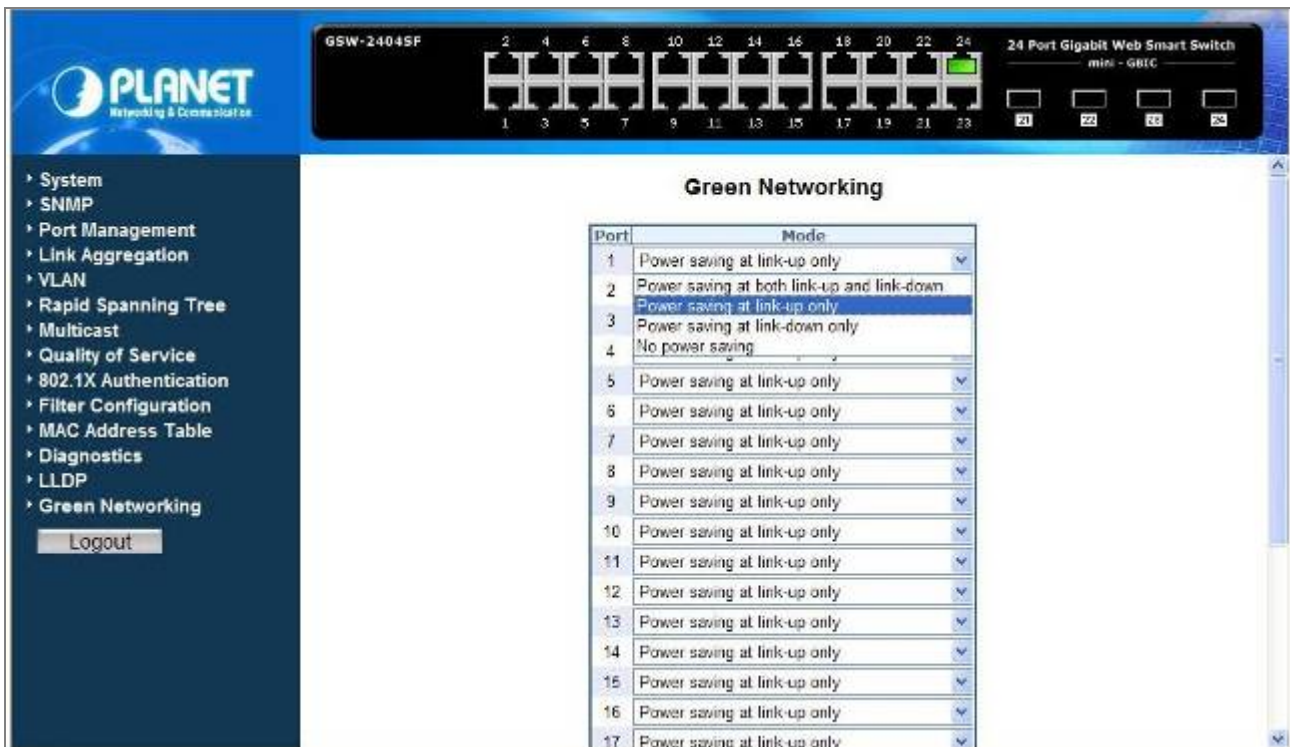
Figure 4-89 Green Networking

The Green Networking configuration table includes the following fields: **Table 4-44** Description of the Green Networking.

Item	Description
Port	Indicate port 1 to port 24 (GSW-24024SF), port 1 to port 16 (GSW-1602SF). Selects the port to be configured. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port.
Mode	This selector lists the options for power saving mode. The power saving mode options are shown as below:: • **Power saving at both link-up and link-down:** enable power saving when the TP port is connected or not connected. • **Power saving at link-up only (Default mode):** enable power saving when the TP port is connected. • **Power saving at link-down only:** enable power saving when the TP port is not connected. • **No power saving:** disable power saving function.
Button	
Apply	Press this button for save current configuration of Web Smart Gigabit Switch.
Refresh	Press this button for refresh Green Networking screen of Web Smart Gigabit Switch.

Table 4-44 Description of the Green Networking Configuration

4.16 Logout

Press this function; the web interface will go back to login screen. The screen in Figure 4-90 & 4-91 appears.

Figure 4-90 Logout screen

Figure 4-91 Login screen

5. SWITCH OPERATION

5.1 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 information comes from the learning process of Ethernet Switch.

5.2 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.

5.3 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. There by increasing the network throughput and availability.

5.4 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 provided 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. However, the switch is most commonly used to segment existing hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to significantly 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, reducing 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.

5.5 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. 1000Base-T can be only connected in Full-duplex mode.

5.6 IGMP Snooping

Theory

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.

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)

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:

IGMP State Transitions

6. TROUBLESHOOTING

This chapter contains information to help you solve problems. If the Switch is not functioning properly, make sure the Ethernet Switch was 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 Switch.

Some stations cannot talk to other stations located on the other port

Solution:

Please check the VLAN, port trunking function that may introduce this kind of problem.

Performance is bad

Solution:

Check the full duplex status of the Ethernet Switch. If the Ethernet Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor.

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.

Why the Switch doesn't connect to the network

Solution:

Check the LNK/ACT LED on the Switch .Try another port on the Switch. Make sure the cable is installed properly Make sure the cable is the right type Turn off the power. After a while, turn on power again.

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

Contact	MDI	MDI-X
1	1	3
2	2	6
3	3	1
6	6	2

A.3 RJ-45 cable pin assignment
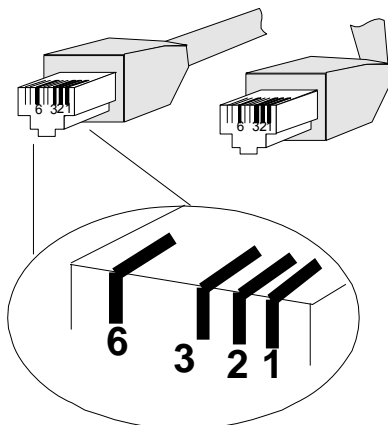
There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

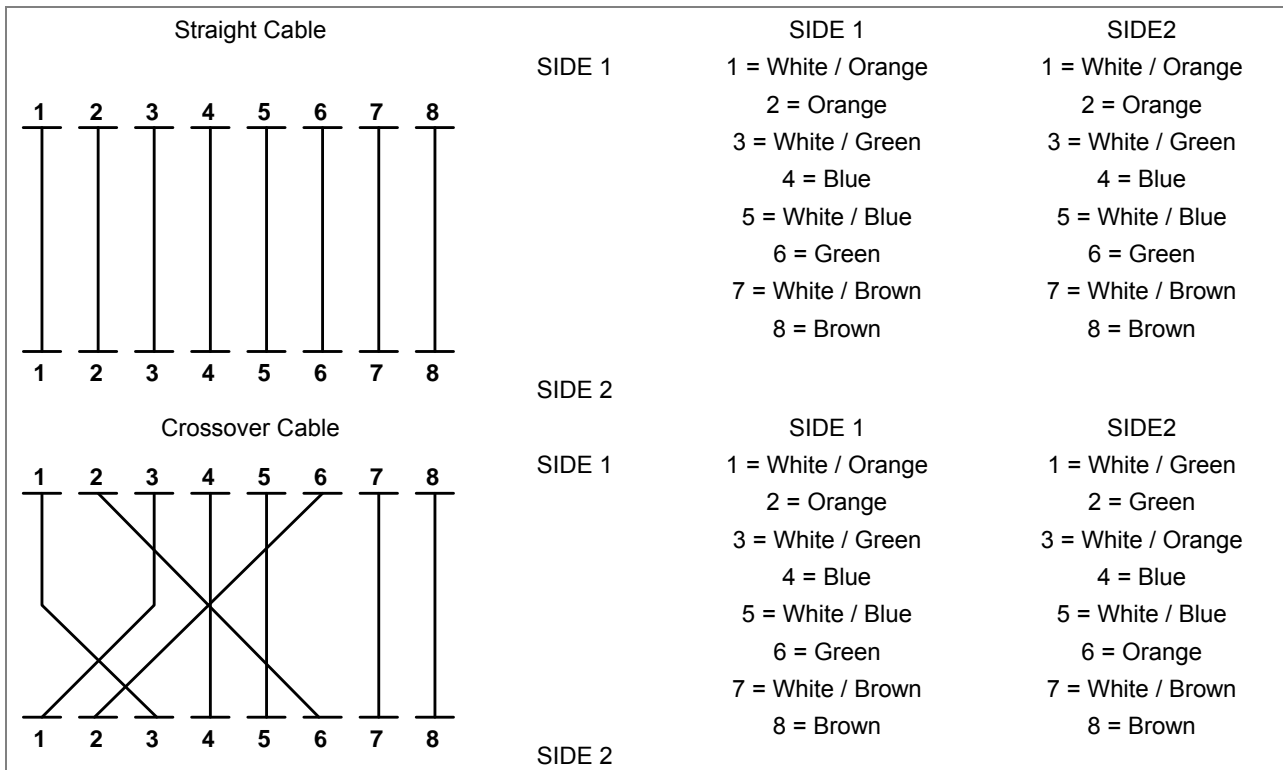|	SIDE 1	SIDE2
Straight Cable	1 = White / Orange	1 = White / Orange
SIDE 1	2 = Orange	2 = Orange
1 2 3 4 5 6 7 8	3 = White / Green	3 = White / Green
	4 = Blue	4 = Blue
	5 = White / Blue	5 = White / Blue
	6 = Green	6 = Green
	7 = White / Brown	7 = White / Brown
1 2 3 4 5 6 7 8	8 = Brown	8 = Brown
SIDE 2		
Crossover Cable	SIDE 1	SIDE2
SIDE 1	1 = White / Orange	1 = White / Green
1 2 3 4 5 6 7 8	2 = Orange	2 = Green
	3 = White / Green	3 = White / Orange
	4 = Blue	4 = Blue
	5 = White / Blue	5 = White / Blue
	6 = Green	6 = Orange
1 2 3 4 5 6 7 8	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 same pin assignment and color as above picture before deploying the cables into your network.

A.4 Available Modules

The following list the available Modules for GSW-1602SF / GSW-2404SF.

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
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) mini-GBIC module-10KM
MGB-LB10	SFP-port 1000Base-LX (WDM,TX:1550nm) mini-GBIC module-10KM
MGB-LA20	SFP-port 1000Base-LX(WDM,TX:1310nm) mini-GBIC module-20KM
MGB-LB20	SFP-port 1000Base-LX (WDM,TX:1550nm) mini-GBIC module-20KM
MGB-LA40	SFP-port 1000Base-LX(WDM,TX:1310nm) mini-GBIC module-40KM
MGB-LB40	SFP-port 1000Base-LX (WDM,TX:1550nm) mini-GBIC module-40KM

2080-A82070-004

CE

PLANET
Networking & Communication

EC Declaration of Conformity

For the following equipment:

*Type of Product: 16/24-Port 10/100/1000Base-T Web Smart Gigabit Ethernet Switch
*Model Number: GSW-1602SF / GSW-2404SF

* Produced by:
Manufacturer's Name   :   **Planet Technology Corp.**
Manufacturer's Address: 11F, No 96, Min Chuan Road,
                             Hsin Tien, Taipei, 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:

LVD	EN 60950-1	(2001)
Conducted / Radiated	EN 55022	(1998 + A1: 2000 + A2: 2003)
Harmonic	EN 61000-3-2	(2000 + A1: 2005)
Flicker	EN 61000-3-3	(1995 + A1: 2001 + A2: 2005)
Immunity	EN 55024	(1998 + A1: 2001 + A2: 2003)
ESD	EN 61000-4-2	(1995 + A1: 1998 + A2: 2001)
RF-Field	EN 61000-4-3	(2002 + A1, 2002)
Burst	EN 61000-4-4	(2004)
Surge	EN 61000-4-5	(1995 + A1 : 2001)
RF-commonmode	EN 61000-4-6	(1996 + A1: 2001)
Voltage Dips	EN 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: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname   **Kent Kang**

Position / Title :   **Product Manager**

  Taiwan   **6th, Aug., 2009**
  Place   *Date*   *Legal Signature*

PLANET TECHNOLOGY CORPORATION