10/100/1000Mbps

16/24-port Web Smart Gigabit

Ethernet Switch

GSW-1602SF/GSW-2404SF

User's Manual

16-Port Gigabit Web Smart Switch
24-Port Gigabit Web Smart Switch

-

Trademarks

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

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

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

FCC Warning

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

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 Web Smart Gigabit Ethernet Switch User's Manual

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

REVISION: 1.0 (SEPTEMBER.2006)

Part No.: 2080-A82070-000

TABLE OF CONTENTS

1. INTRODUCTION

Package Contents

Check the contents of your package for following parts:

- Web Smart Gigabit Ethernet Switch x1
- CD-ROM user's manual x1
- Quick installation guide x1
- 19" rack mounting kit x1
- Power cord x1
- Rubber feet x 4

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.

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 GSW-1602SF/2404SF and how to physically install the GSW-1602SF/2404SF.
- Section 3, **Configuration**

  It contains information about the Smart function of GSW-1602SF/2404SF.
- Section 4, **Switch operation**

  It contains specifications of GSW-1602SF/2404SF.
- **Appendices**

  It contains cable information of GSW-1602SF/2404SF.

Product Features

- **Generic Features**
  - Complies with IEEE 802.3, 10Base-T, IEEE 802.3u, 100Base-TX, IEEE 802.3ab,1000Base-T, IEEE 802.3z,1000Base-SX/LX, Ethernet standard
  - 16/24-Port 10/100/1000Mbps Gigabit Ethernet ports
  - 2/4-Port SFP (Small Form-factor Pluggable) for 3.3V mini GBIC module, shared with Port-15 and Port-16, or Port-21 to Port-24
  - Each Switching ports support auto-negotiation-10/20, 100/200Mbps and 1000/2000 supported
  - Auto-MDI/MDI-X detection on each RJ-45 port, support CSMA/CD protocol
  - Prevents packet loss with back pressure (half-duplex) and 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 (10/100/1000 Mbps)

Layer-2 Switching

- Support port-based and 802.1q VLAN function, up to 64 VLAN groups
- 802.1w Rapid-Spanning Tree protocol support
- Link Aggregation support static mode and LACP (802.3ad) - up to 8 Trunk groups, each trunk for up to maximum 12 ports
- IGMP Snooping – multicast filtering

Quality of Service

- 4 QoS classes per port
- Traffic class assignment based on 802.1p tag, or DSCP field
- Multicast and Broadcast Storm Control as well as Flooding Control
- Rate Limit bandwidth control at both inband and outband in steps of 128kbps

Security

- Port Mirroring support for dedicated port monitoring
- 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

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

PRODUCT SPECIFICATION

Model	GSW-1602SF	GSW-2404SF
Hardware Specification		
Network ports	16	24
Switch architecture	Store-and-Forward	
Switch Fabric	32Gbps	48Gbps
Switch throughput	23.8Mpps	35.7Mpps
Address Table	8K entries	8K entries
Share data Buffer	340KB	500KB
Flow Control	Back pressure for half duplex, IEEE 802.3x Pause Frame for full duplex	
Dimensions (mm)	440 x 210 x 44 (1U height)	
Weight	2kg	2kg
Power Requirement	100-240V AC, 50-60 Hz	
Power Consumption	30 watts, 102.5 BTU	30 watts, 102.5 BTU
Standards Conformance		
Network Standards	IEEE 802.3 (Ethernet), IEEE 802.3u (Fast Ethernet) IEEE 802.3ab (Gigabit Ethernet) IEEE 802.3z (Gigabit Ethernet, 1000Base-SX/LX) IEEE 802.1q (Tagged VLAN) IEEE 802.1w (Rapid Spanning Tree) IEEE 802.1X (Port-Based Authentication) IEEE 802.3ad (Link Aggregation Control Protocol) IEEE 802.3x (full-duplex flow control)	
Operating Temperature	0~50ºC	
Storage Temperature	-40~70ºC	
Operating Humidity	5% to 90% , relative humidity, non-condensing	
Storage Humidity	5% to 90% , relative humidity, non-condensing	
Regulation Compliance	FCC Part 15 Class A, CE	

2. INSTALLATION

This section describes the functionalities of GSW-1602SF/2404SF's 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 Product Description

The PLANET GSW-1602SF/GSW-2404SF is a 16/24-port 10/100/1000 Mbps Web Smart Ethernet Switch with non-blocking wire-speed performance. With 32/48Gbps internal switching fabric, the GSW-1602SF/GSW-2404SF can 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 /500 KB 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.

2.1.1 Product Overview

PLANET GSW-1602SF/2404SF is a Web Smart Gigabit Ethernet Switch with 16/24 RJ-45 10/100/1000Mbps ports for high-speed network connectivity. The GSW-1602SF/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 port can handle large amounts of data transmission in a secure topology linking to a backbone or high-power servers.

This products 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/2404SF could recognize up to 8K different MAC address and enables filtering and forwarding at full wire speed.

2.1.2 GSW-1602SF/2404SF Front Panel

Figure 2-1 & 2-2 shows a front panel of GSW-1602SF/2404SF.

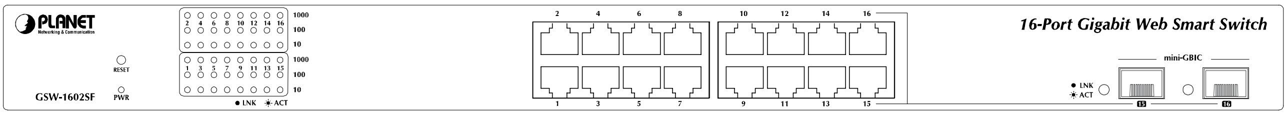


Figure 2-1 PLANET GSW-1602SF Front Panel

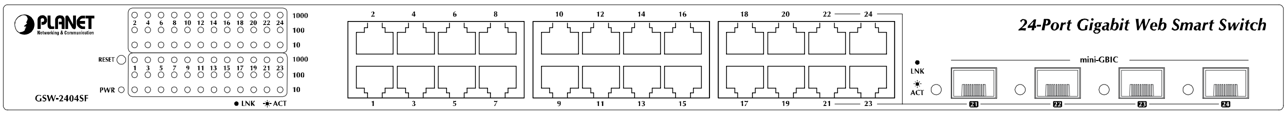


Figure 2-2 PLANET GSW-2404SF Front Panel

2.1.3 LED Indicators

LED	Color	Function
PWR	Green	**Lights** to indicate that the Switch is powered on.
1000 LNK/ACT	Green	**Lights** to indicate that the Switch is successfully connecting to the network at 1000Mbps. **Blinks** to indicate the Switch is receiving or sending data.
100 LNK/ACT	Green	**Lights** to indicate that the Switch is successfully connecting to the network at 100Mbps. **Blinks** to indicate the Switch is receiving or sending data.
10 LNK/ACT	Green	**Lights** to indicate that the Switch is successfully connecting to the network at 10Mbps. **Blinks** to indicate the Switch is receiving or sending data.
SFP LNK/ACT	Green	**Lights** to indicate that the Switch is successfully connecting to the network at 1000Mbps through SFP interface. **Blinks** to indicate the Switch is receiving or sending data.

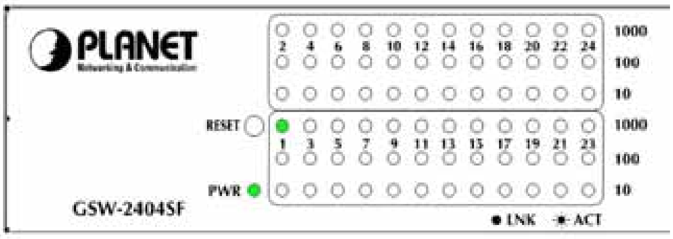


Figure 2-3 PLANET GSW-2404SF LED panel

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

2.1.4 GSW-1602SF/2404SF Rear Panel

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

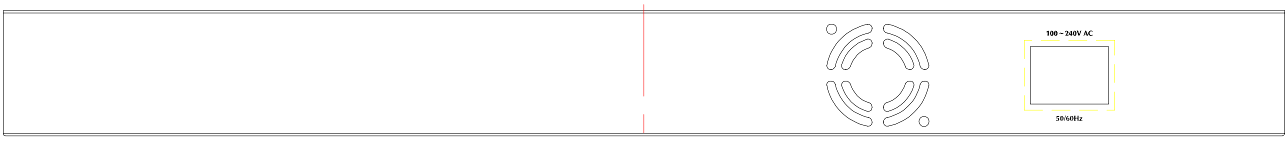


Figure 2-4 Rear Panel of GSW-1602SF/2404SF

Power Notice:

1. 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.

2. In some area, installing a surge suppression device may also help to protect your switch from being damaged by unregulated surge or current to the Switch or the power adapter.

2.2 Install the GSW-1602SF/2404SF

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

2.2.1 Desktop Installation

To install a GSW-1602SF/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 switch.

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

Step3: Keep enough ventilation space between the 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/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/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 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 Switch.

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

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

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

2.2.2 Rack Mounting

To install the switch in a **19-inch** standard rack, follow the instructions described below.

Step1: Place your GSW-1602SF/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 switch with supplied screws attached to the package. Figure 2-4 shows how to attach brackets to one side of the switch.

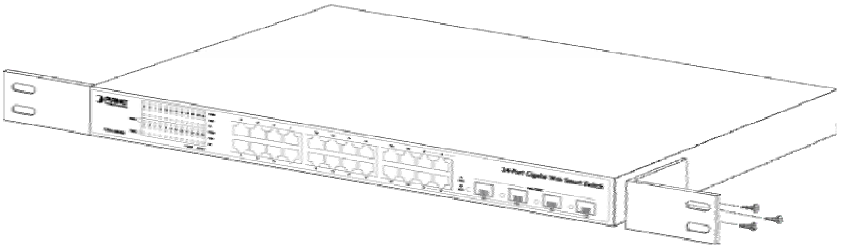


Figure 2-5 Attaching the brackets to the GSW-2404SF

Caution: 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 Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-5

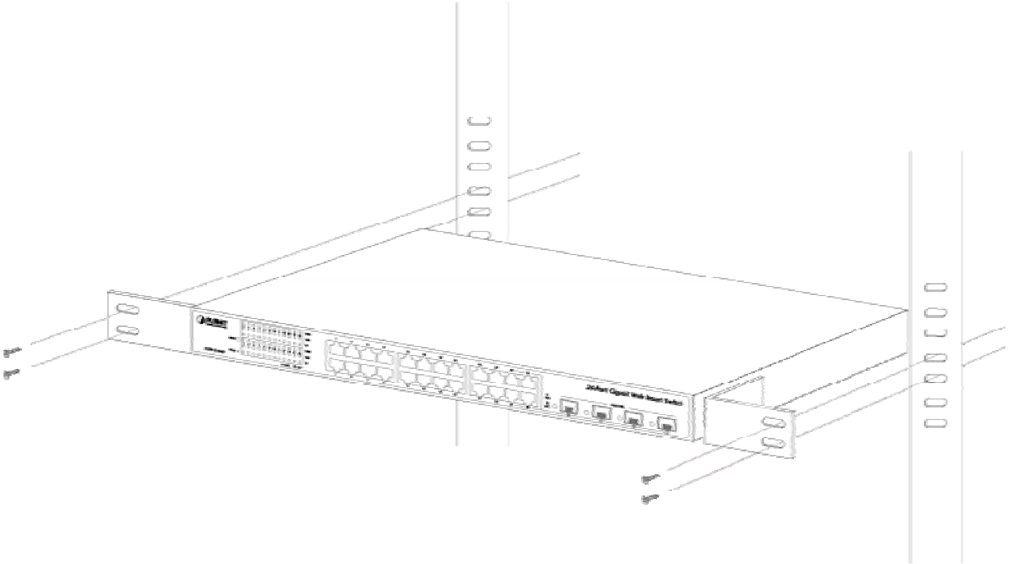


Figure 2-6 Mounting the Switch in a Rack

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 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 e and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Switch. As the Figure 2-7 appears.

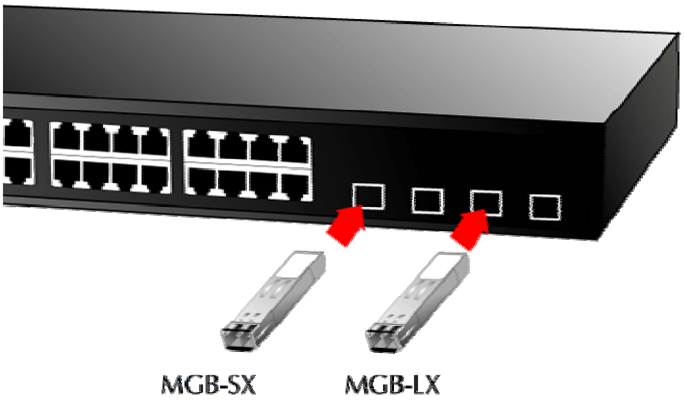


Figure 2-7 Plug-in the SFP transceiver

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)

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

Before connect the other switches, workstation or Media Converter.

1. Make sure both side of the SFP transfer 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 transfer model.
   - To connect to **1000Base-SX** SFP transfer, use the **multi-mode** fiber cable- with one side must be male duplex LC connector type.
   - To connect to **1000Base-LX** SFP transfer, 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 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/2404SF. Topics include:

- Overview
- Management methods
- Assigning an IP address to the GSW-1602SF/2404SF
- Logging on to the GSW-1602SF/2404SF

3.1 Overview

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

- System
- Port Configuration
- Port Mirroring
- Storm Control
- VLANs
- Rapid Spanning Tree
- Link Aggregation
- IGMP Snooping
- Quality of Service
- 802.1X Management
- MAC Address
- Tools
- Status

Please refer to the following Chapter 4 for more details.

3.2 Management Methods

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

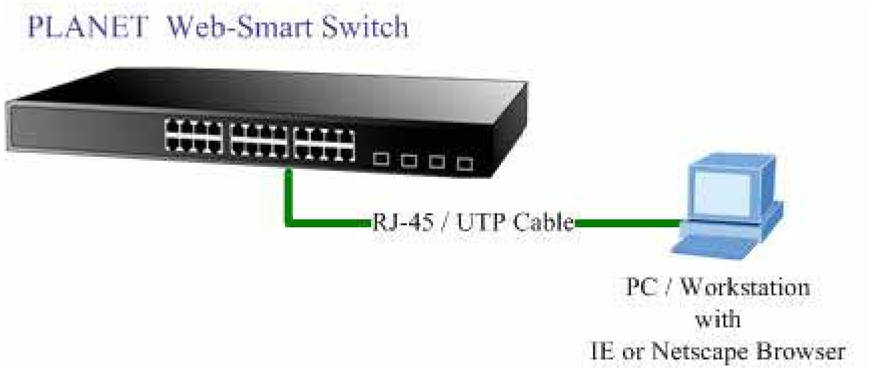
- Web Management via a network or dial-up connection.

3.2.1 Web Management

The PLANET Web-Smart Switch provides a built-in browser interface. You can manage the GSW-1602SF/2404SF remotely by having a remote host with web browser, such as Microsoft Internet Explorer, Netscape Navigator or Mozilla Firefox.

Using this management method:

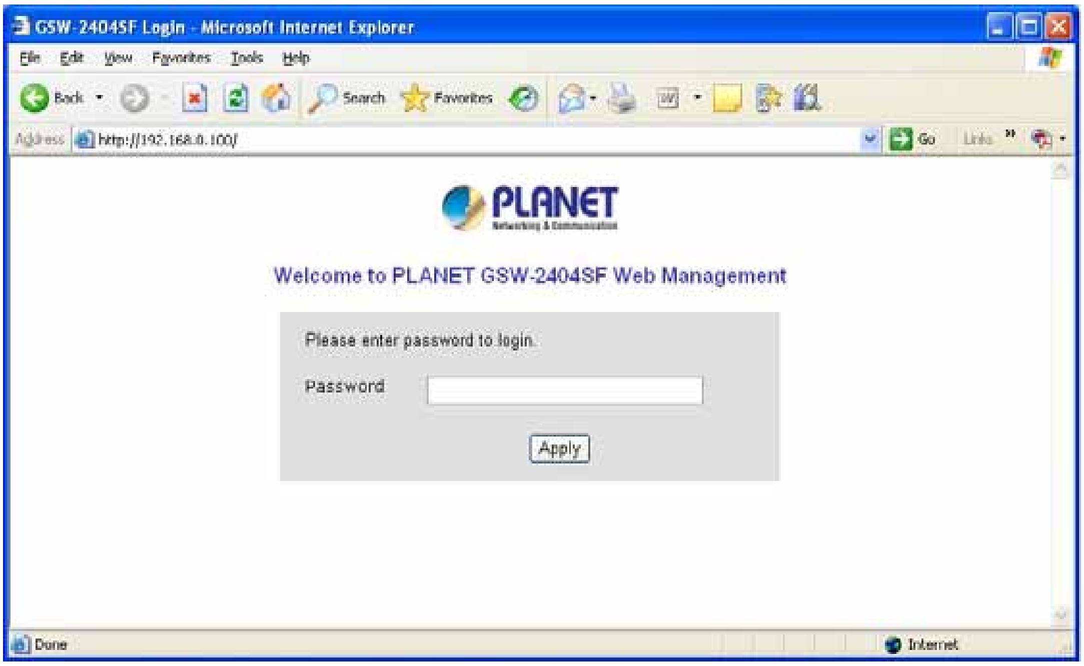
The GSW-1602SF/2404SF must have an Internet Protocol (IP) address accessible for the remote host.



3.2.2 Login the Switch

Before you start configure the GSW-1602SF/2404SF, please note the GSW-1602SF/2404SF is configured through an Ethernet connection, make sure the manager PC must be set on same the **IP subnet address**. For example, the default IP address of the GSW-1602SF/2404SF is ***192.168.0.100***, then the manager PC should be set at 192.168.0.x (where x is a number between 2 and 254), and the default subnet mask is 255.255.255.0. Use Internet Explorer 5.0 or above Web browser. Enter IP address ***http://192.168.0.100*** (the factory-default IP address) to access the Web interface.

When the following login screen appears, please enter the default password ***"admin"*** and press Login to enter the main screen of GSW-1602SF/2404SF. The login screen in Figure 3-1 appears.


GSW-2404SF Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.0.100/
Go Links
PLANET
Networking & Communication

Welcome to PLANET GSW-2404SF Web Management

Please enter password to login.

Password

Figure 3-1 Login screen

Note:

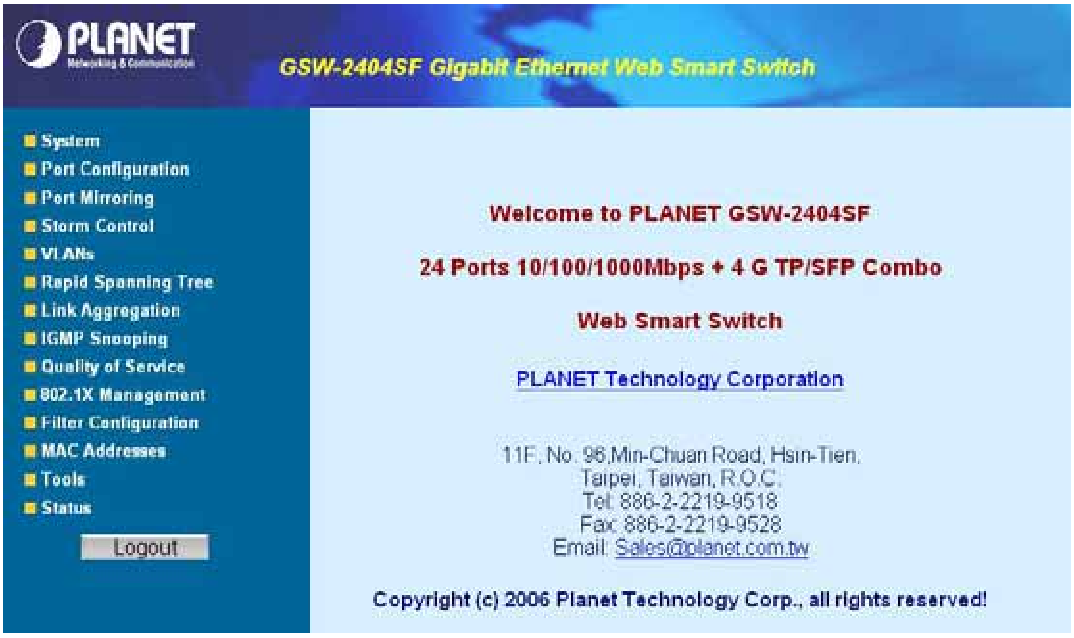
1. For security reason, please change and memorize the new password after this first setup.
2. Only accept command in lowercase letter under web interface.

4. CONFIGURATION

The GSW-1602SF/2404SF Web Smart Gigabit Ethernet 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 /2404SF from the local LAN. This section indicates how to configure the Switch to enable its smart function.

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.



Welcome to PLANET GSW-2404SF

24 Ports 10/100/1000Mbps + 4 G TP/SFP Combo

Web Smart Switch

PLANET Technology Corporation

11F, No. 96,Min-Chuan Road, Hsin-Tien,
Taipei, Taiwan, R.O.C.
Tel: 886-2-2219-9518
Fax: 886-2-2219-9528
Email: Sales@planet.com.tw

Copyright (c) 2006 Planet Technology Corp., all rights reserved!

Figure 4-1 Web Main screen

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

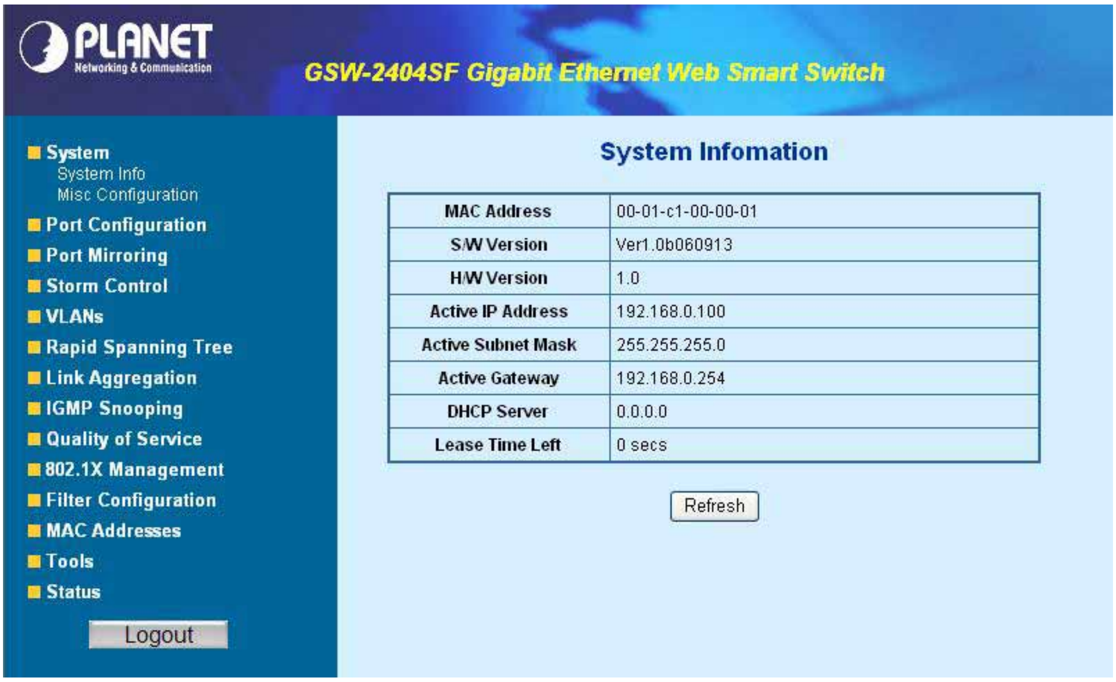
- **System** – Check the hardware, software version and System MAC address. Setting the IP address and SNMP management for the switch.
- **Port Configuration** - Setup per port Speed/Duplex mode, Flow Control and jumbo frame
- **Port Mirroring -** dedicated port monitoring for incoming packets
- **VLANs** – Configure VLAN Member / Port Configuration
- **Rapid Spanning Tree –** Configure Rapid spanning tree topography for any arrangement of bridges. .
- **Link Aggregation** – Port Trunk / LACP
- **IGMP Snooping -** Enables or disables IGMP Snooping on the device to filter the multicast stream.
- **Quality of Service** – Mapping the packet level to classify the packets priority.
- **802.1X Management –** Specify ports with network access control.
- **MAC Address** – Dynamic Address Table / Static MAC Address
- **Tools** – Reboot / Factory Reset / Firmware Update / Configuration Upload / Ping / Cable Diagnostic

- **Status** – Port Statistics Overview / Port Statistics Detail / LACP Status / RSTP Status / IGMP Snooping Status / Multicast Group Status

4.2 System

4.2.1 System Info

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



System Infomation

MAC Address	00-01-c1-00-00-01
S/W Version	Ver1.0b060913
H/W Version	1.0
Active IP Address	192.168.0.100
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.0.254
DHCP Server	0.0.0.0
Lease Time Left	0 secs

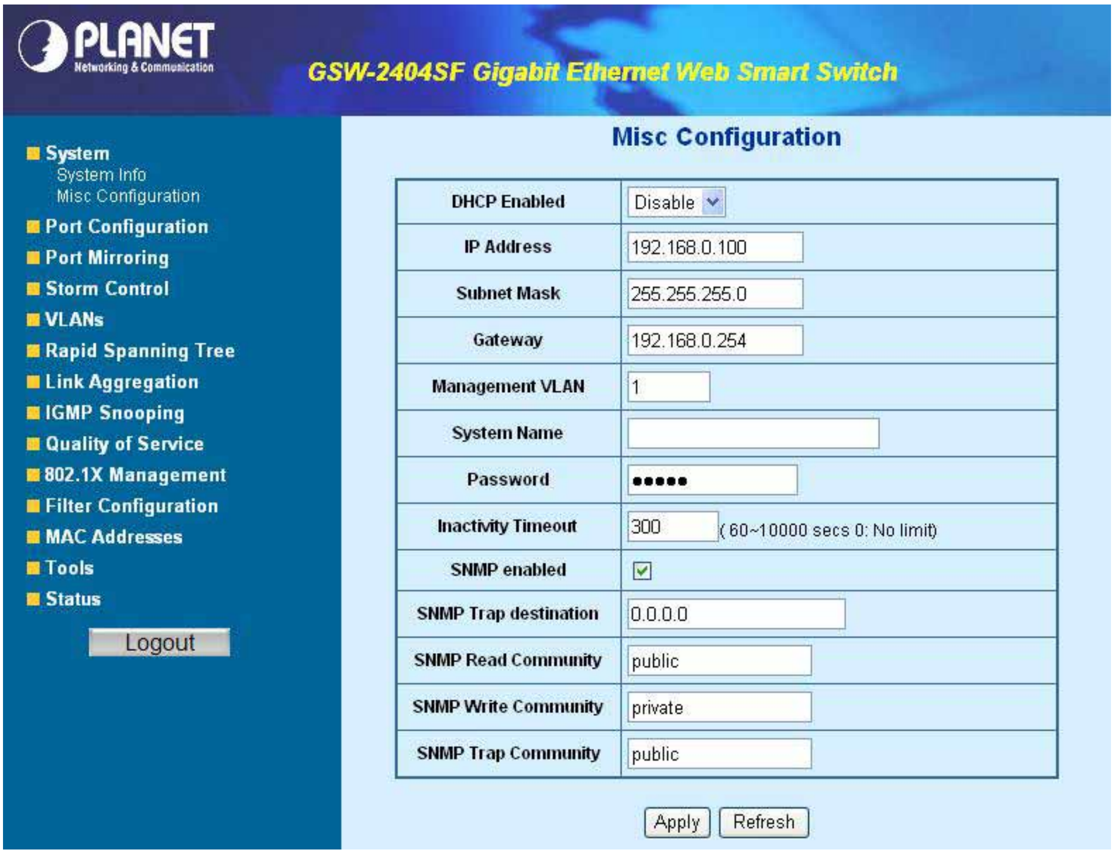
Figure 4-2 System Information screen

The page includes the following fields:

- **MAC Address** Specifies the device MAC address.
- **S/W Version** The current software version running on the device.
- **H/W Version** The current hardware versions running on the device
- **Active IP Address** The current IP Address of the device. The IP Address could be manual assigned or get via DHCP server.
- **Active Subnet Mask** The current IP Subnet Mask setting on the device.
- **DHCP Server** If the IP address is got and assigned via a DHCP server, the field shows the IP Address of the DHCP server.
- **Lease Time left** If the IP address of the device be assigned via a DHCP Server, a DHCP lease time would be apply to the device too. The lease time left shows the left time if the device didn't request the IP Address to the DHCP server, then the IP address will be released.

4.2.2 Misc Configuration

The Misc Configuration includes the System name, Location name, Login Timeout, IP Address, Subnet Mask and Gateway. Through the Web Switch Utility, you can easily recognize the device by using the System Name and the Location Name. The Login Timeout is to set the idle time-out for security issue, when there is no action in running the Web Switch Utility and the time is up, you must re-login to Web Switch Utility before you set the Utility. Fill up the IP Address, Subnet Mask and Gateway for the device. The screen in Figure 4-3 appears.



Misc Configuration

DHCP Enabled	Disable
IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Gateway	192.168.0.254
Management VLAN	1
System Name	
Password	●●●●●
Inactivity Timeout	300 (60~10000 secs 0: No limit)
SNMP enabled	☑
SNMP Trap destination	0.0.0.0
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Community	public

Figure 4-3 Misc Configuration screen

The page includes the following configurable data:

DHCP Enable - Choose what the 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 interface. The factory default value is **192.168.0.100**

Subnet Mask - The IP subnet mask for the interface. The factory default value is **255.255.255.0**

Gateway - The default gateway for the IP interface. The factory default value is 192.168.0.254

Management VLAN - Specifies the management VLAN ID of the switch. It may be configured to any value in the range of 1 - 4093. The management VLAN is used for management of the switch.

System Name – Defines the user-defined device name

Password - This function provides administrator to secure Web login

Inactivity Timeout – Specifies a time period for the user login. The web interface will be auto logout if there're no actions from the login user.

The default value is **300** seconds; 0 means no inactivity time limit.

SNMP Enable – 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.

SNMP Trap The Trap function enables the Switch to monitor the Trap through the Web Switch

destination – Utility, set the Trap IP Address of the manager workstation where the trap to be sent

SNMP 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.

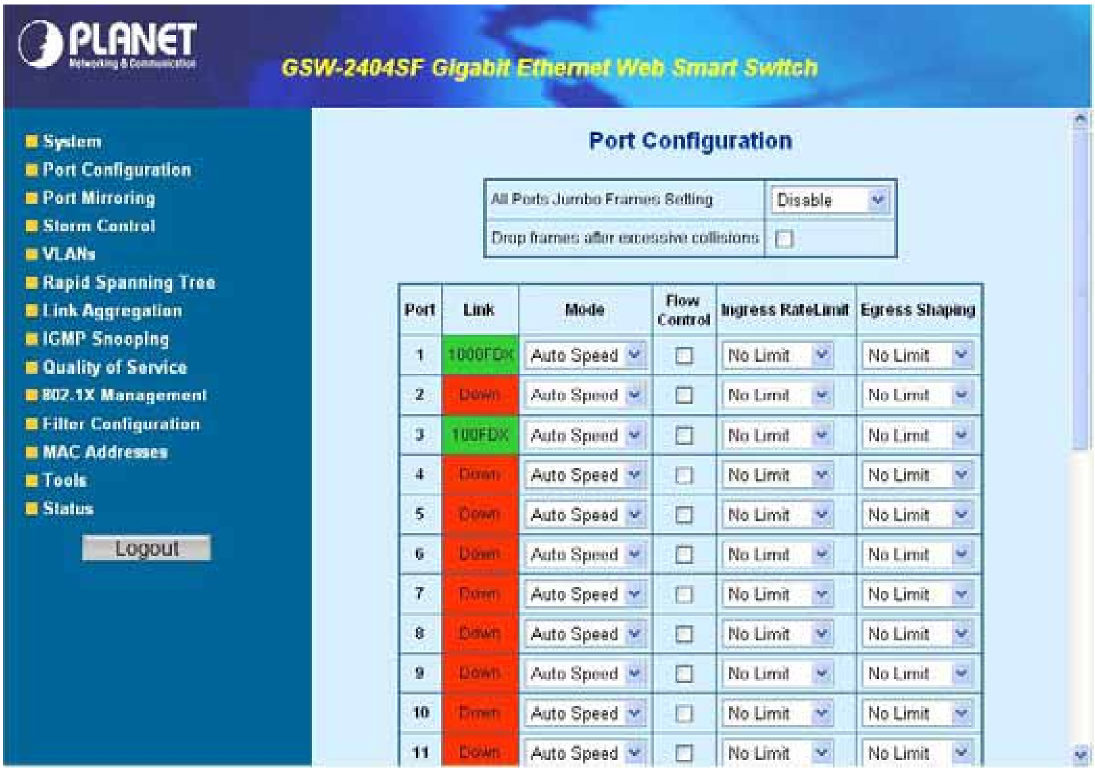
SNMP write Community – Functions as a password and used to authenticate the access right of the device. The Write Community accesses the device both read and write - configure to the device via SNMP.

SNMP Trap Community – Identifies the community string of the trap manager

✍ ***Note:*** After change the default password, if you forget the password. Please press and release the ***"Reset"*** button in the front panel of GSW-1602SF/2404SF, the current setting includes VLAN, will be lost and the GSW-1602SF/2404SF will restore to the default mode.

4.3 Port Configuration

This function allows displaying each port’s status. The Link Status in the screen displays the current connection speed and duplex mode; else this function will show *down* when the port is disconnected. Press the ***“Refresh”*** button to renew the screen. The screen in Figure 4-4 appears.



Port Configuration

All Ports Jumbo Frames Setting	Disable
Drop frames after excessive collisions	□

Port	Link	Mode	Flow Control	Ingress RateLimit	Egress Shaping
1	1000FDX	Auto Speed	□	No Limit	No Limit
2	Down	Auto Speed	□	No Limit	No Limit
3	100FDX	Auto Speed	□	No Limit	No Limit
4	Down	Auto Speed	□	No Limit	No Limit
5	Down	Auto Speed	□	No Limit	No Limit
6	Down	Auto Speed	□	No Limit	No Limit
7	Down	Auto Speed	□	No Limit	No Limit
8	Down	Auto Speed	□	No Limit	No Limit
9	Down	Auto Speed	□	No Limit	No Limit
10	Down	Auto Speed	□	No Limit	No Limit
11	Down	Auto Speed	□	No Limit	No Limit

Figure 4-4 Port Configuration screen

The page includes the following configurable data:

- **All Ports Jumbo Frames Setting**

  The maximum Ethernet frame size the interface supports or is configured, including Ethernet header, CRC, and payload. Draw the menu bar to select the mode.

  - Disable - The default maximum frame size is 1518
  - 4096 Kbytes – Set the maximum frame size to 4096 Bytes
  - 9600 Kbytes - Set the maximum frame size to 9600 Bytes

- **Drop frames after excessive collisions**

  Enable or Disable the device to drop frames once the excessive collisions be detected.

- **Port**

  Indicate port 1 to port 24.

- **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.

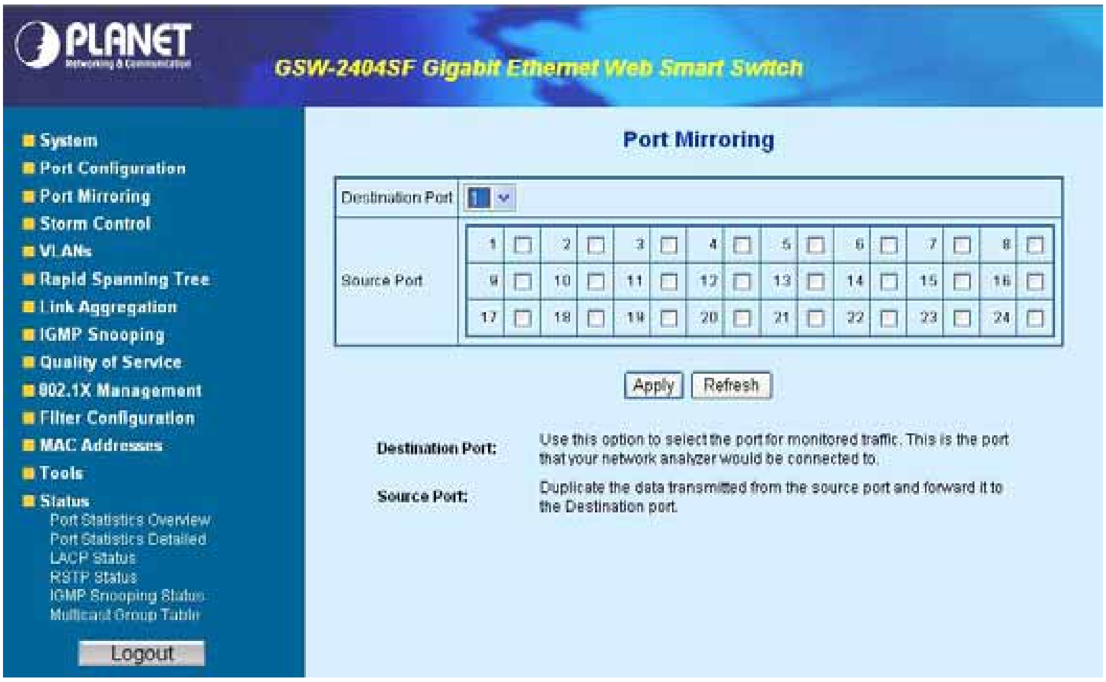
  Default : **No Limit**

  The range between 128 Kbps to 3968 kbps.

Note: When set each port to run at 100M Full, 100M Half, 10M Full, and 10M Half-speed modes. The Auto-MDIX function will disable.

4.4 Port Mirroring

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 screen in Figure 4-5 appears.



Port Mirroring

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

Destination Port: Use this option to select the port for monitored traffic. This is the port that your network analyzer would be connected to.

Source Port: Duplicate the data transmitted from the source port and forward it to the Destination port.

Figure 4-5 Mirror Setting screen

The page includes the following configurable data:

• **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.

Configuring the port mirroring by assigning a source port from which to copy all packets and a destination port where those packets will be sent.

Note: With the Chipset specification – the GSW-1602SF/2404SF port mirroring support **RX (receive) mode only -** this mode will duplicate the data that send to the source and forward to the destination port.

4.5 VLANs

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/2404SF switch supports 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.

4.5.1 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 4-6 appears.

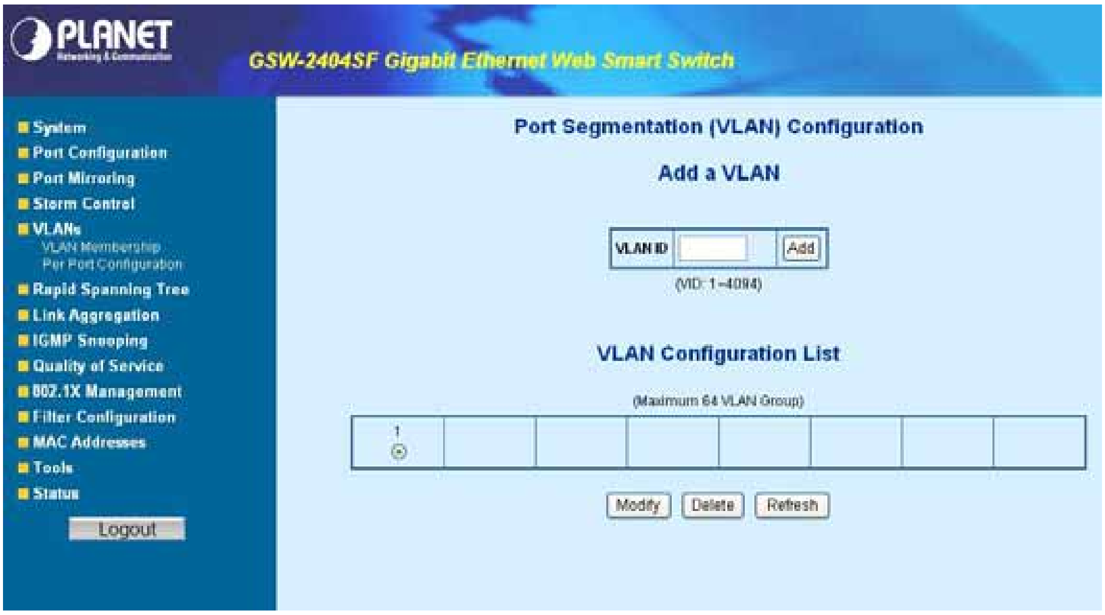


Figure 4-6 VLAN Membership screen

The page includes the following items:

- **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 assign 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.

4.5.1.1 Add a VLAN Group

The PLANET Web-Smart switch supports up to 64 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.

As show in Figure 4-7 and Figure 4-8

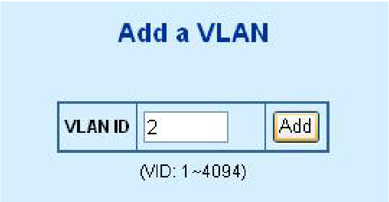
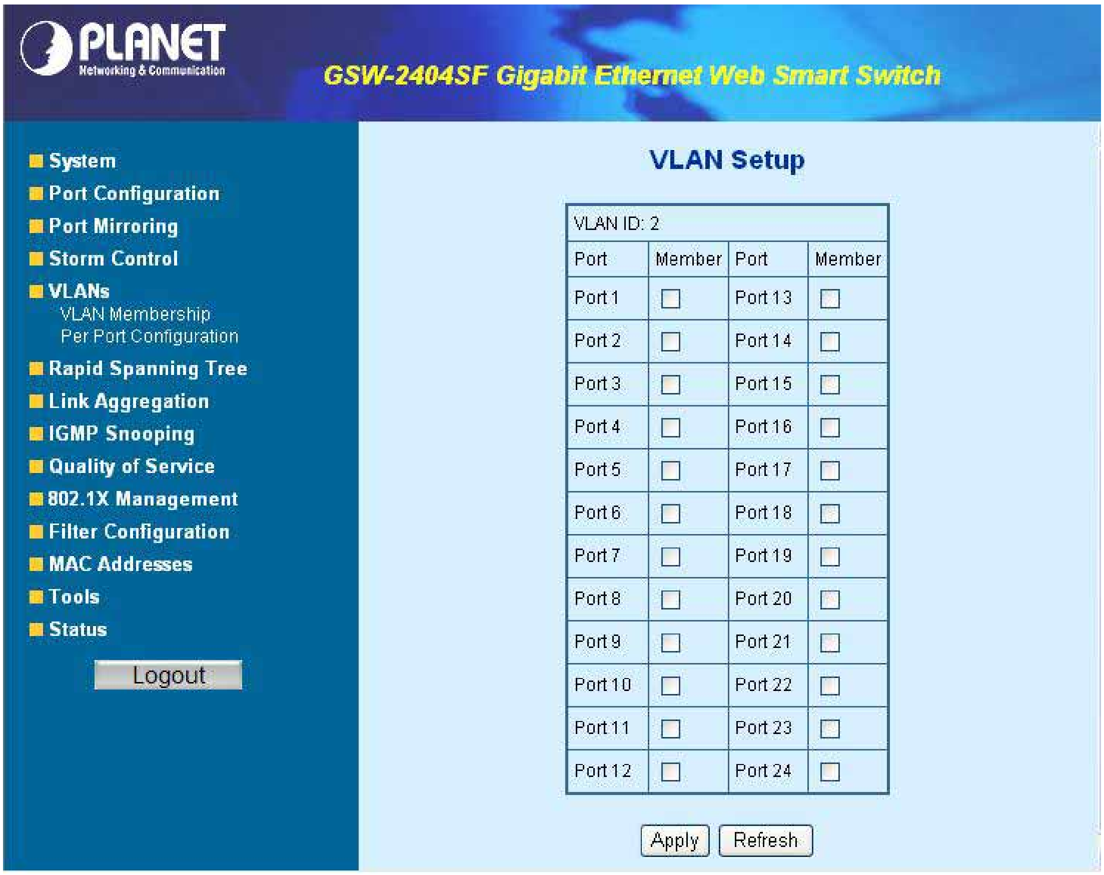


Figure 4-7 Add a VLAN screen



VLAN ID: 2			
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	☐

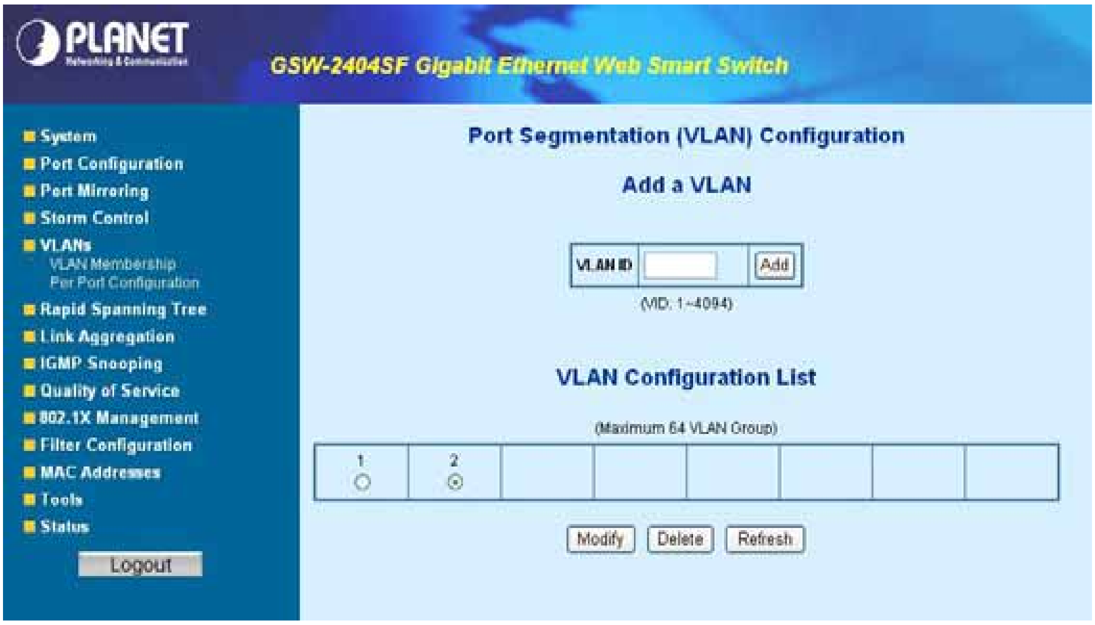
Figure 4-8 VLAN Member Setup screen

4.5.1.2 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 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 4-9 appears.



Port Segmentation (VLAN) Configuration

Add a VLAN

VLAN ID [ ] (VID: 1~4094)

VLAN Configuration List

(Maximum 64 VLAN Group)

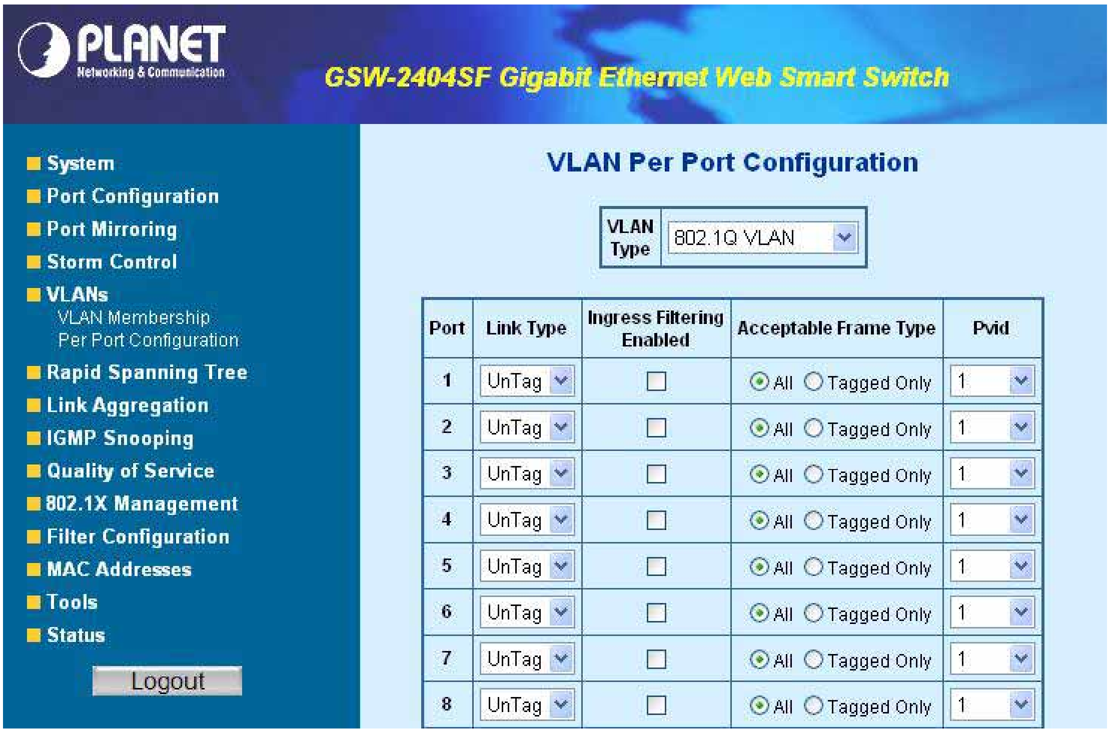
1	2						
○	●						

Figure 4-9 VLAN Group – member modify and delete VLAN Group screen

Note: 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"

4.5.2 Per Port Configuration

The VLAN Per Port Configuration page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Configuration page. All untagged packets arriving to the device are tagged by the ports PVID. The screen in Figure 4-10 appears.



VLAN Per Port Configuration

VLAN Type: 802.1Q VLAN

Port	Link Type	Ingress Filtering Enabled	Acceptable Frame Type	Pvid
1	UnTag	□	● All ○ Tagged Only	1
2	UnTag	□	● All ○ Tagged Only	1
3	UnTag	□	● All ○ Tagged Only	1
4	UnTag	□	● All ○ Tagged Only	1
5	UnTag	□	● All ○ Tagged Only	1
6	UnTag	□	● All ○ Tagged Only	1
7	UnTag	□	● All ○ Tagged Only	1
8	UnTag	□	● All ○ Tagged Only	1

Figure 4-10 VLAN Port Configuration

The page includes the following fields:

- **VLAN Type -** There’re two VLAN mode support – 802.1Q VLAN and Port-Bas VLAN

  - **802.1Q** – Packets income will be tagged with VID as the PVID setting. All ports on the 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.

- **Port -** Select the physical interface for which you want to display or configure data.

- **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 Types -** 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.

- **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.

4.5.3 VLAN setting example:

4.5.3.1 Two separate 802.1Q VLAN

The diagram shows how the 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 4-11 appears and Table 4-1 describes the port configuration of switch.

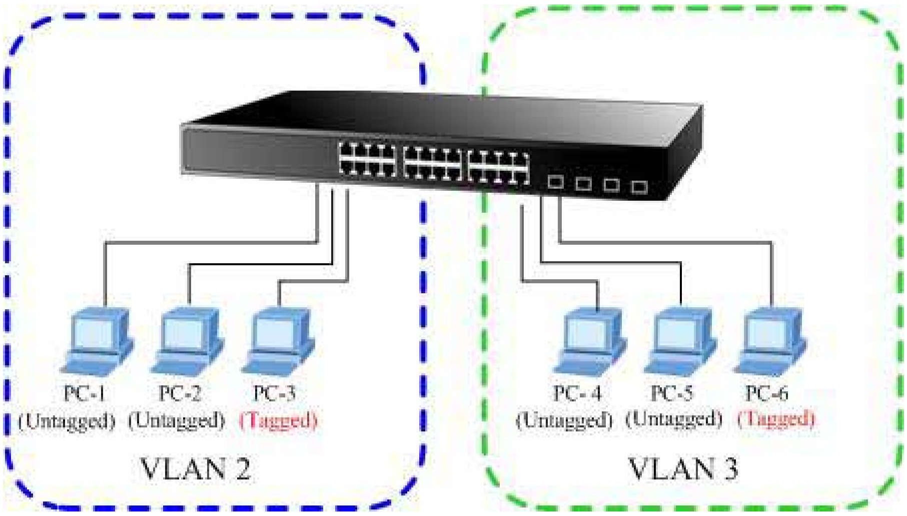


Figure 4-11 two separate VLAN diagram

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 4-1 VLAN and Port Configuration

The scenario described as follow:

- **Untagged packet entering VALN 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**.

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

Setup steps

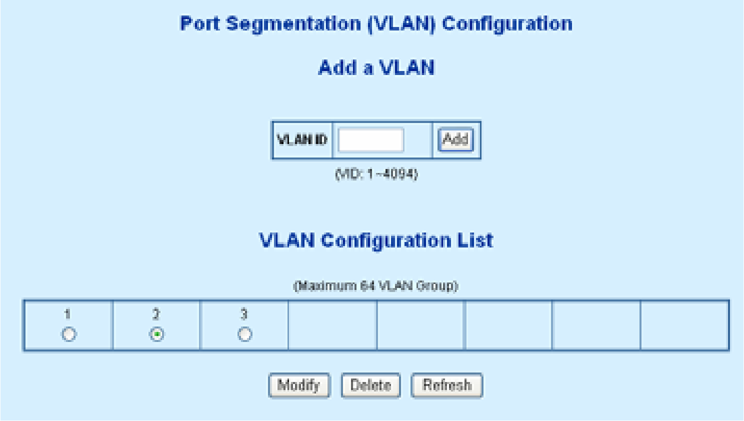
1. Create VLAN Group

Set VALN 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*



Port Segmentation (VLAN) Configuration

Add a VLAN

VLAN ID [ ] (VID: 1~4094)

VLAN Configuration List

(Maximum 64 VLAN Group)

1	2	3					
○	●	○					

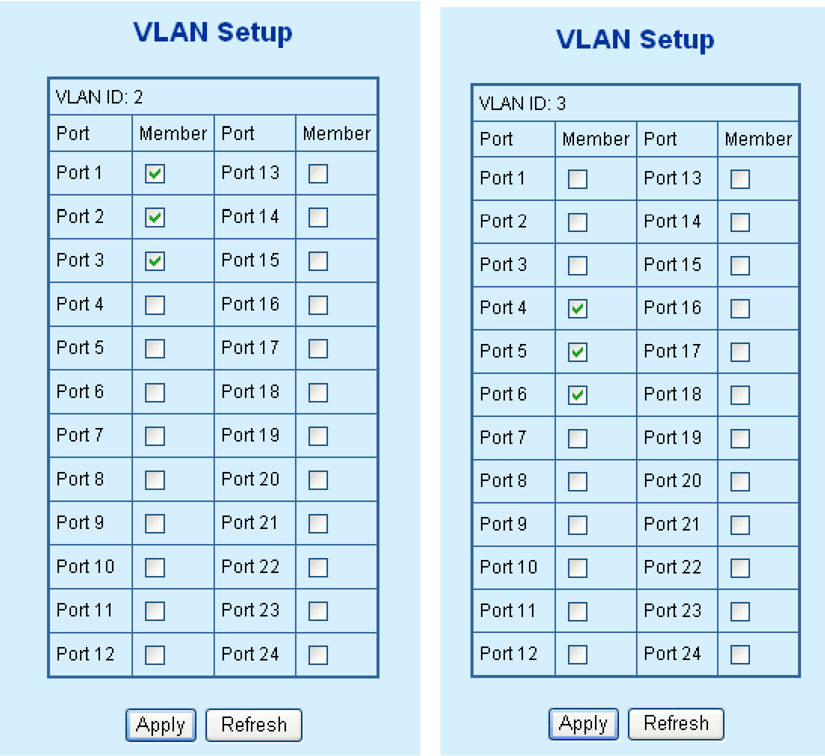
Figure 4-12 Add new VLAN Group screen

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*



VLAN Setup

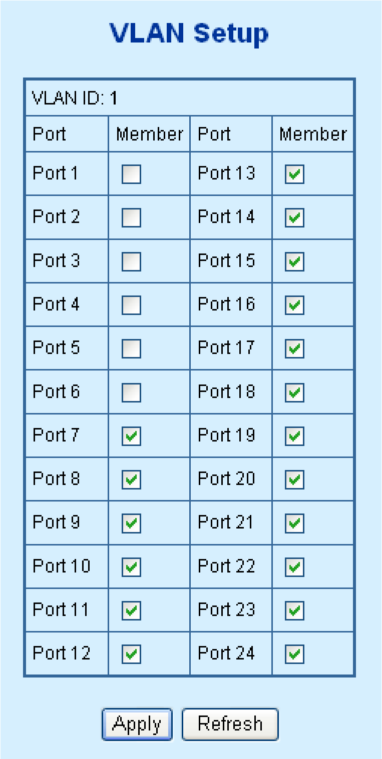
VLAN ID: 2			
Port	Member	Port	Member
Port 1	☑	Port 13	□
Port 2	☑	Port 14	□
Port 3	☑	Port 15	□
Port 4	□	Port 16	□
Port 5	□	Port 17	□
Port 6	□	Port 18	□
Port 7	□	Port 19	□
Port 8	□	Port 20	□
Port 9	□	Port 21	□
Port 10	□	Port 22	□
Port 11	□	Port 23	□
Port 12	□	Port 24	□

VLAN Setup

VLAN ID: 3			
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	□

Figure 4-13 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 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	☑

Figure 4-14 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*

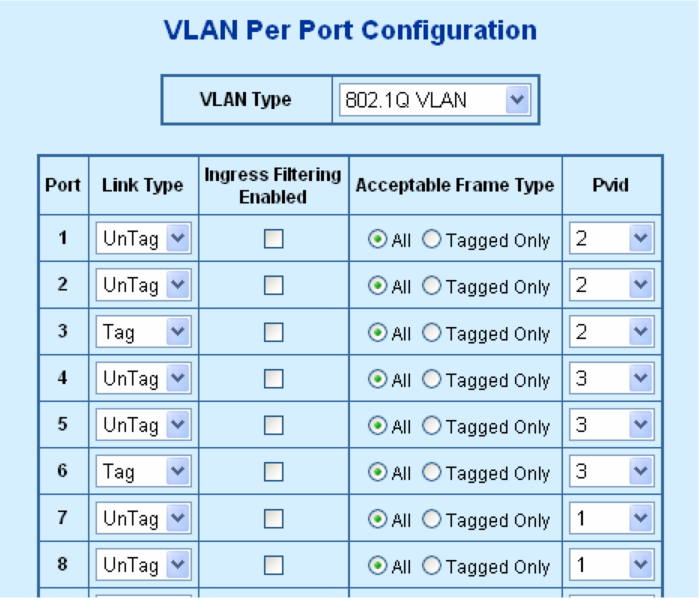
   Port-4,Port-5 and Port-6 : PVID=*3*

   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 4-15 appears.



VLAN Per Port Configuration

VLAN Type: 802.1Q VLAN

Port	Link Type	Ingress Filtering Enabled	Acceptable Frame Type	Pvid
1	UnTag	□	● All ○ Tagged Only	2
2	UnTag	□	● All ○ Tagged Only	2
3	Tag	□	● All ○ Tagged Only	2
4	UnTag	□	● All ○ Tagged Only	3
5	UnTag	□	● All ○ Tagged Only	3
6	Tag	□	● All ○ Tagged Only	3
7	UnTag	□	● All ○ Tagged Only	1
8	UnTag	□	● All ○ Tagged Only	1

Figure 4-15 Port 1-Port 6 VLAN Configuration

4.5.3.2 Two VLANs with overlap area

Follow the example of 4.5.3.1. 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 4-16 appear. This section will show you how to configure the port for the server – that could be accessed by both VLAN 2 and VLAN 3.

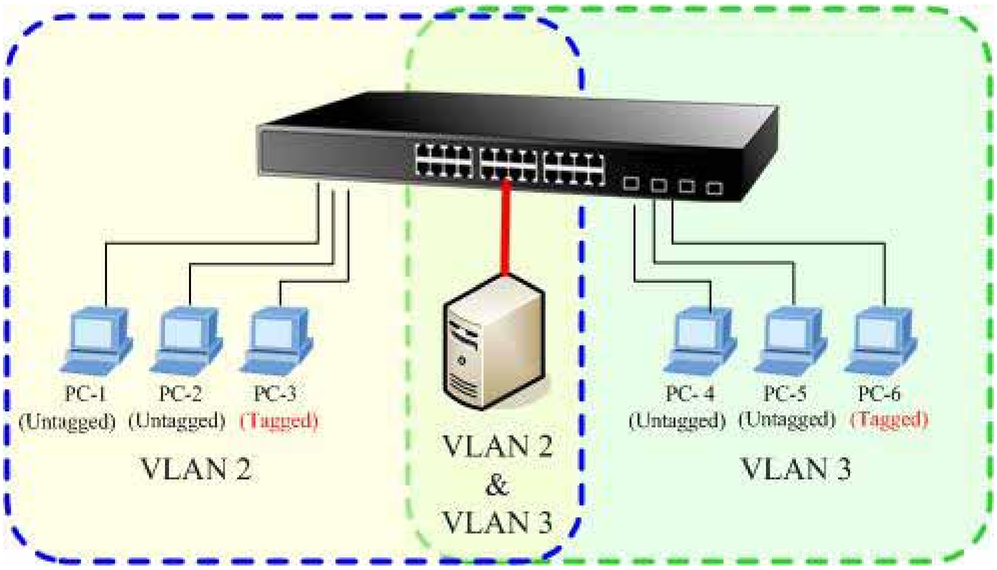
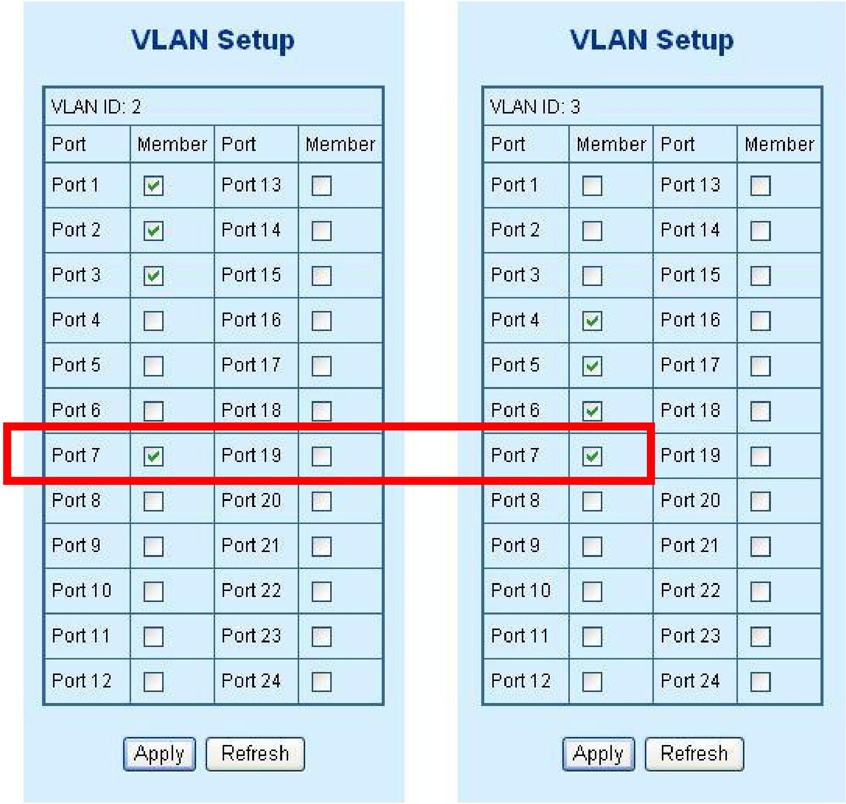


Figure 4-16 A Server connect to the VLAN overlap area

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 4-17 appears.



VLAN Setup

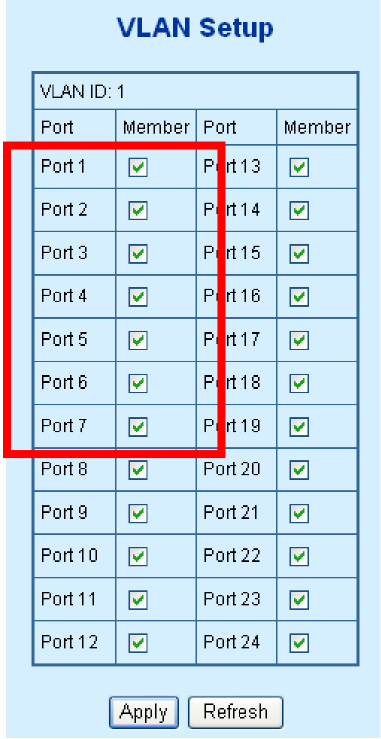
VLAN ID: 2			
Port	Member	Port	Member
Port 1	☑	Port 13	□
Port 2	☑	Port 14	□
Port 3	☑	Port 15	□
Port 4	□	Port 16	□
Port 5	□	Port 17	□
Port 6	□	Port 18	□
Port 7	☑	Port 19	□
Port 8	□	Port 20	□
Port 9	□	Port 21	□
Port 10	□	Port 22	□
Port 11	□	Port 23	□
Port 12	□	Port 24	□

VLAN Setup

VLAN ID: 3			
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	□

Figure 4-17 VLAN overlap port setting

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

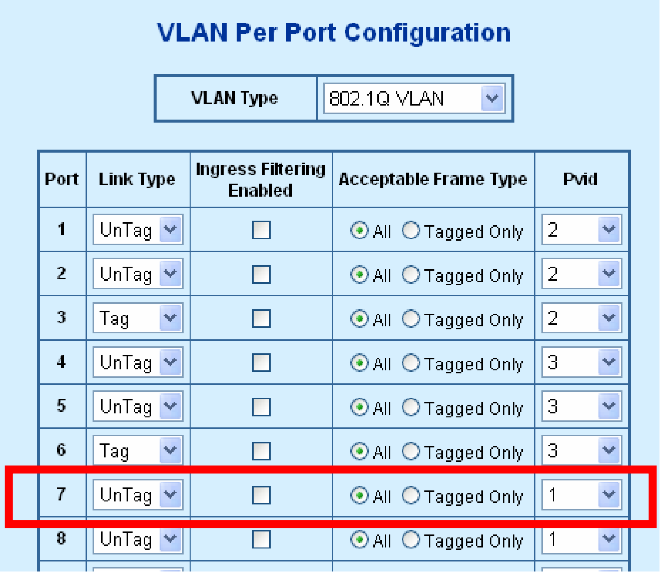


VLAN Setup

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	☑

Figure 4-18 VLAN 1 – The public area member assign

4. Setup **Port-7** with "**PVID=1**" at VLAN Per Port Configuration page. The screen in Figure 4-19 appears.



VLAN Per Port Configuration

VLAN Type: 802.1Q VLAN

Port	Link Type	Ingress Filtering Enabled	Acceptable Frame Type	Pvid
1	UnTag	□	● All ○ Tagged Only	2
2	UnTag	□	● All ○ Tagged Only	2
3	Tag	□	● All ○ Tagged Only	2
4	UnTag	□	● All ○ Tagged Only	3
5	UnTag	□	● All ○ Tagged Only	3
6	Tag	□	● All ○ Tagged Only	3
7	UnTag	□	● All ○ Tagged Only	1
8	UnTag	□	● All ○ Tagged Only	1

Figure 4-19 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 belong to VLAN 1. But with different PVID settings, packets form VLAN 2 or VLAN 3 is not able to access to the other VLAN.

4.5.3.3 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-20 appears.

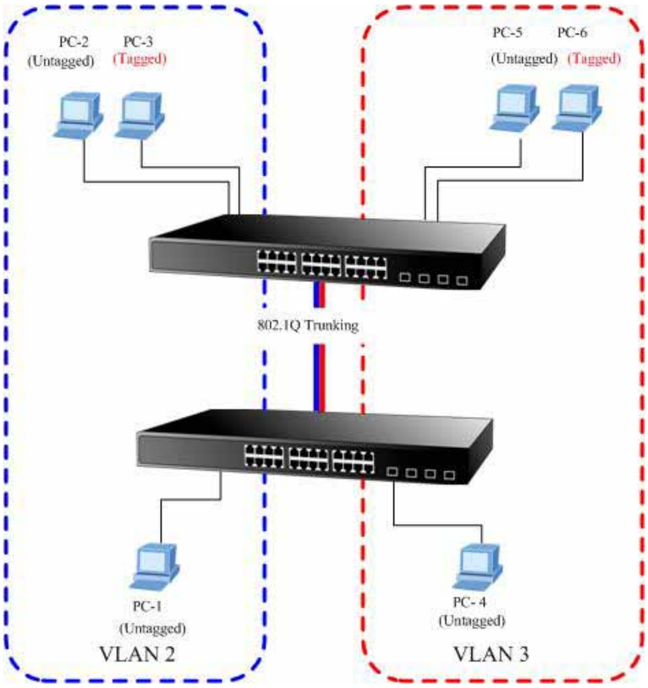
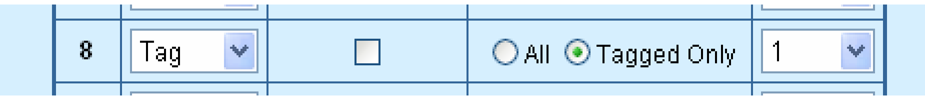


Figure 4-20 802.1Q Trunking with other VLAN aware device

About the VLAN ports connect to the hosts, please refer to 4.5.3.1 and 4.5.3.2 examples. The following steps will focus on the VLAN **Trunk port** configuration.

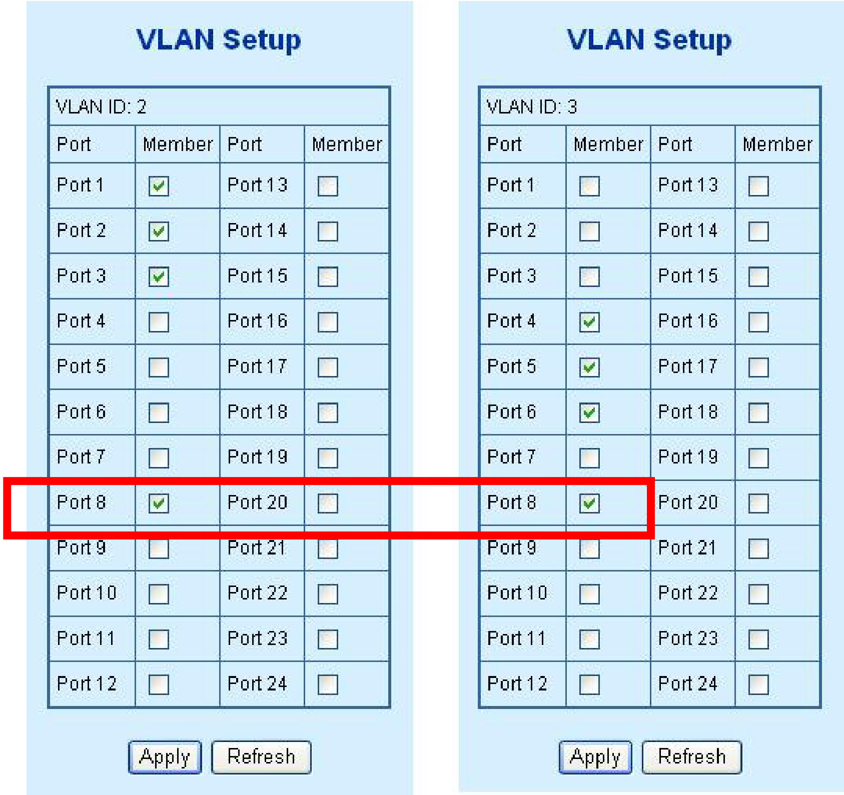
1. Specify **Port-8** to be the 802.1Q VLAN **Trunk port**, and the Trunking port must be a **Tagged** port while egress. The Port-8 configuration as the following screen in Figure 4-21.



8	Tag	□	○ All ● Tagged Only	1

Figure 4-21 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.



VLAN Setup

VLAN ID: 2			
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	□

VLAN Setup

VLAN ID: 3			
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	□

Figure 4-22 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.

4.6 Rapid Spanning

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.

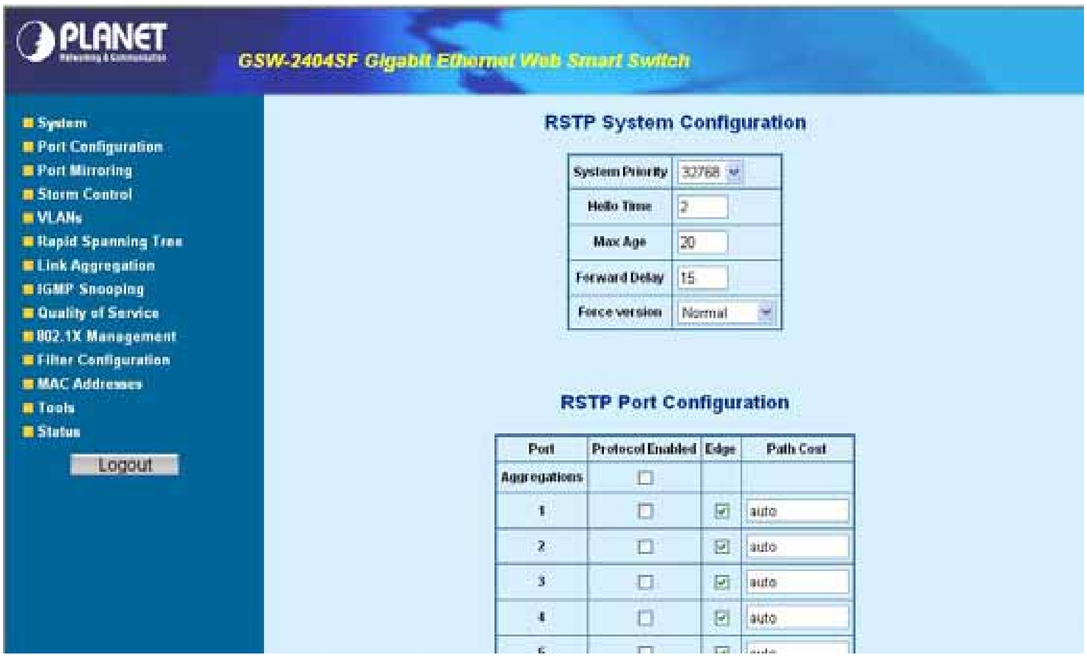
Rapid Spanning Tree Protocol (RSTP) - While Classic Spanning Tree guarantees preventing L2 forwarding loops in a general network topology, convergence can take up to 30-60 seconds. The convergence time is considered too long for many applications. When network topology allows, faster convergence may 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 devices 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 switch support IEEE 802.1d Spanning Tree (STP), IEEE 802.1w Rapid Spanning Tree (RSTP). The screen in Figure 4-23 appears.



RSTP System Configuration

System Priority	32768
Hello Time	2
Max Age	20
Forward Delay	15
Force version	Normal

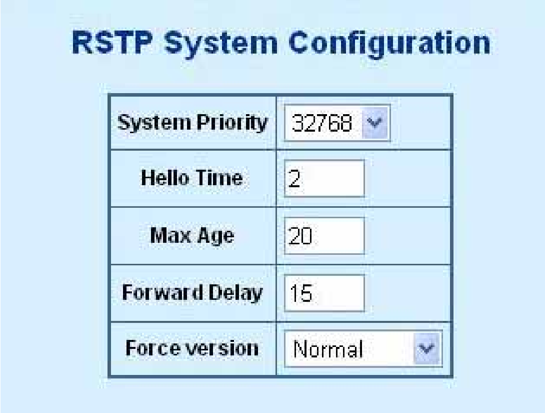
RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost
Aggregations	□		
1	□	☑	auto
2	□	☑	auto
3	□	☑	auto
4	□	☑	auto
5	□	☑	auto

Figure 4-23 Rappid Spanning Tree System/Port Configuration

4.6.1 RSTP System Configuration

The “RSTP System Configuration” table allows configuring the spanning tree parameters.



RSTP System Configuration

System Priority	32768
Hello Time	2
Max Age	20
Forward Delay	15
Force version	Normal

Figure 4-24 RSTP System Configuration

The page includes the following fields:

- **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.

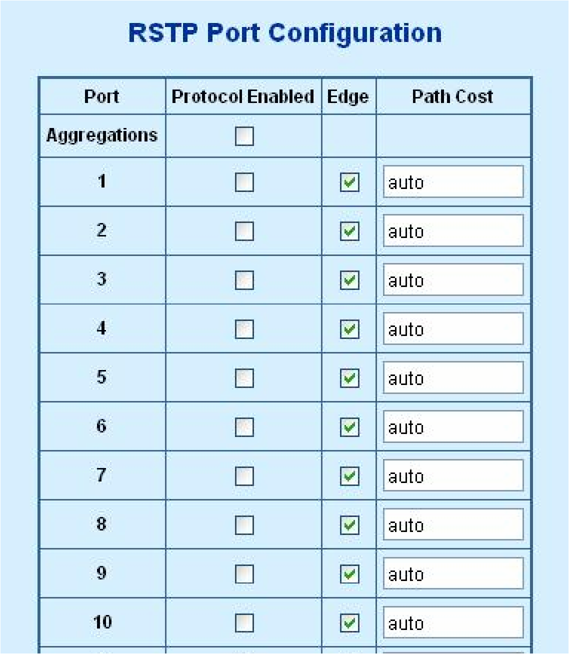
  Compatible – Classis STP(802.1d) : Provides a single path between end stations, avoiding and eliminating loops.

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.

4.6.2 RSTP Port Configuration

The RSTP Port Configuration page contains fields for assigning RSTP properties to individual ports. The screen in Figure 4-25 appears.



RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost
Aggregations	□		
1	□	☑	auto
2	□	☑	auto
3	□	☑	auto
4	□	☑	auto
5	□	☑	auto
6	□	☑	auto
7	□	☑	auto
8	□	☑	auto
9	□	☑	auto
10	□	☑	auto

Figure 4-25 RSTP Port Configuration

The page includes the following fields:

- **Port** Indicate port 1 to port 24.
- **Aggregations** Link Aggregation group setting, created by Port Trunk or LACP
- **Protocol Enabled** Enables or disables RSTP protocol on the selected port.
- **Edge** Indicates whether the port is enabled as an edge port.

  Edge port cannot create loops, but it loses edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status
- **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 Rage : 1-20000000

  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

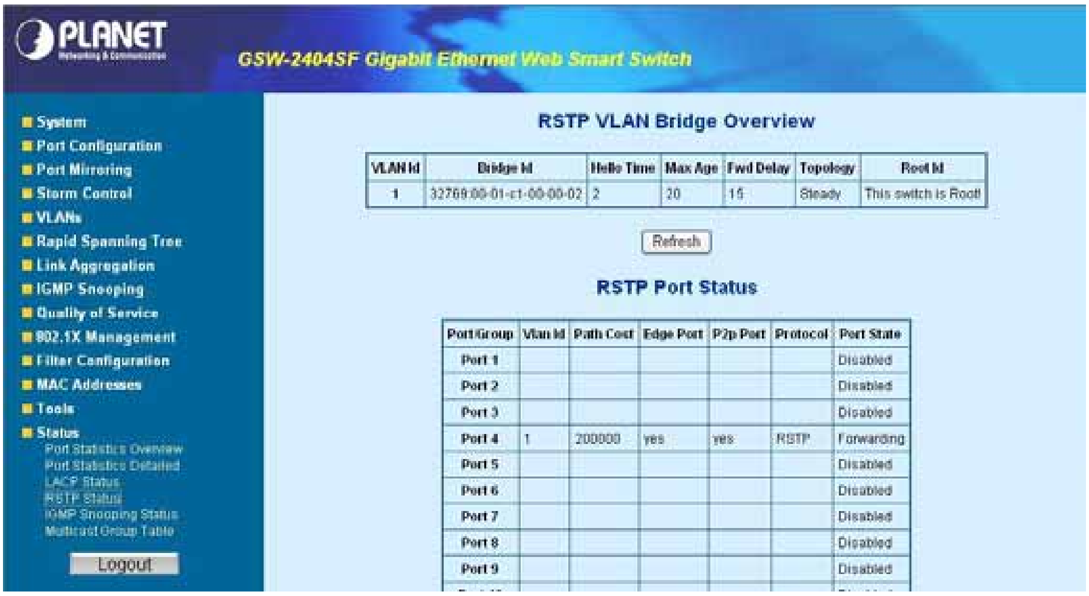
4.6.3 RSTP Status

The RSTP Status page display the current STP bridge , roor bridge and per port stp status.

To open **RSTP Status** screen perform the folling:

1. Click Status -> RSTP Status

2. The “RSTP VLAN Bridge Overview” and “RSTP Port Status” screen is displayed as in Figure 4-26.



RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-01-c1-00-00-02	2	20	15	Steady	This switch is Root!

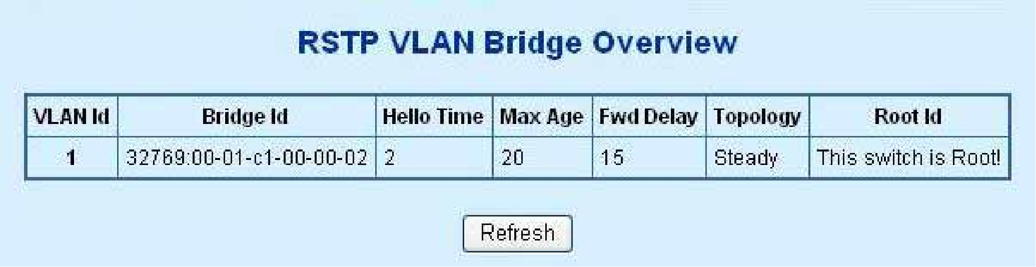
RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Disabled
Port 2						Disabled
Port 3						Disabled
Port 4	1	200000	yes	yes	RSTP	Forwarding
Port 5						Disabled
Port 6						Disabled
Port 7						Disabled
Port 8						Disabled
Port 9						Disabled

Figure 4-26 RSTP Status screen

- **RSTP VLAN Bridge Overview**

The information of the RSTP Root shows in the Bridge overview table. The screen in Figure 4-27 appears.



RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-01-c1-00-00-02	2	20	15	Steady	This switch is Root!

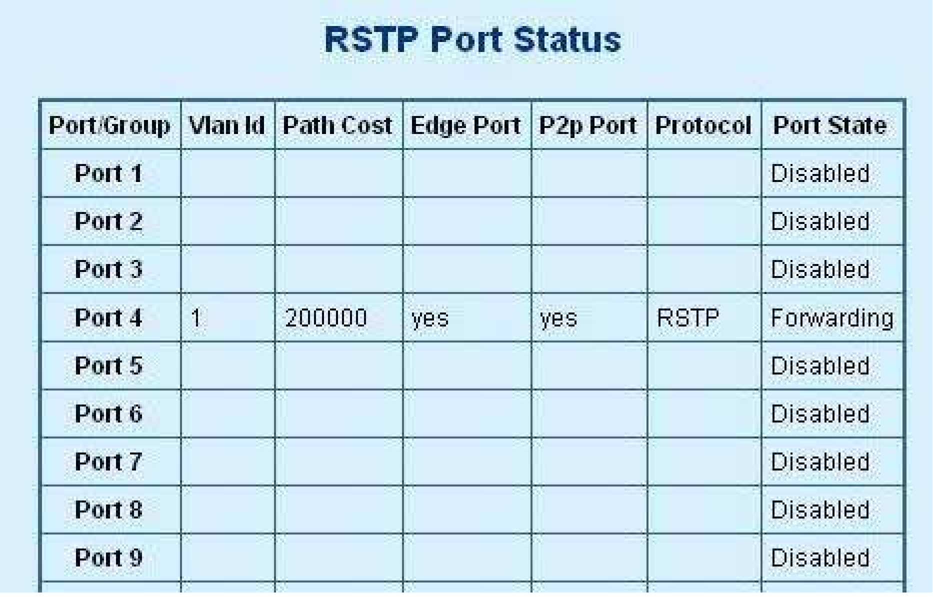
Figure 4-27 RSTP Status screen

The page includes the following fields:

• **VLAN Id**	Identifies VLANs associated with the Rapid Spanning Tree.
• **Bridge IDd**	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.

■ RSTP Port Status

The information of the RSTP Per Port and Trunk group shows in the RSTP Port Status table. The screen in Figure 4-28 appears.



RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Disabled
Port 2						Disabled
Port 3						Disabled
Port 4	1	200000	yes	yes	RSTP	Forwarding
Port 5						Disabled
Port 6						Disabled
Port 7						Disabled
Port 8						Disabled
Port 9						Disabled

Figure 4-28 RSTP Status screen

The page includes the following fields:

- **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.

✍ *Note:* **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

4.7 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 :

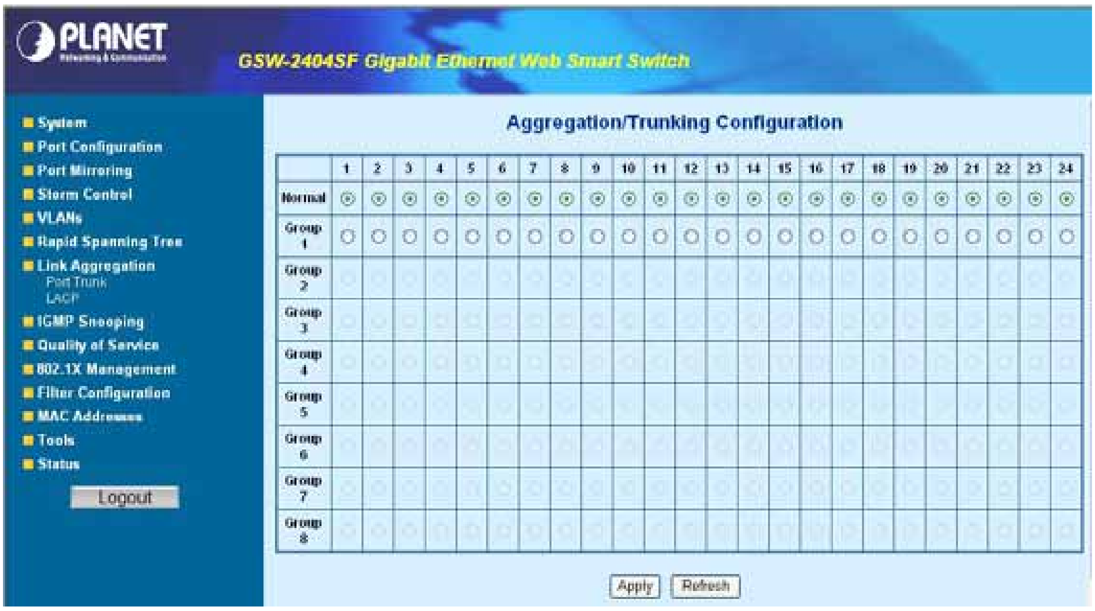
- **Static LAGs** (**Port Trunk**) – Force aggregared selected ports to be a trounk group.
- **Link Aggregation Control Protocol** (**LACP**) LAGs - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

4.7.1 Port Trunk

This function provides to cascade two Switch devices with a double bandwidth (maximum up to 1.6/2.4Gbps in full duplex mode).

- Eight Trunk Group per system
- For GSW-1602SF, up to 8 ports per Trunk Group
- For GSW-2404SF, up to 12 ports per Trunk Group

The Port Trunking configuration screen in Figure 4-29 appears.



Aggregation/Trunking Configuration

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
Group 1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 4-29 Aggregation/Trunking Configuration screen

The page includes the following fields:

- **Port** Indicate port 1 to port 24.
- **Normal** While a port be checked as "Normal", the port is not join to any Static Trunk Group.
- **Group** 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:

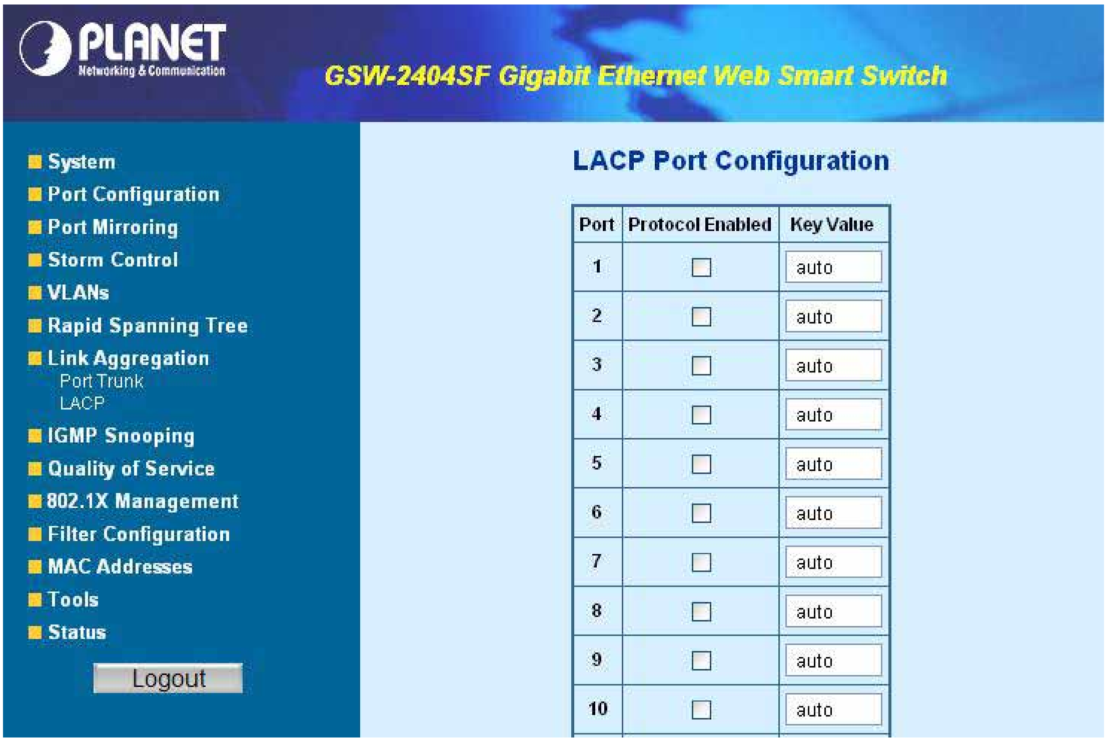
  GSW-1602SF – Up to 8 ports per Trunk Group
  GSW-2404SF – Up to 12 ports per Trunk Group

  A port can be assigned to only one Trunk Group.

4.7.2 LACP

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 4-30 appears.



LACP Port Configuration

Port	Protocol Enabled	Key Value
1	☐	auto
2	☐	auto
3	☐	auto
4	☐	auto
5	☐	auto
6	☐	auto
7	☐	auto
8	☐	auto
9	☐	auto
10	☐	auto

Figure 4-30 LACP Port Configuration

The page includes the following fields:

- **Port** Indicate port 1 to port 24.
- **Protocol 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** 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 “**Auto**”

✍ ***Note:***

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.

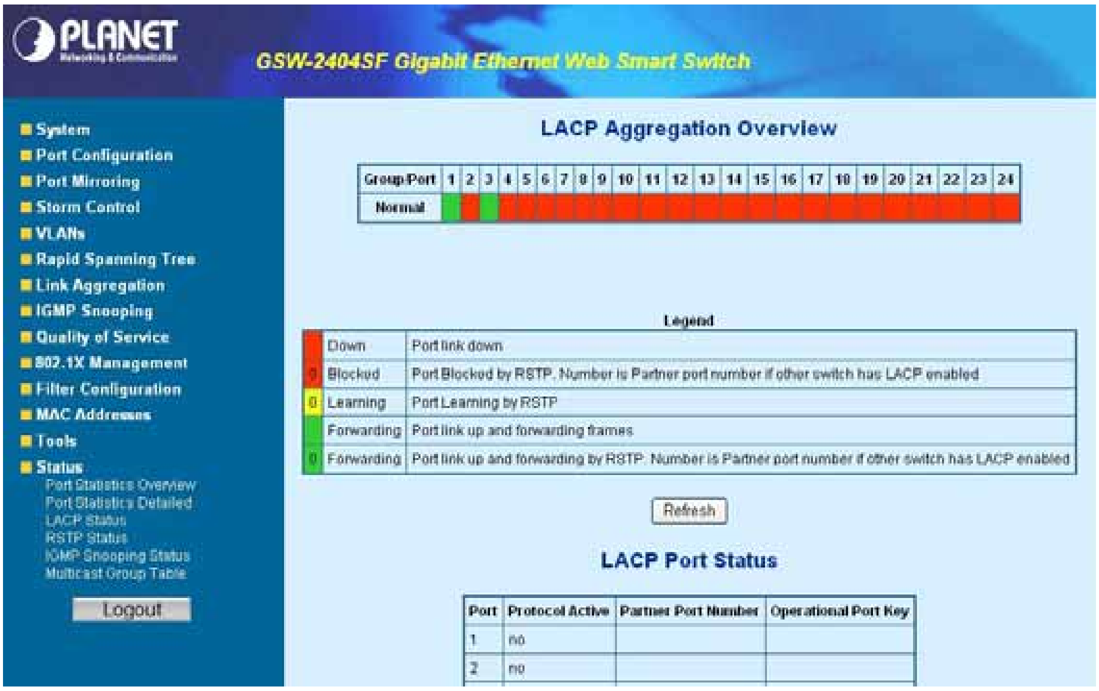
4.7.3 LACP Status

The LACP Status page display the current LACP aggregation Groups and LACP Port status.

To open **LACP Status** screen perform the folling:

1. Click Status -> LACP Status

2. The “LACP Aggregation Overview” and “LACP Port Status” screen is displayed as in Figure 4-31.



LACP Aggregation Overview

Group/Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	🟩	🟥	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

Legend

🟥	Down	Port link down
0	Blockud	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
0	Learning	Port Learning by RSTP
🟩	Forwarding	Port link up and forwarding frames
0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

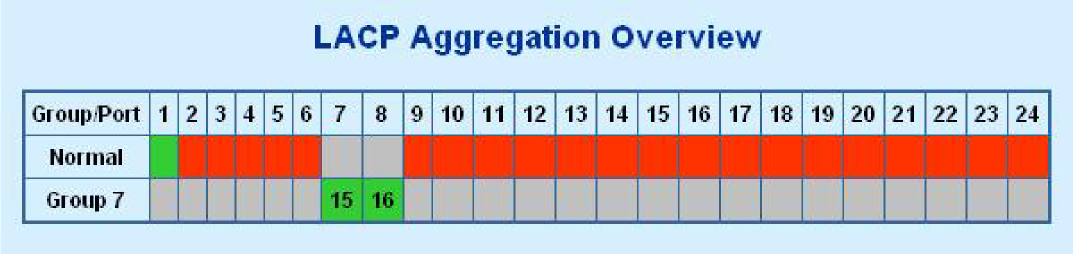
LACP Port Status

Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		

Figure 4-31 LACP Status

- **LACP Aggregation Overview Table**

The LACP Aggregation Overview Table lists the active LACP ports and mapped Group. It also indicate the Partner Port number of the other LACP aware switches. The screen in Figure 4-32 appears.



LACP Aggregation Overview

Group/Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	🟩	🟥	🟥	🟥	🟥	🟥			🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Group 7							🟩 15	🟩 16																

Figure 4-32 LACP Aggregation Overview

The page includes the following fields:

- **Group / Port** Indicate port 1 to port 24.
- **Normal** While a port be checked as “Normal”, the port is not join to any LACP Trunk Group.
- **Group #** The Linked LACP aggregation group. The Group ID is the fist port ID of the LACP group member.

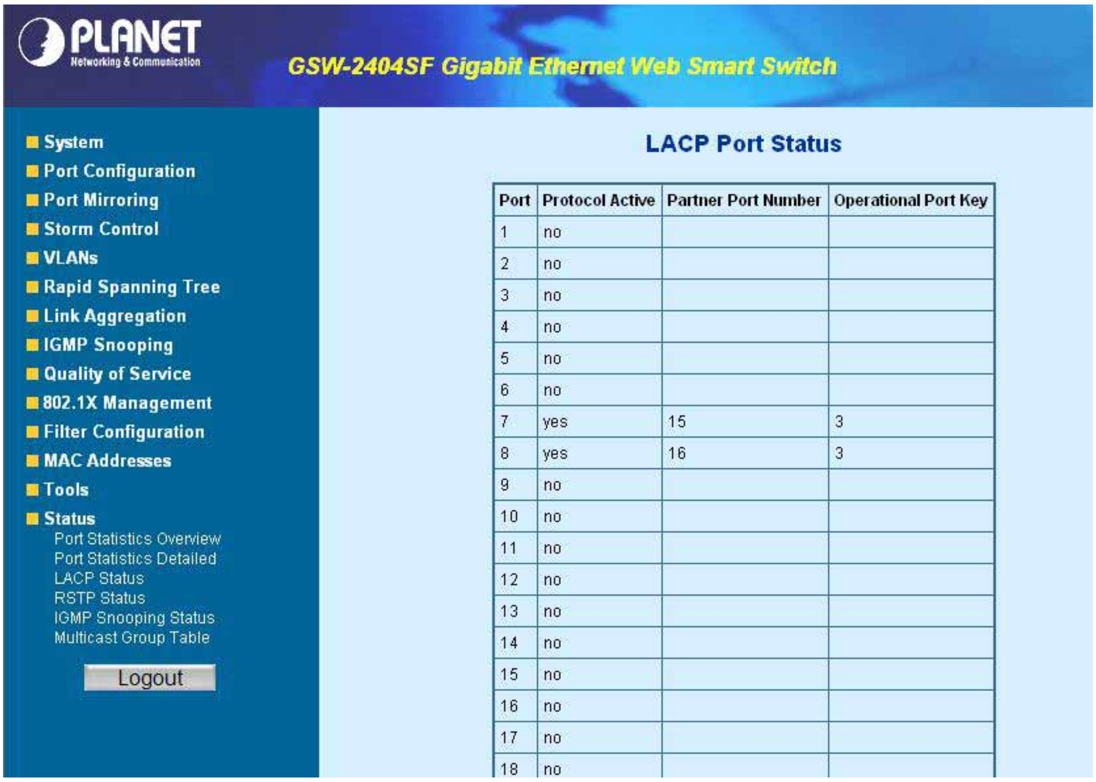
  ex. Port 7 and Port 8 as a LACP group-> Group 7;
  Port 23 and Port 24 as a LACP group-> Group 23

The Color and ID legend

🟥	Down	Port link down
🟥 0	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
🟨 0	Learning	Port Learning by RSTP
🟩	Forwarding	Port link up and forwarding frames
🟩 0	Forwarding	Port link up and forwarding by RSTP. Number is **Partner port number** if other switch has LACP enabled

■ LACP Port Status Table

The LACP Port Status Table lists the active LACP ports and the Partner Port number with the operational Port Key value. The screen in Figure 4-33 appears.



LACP Port Status

Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		
3	no		
4	no		
5	no		
6	no		
7	yes	15	3
8	yes	16	3
9	no		
10	no		
11	no		
12	no		
13	no		
14	no		
15	no		
16	no		
17	no		
18	no		

Figure-4-33 LACP Port Status

The page includes the following fields:

- **Port** Indicate port 1 to port 24.

- **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/ID of the linked partner switch**-** if other switch has LACP enabled.

  Ex. Row of Port 7with 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.

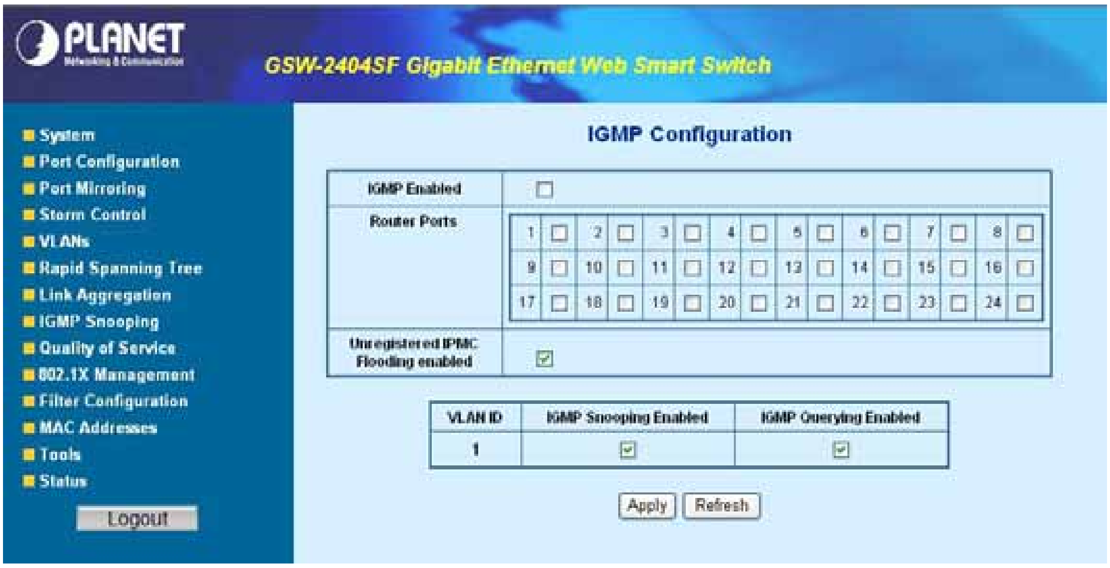
- **Operational Port Key** The current operational key value of the partner port. Within the same LACP group, the port key value should be the same with the other LACP active ports.

4.8 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.

4.8.1 IGMP Snooping Configuration

The IGMP Configuration page let the administrator to configure the parameters for IGMP Snooping, which is used to build forwarding lists for multicast traffic. The screen in Figure 4-34 appears.



IGMP Configuration

IGMP Enabled	□
Router Ports	1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24 □
Unregistered IPMC Flooding enabled	☑

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	☑	☑

Figure 4-34 IGMP Snooping Configuration and Status

The page includes the following fields:

- **IGMP Enable**
  Enables or disables IGMP global function on the device.
  Disabled is the default value.

- **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.
  Enabled is the default value.

- **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.

Enabled is the default value.

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

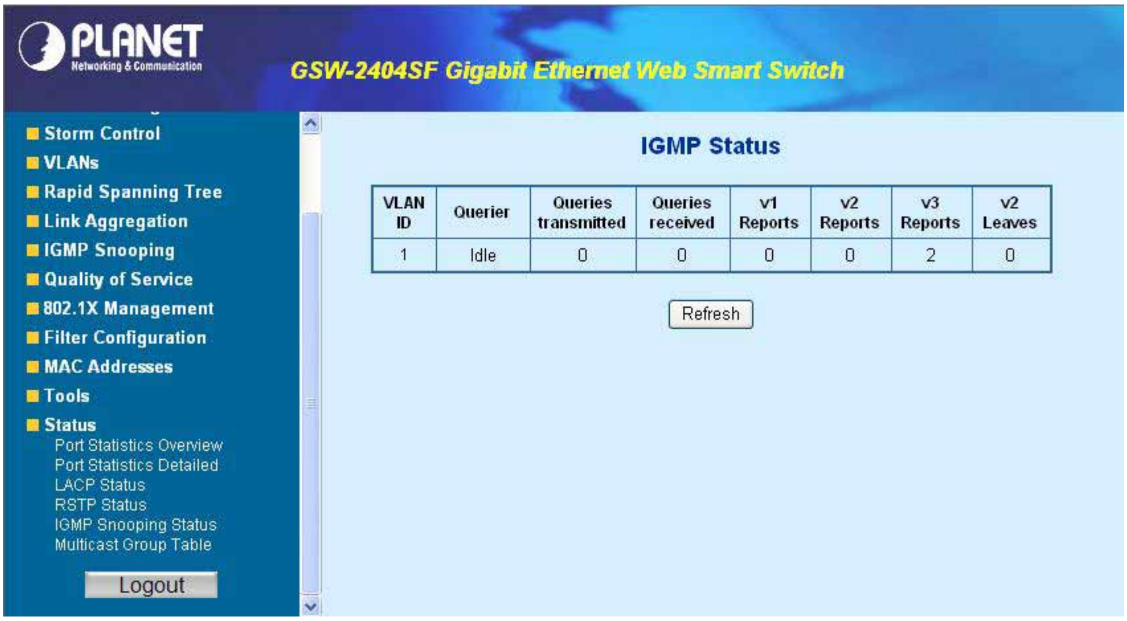
4.8.2 IGMP Snooping Status

The IGMP Snooping page display the current IGMP Status and the statistics of received Query / report packets.

To open **IGMP Status** screen perform the folling:

1. Click Status -> IGMP Snooping Status

2. The "IGMP Status" screen is displayed as in Figure 4-35.



IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Idle	0	0	0	0	2	0

Figure 4-35 IGMP Snooping Status

The page includes the following fields:

- **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.

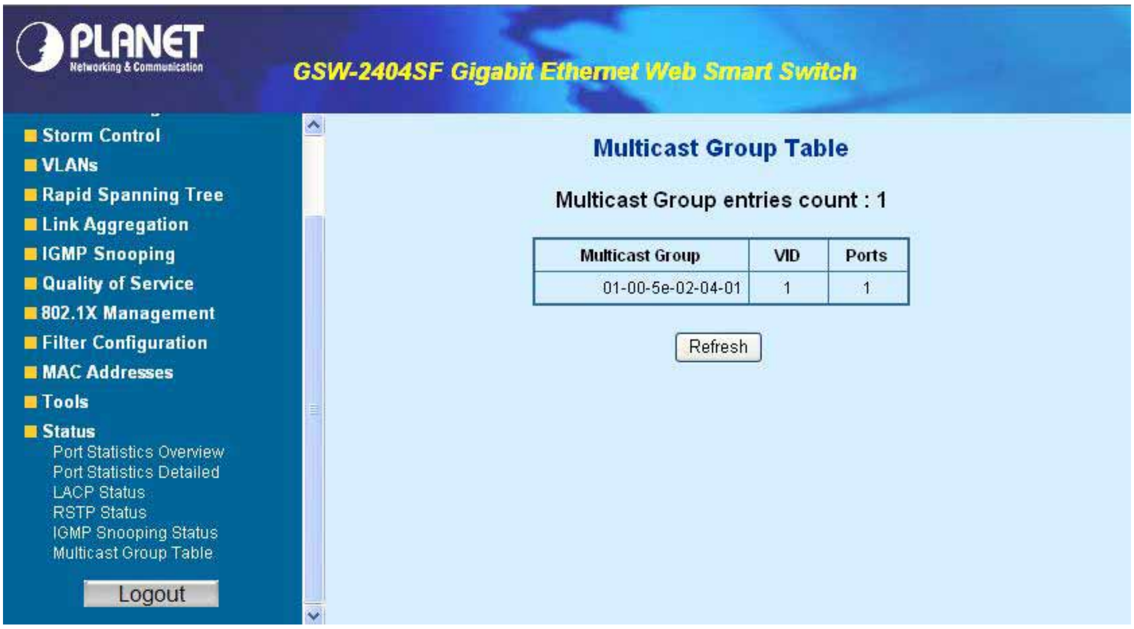
  (Packets with content type = **0x17** ; Leave a Group (version 2))

4.8.3 Multicast Group Table

The Multicast Group page 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.

To open **Multicast Group Tables** screen perform the folling:

1. Click Status -> Multicast Group Table
2. The Multicast Group Table screen is displayed as in Figure 4-36



Multicast Group Table

Multicast Group entries count : 1

Multicast Group	VID	Ports
01-00-5e-02-04-01	1	1

Figure 4-36 The Multicast Group Table screen

The page includes the following fields:

• **Multicast Group entries Count**	The total count of the current Multicast Group entries of the 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.

4.9 Quality of Service

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:

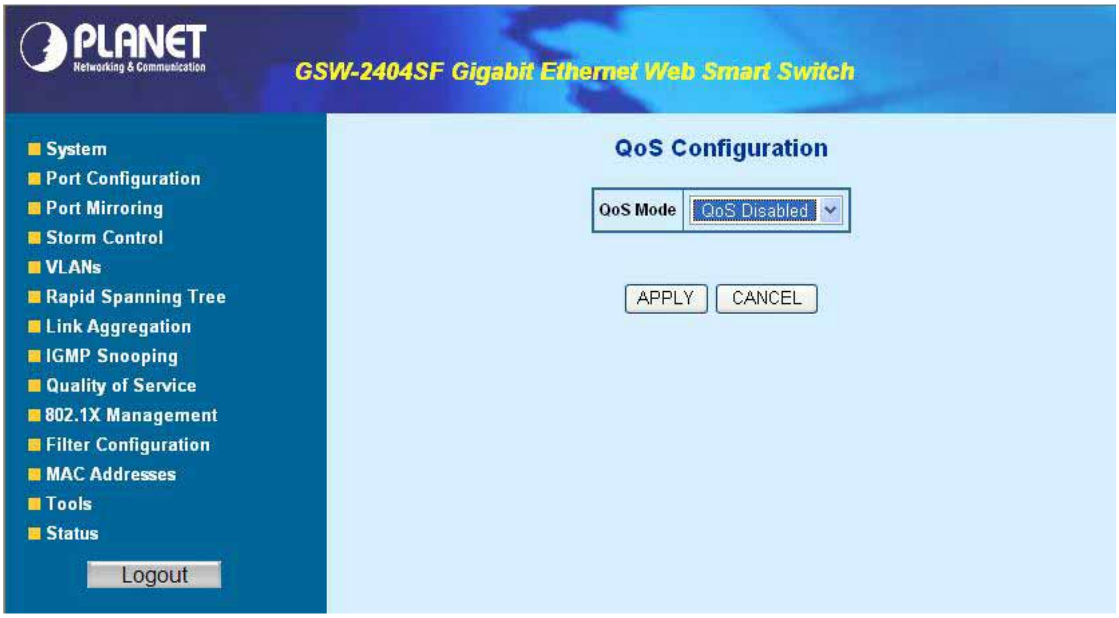
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video 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 current version of GSW-1602SF/2404SF support QoS **Strict** mode only. The strict mode is to specifies if traffic scheduling is based strictly on the queue priority.

The QoS Configuration page in Figure 4-37 appears.



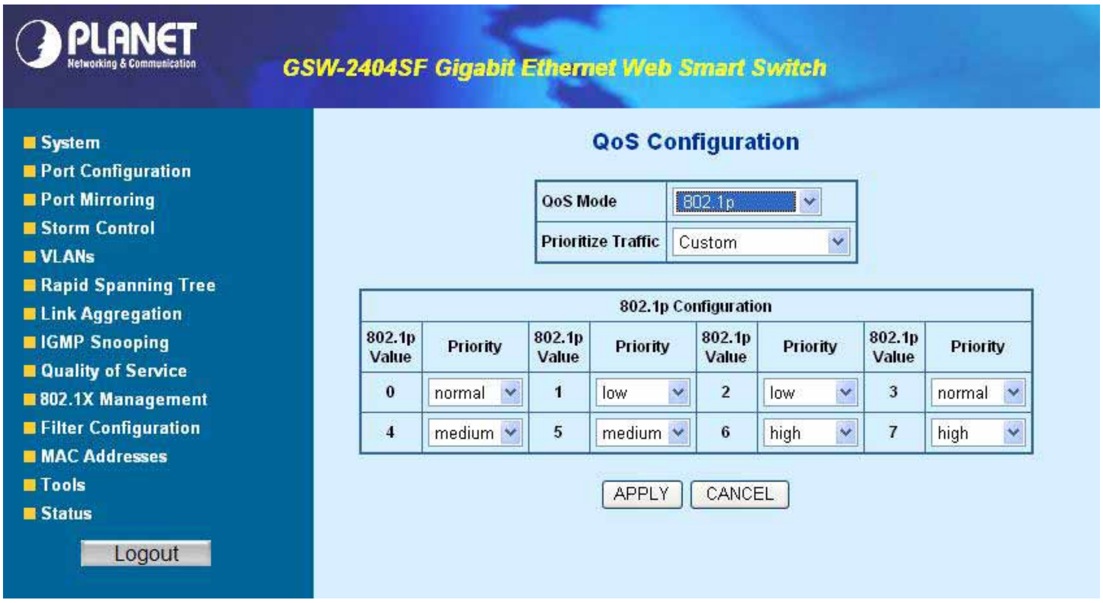
QoS Configuration

QoS Mode	QoS Disabled

Figure 4-37 QoS Configuration screen

4.9.1 802.1p QoS Mode

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. The IEEE 802.1p Priority specification uses 8 priority levels to classify data packets. The screen in Figure 4-38 and Figure 4-39 appears.



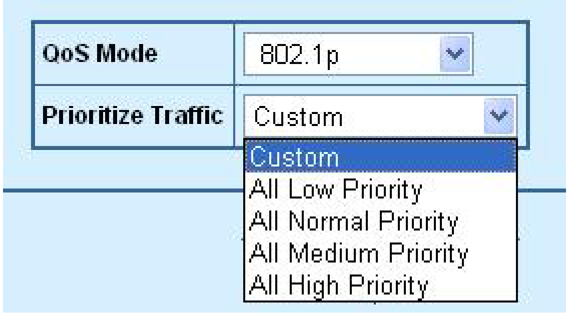
QoS Configuration

QoS Mode	802.1p
Prioritize Traffic	Custom

802.1p Configuration

802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	normal	1	low	2	low	3	normal
4	medium	5	medium	6	high	7	high

Figure 4-38 802.1p QoS Configuration screen



QoS Mode	802.1p
Prioritize Traffic	Custom

Figure 4-39 Prioritize Traffic screen

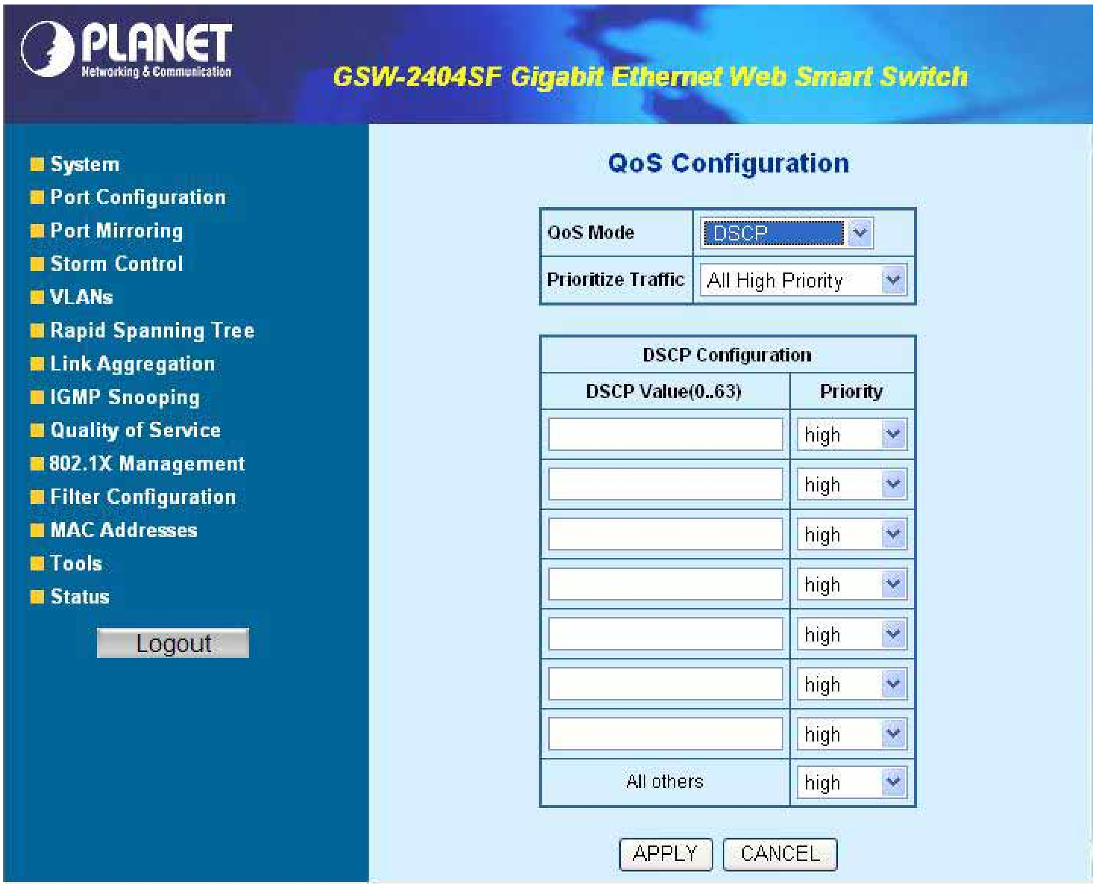
The page includes the following fields:

- **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**

4.9.2 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 4-40 shows.



QoS Configuration

QoS Mode	DSCP
Prioritize Traffic	All High Priority

DSCP Configuration

DSCP Value(0..63)	Priority
	high
	high
	high
	high
	high
	high
	high
All others	high

Figure 4-40 DSCP QoS Configuration screen

The page includes the following fields:

- **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**

4.10 802.1X Management

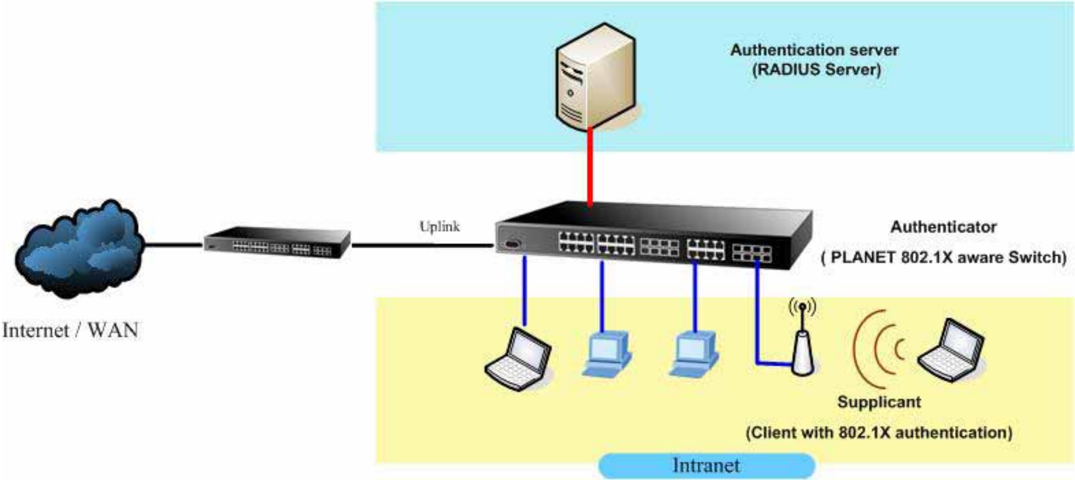
The PALENT GSW-1602SF/2404SF supports IEEE 802.1X Port-base network access control and RADIUS server authentication to enhance the host link more security. An 802.1X Infrastructure is composed of three major components: Authenticator, Authentication server, and Supplicant.

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 Switch.
2. Web-Smart Switch replies with an EAP Request ID message.
3. The client sends its Network Access Identifier (NAI) – its user name – to Web-Smart Switch in an EAP Respond message.
4. Web-Smart 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 Switch a RADIUS ACCEPT message.

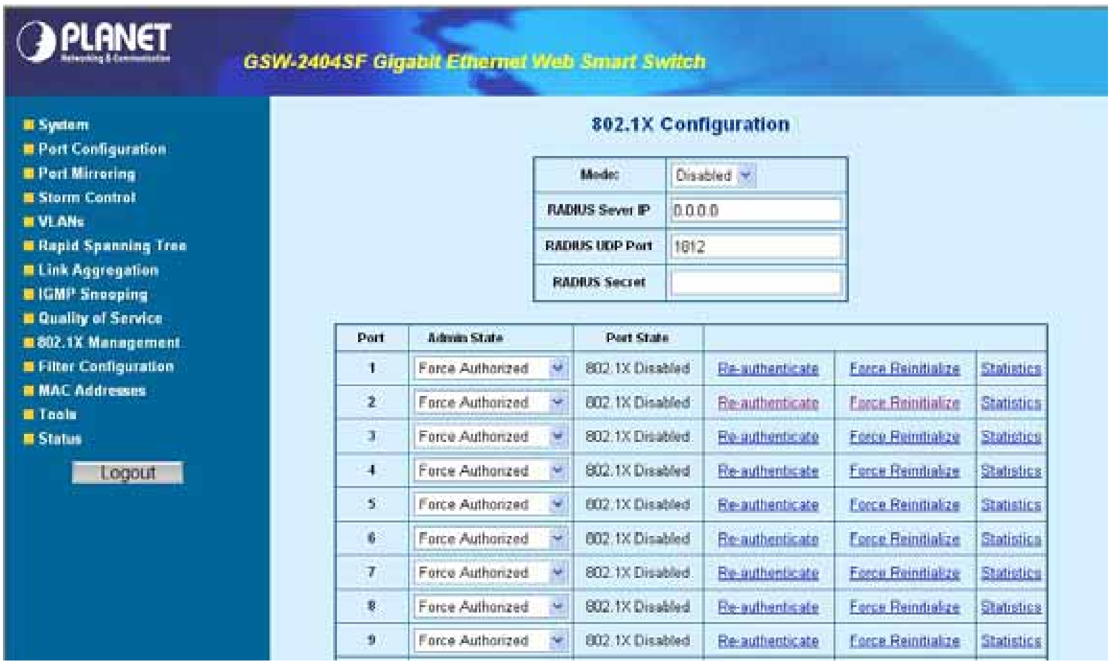
10. Web-Smart Switch sends the client an EAP Success message along with the broadcast key and key length.

This section is to control the access of the switch, includes the user access and management control. The 802.1X Management page contains links to the following topics:

- **RADIUS Server Configuration**
- **Port Access Control**

4.10.1 RADIUS Server Configuration

This page is to configure the RADIUS server connection features. The screen in Figure 4-41 and Figure 4-42 appears.

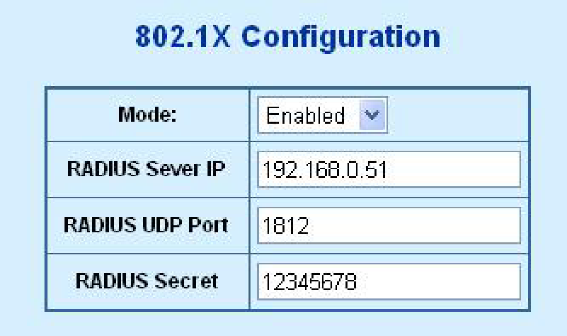


802.1X Configuration

Mode:	Disabled
RADIUS Sever IP	0.0.0.0
RADIUS UDP Port	1812
RADIUS Secret	

Port	Admin State	Port State			
1	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
2	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
3	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
4	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
5	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
6	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
7	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
8	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
9	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics

Figure 4-41 802.1X Configuration screen



802.1X Configuration

Mode:	Enabled
RADIUS Sever IP	192.168.0.51
RADIUS UDP Port	1812
RADIUS Secret	12345678

Figure 4-42 RADIUS Server configuration table screen

The RADIUS Server configuration table includes the following fields:

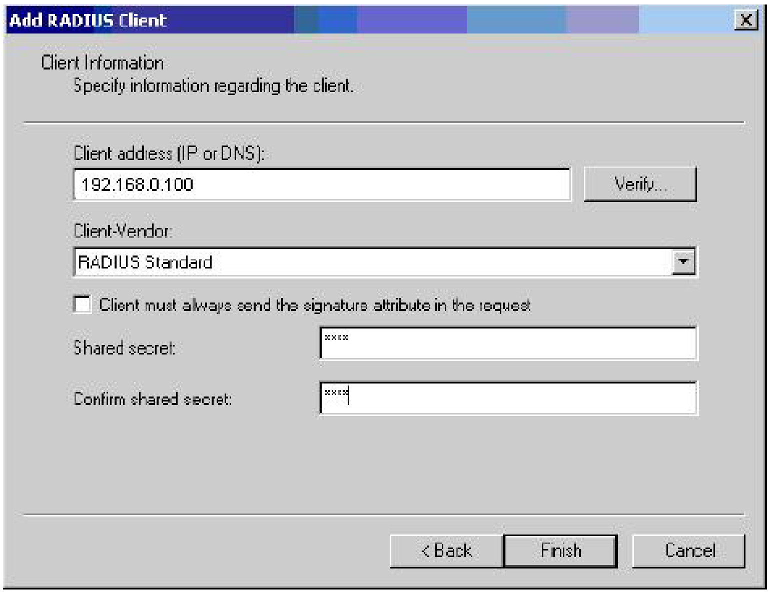
- **Mode** To Enable/Disable the port access control administrative mode

  This selector lists the two options for administrative mode: enable and disable. The default value 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.

Setup the RADIUS server and assign the client IP address to the Web-Smart switch. In this case, field in the default IP Address of the Web-Smart 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.



Client address (IP or DNS): 192.168.0.100

Client-Vendor: RADIUS Standard

□ Client must always send the signature attribute in the request

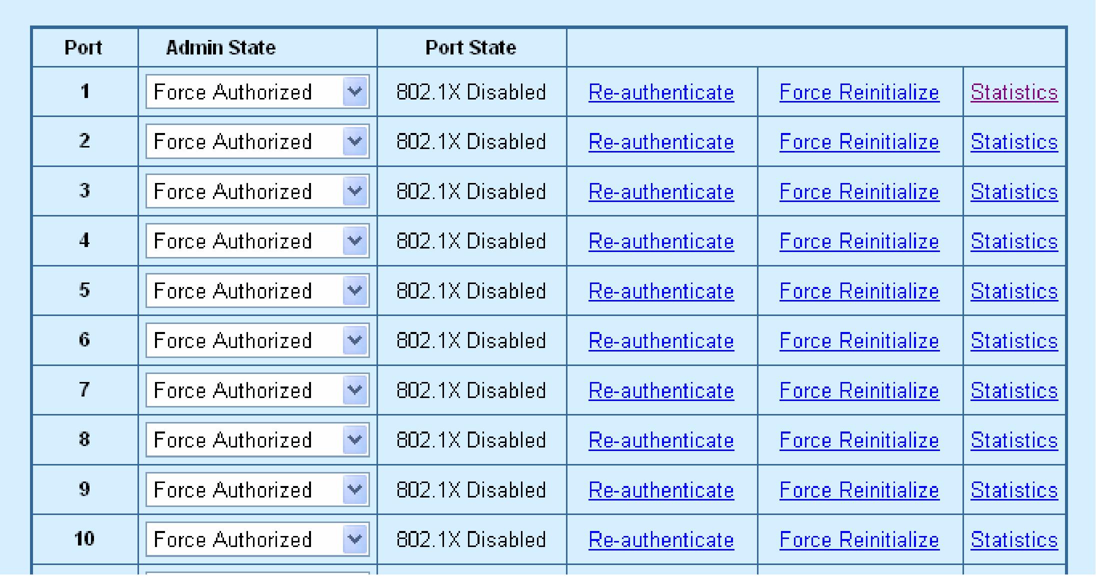
Shared secret: ****

Confirm shared secret: ****

Figure 4-43 RADIUS Server configuration

4.10.2 Port Access Control

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 4-44 and Figure 4-45 appears.



Port	Admin State	Port State			
1	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
2	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
3	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
4	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
5	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
6	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
7	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
8	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
9	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
10	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics

Figure 4-44 Per Port network access control configure table

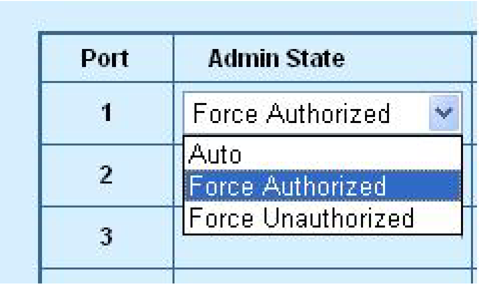


Figure 4-45 802.1X Network access control mode selection

The Network Access Control port configuration table includes the following fields:

- **Port** 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.

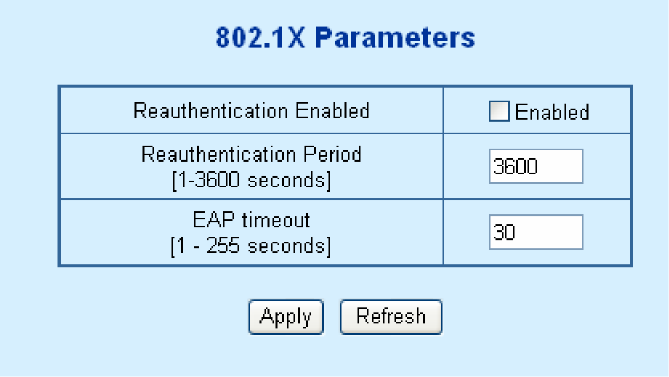
- **Force Reinitialize** This button begins the re-initialization sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the 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 the all ports.

- **Force Reinitialize All** This button begins the re-initialization sequence on all ports.

At the bottom of this page, click “Parameter” button will redirect to the “802.1X parameter” configure page. The screen in Figure 4-46 appears.



802.1X Parameters

Reauthentication Enabled	□ Enabled
Reauthentication Period [1-3600 seconds]	3600
EAP timeout [1 - 255 seconds]	30

Figure 4-46 802.1X Parameter configuration screen

The 802.1X Parameters table includes the following fields:

- **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**.

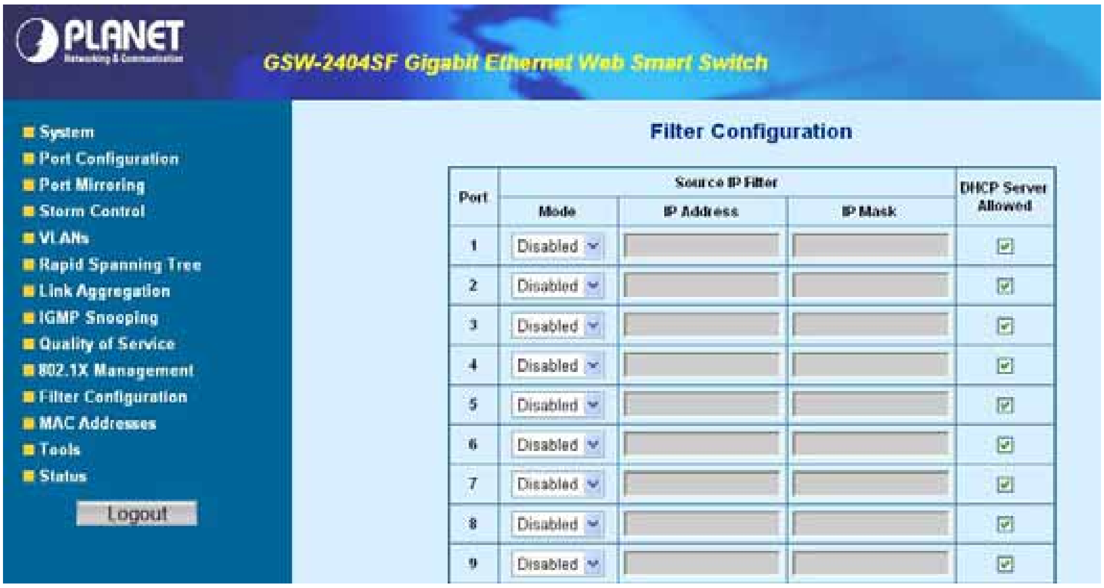
- **EAP Timeout [1-255 seconds]**

  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**.

4.11 Filter Configuration

The GSW-1602SF/GSW2404SF support 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 4-47 appears.



Filter Configuration

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled			☑
2	Disabled			☑
3	Disabled			☑
4	Disabled			☑
5	Disabled			☑
6	Disabled			☑
7	Disabled			☑
8	Disabled			☑
9	Disabled			☑

Figure 4-47 Filter Configuration screen

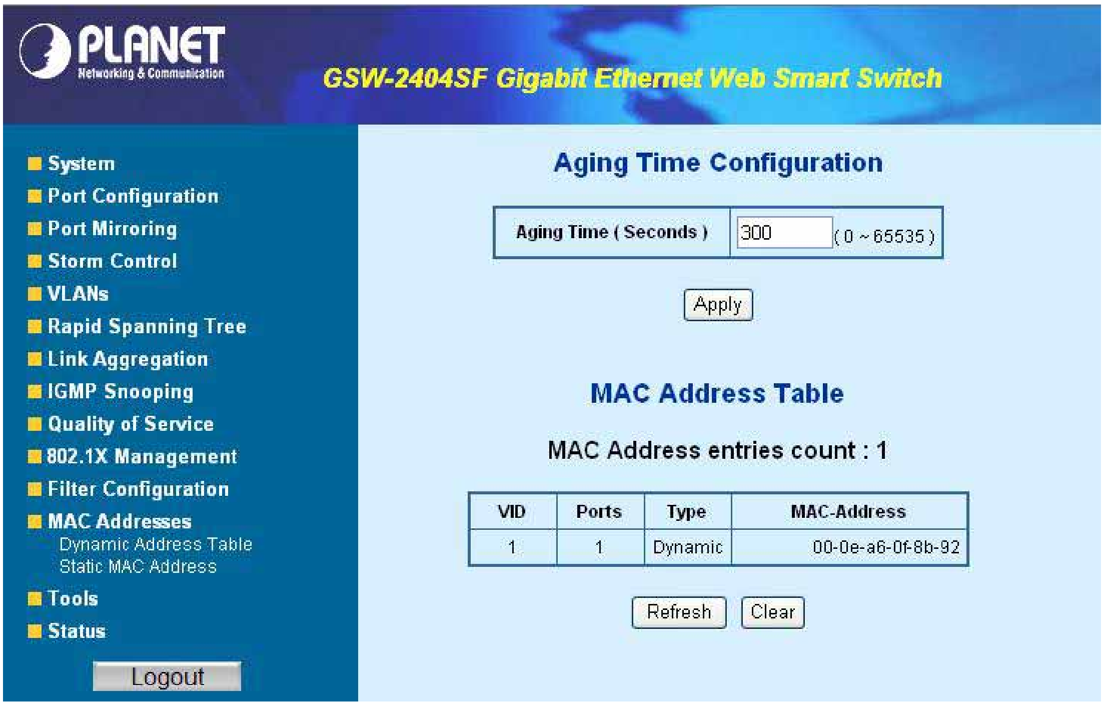
The Filter Configuration page includes the following fields:

- **Port** Indicate port 1 to port 24 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.

4.12 MAC Addresses

4.12.1 Dynamic Address Table

Use this page to set the Address Ageing Timeout for the MAC Address database, and to 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 Figure 4-48 appears.



Aging Time Configuration

Aging Time (Seconds) 300 (0 ~ 65535)

MAC Address Table

MAC Address entries count : 1

VID	Ports	Type	MAC-Address
1	1	Dynamic	00-0e-a6-0f-8b-92

Figure 4-48 Dynamic Address Table

- **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.

- **MAC Address Table**

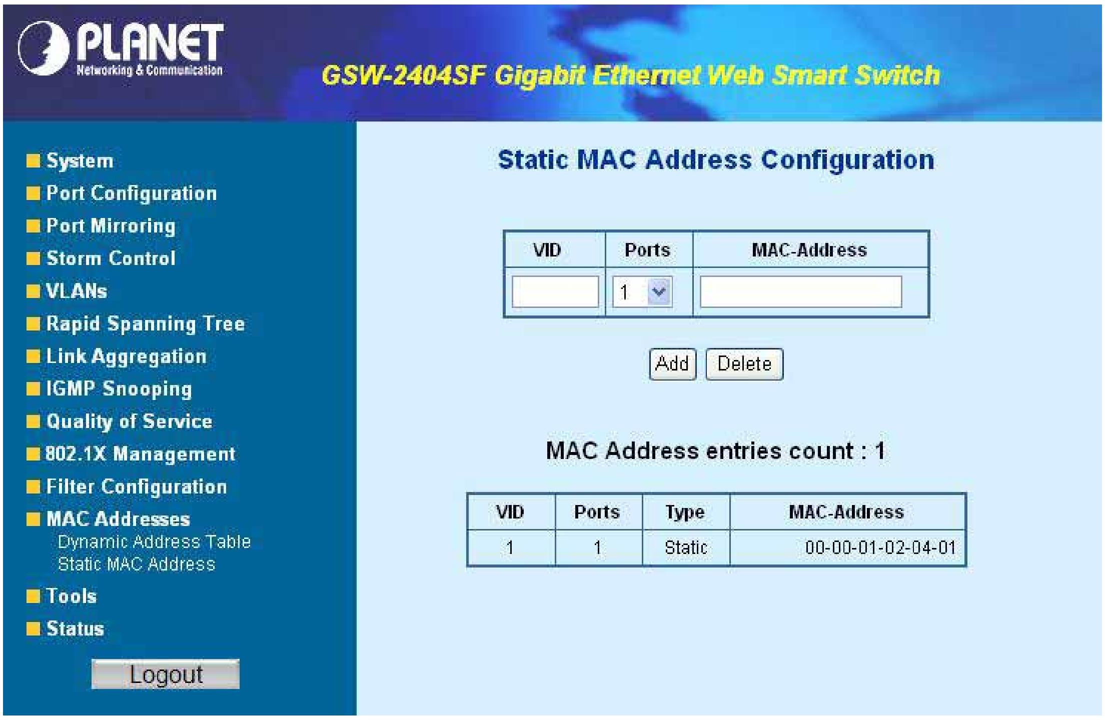
The MAC Address Table includes the following fields:

- **MAC Address entries count**
- **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.

4.12.2 Static MAC Address

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 Figure 4-49 appears.



Static MAC Address Configuration

VID	Ports	MAC-Address
	1	

MAC Address entries count : 1

VID	Ports	Type	MAC-Address
1	1	Static	00-00-01-02-04-01

Figure-4-49 Static MAC Address Configuration

The configable filelds includes the following items:

- **VID** The VLAN ID attached to the MAC Address
- **Ports** Specifies the port numbers for which the table is queried.
- **MAC-Address** Input the MAC address entry be manualed bind to the specify port.

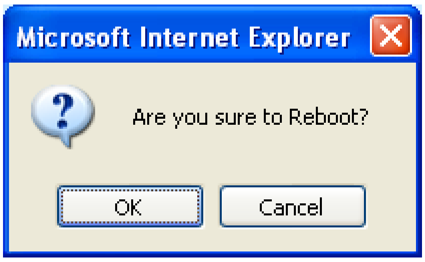
The MAC Address Table includes the following fields:

- **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.

4.13 Tools

4.13.1 Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button be pressed, user have to re-login the WEB interface about 20 seconds later.

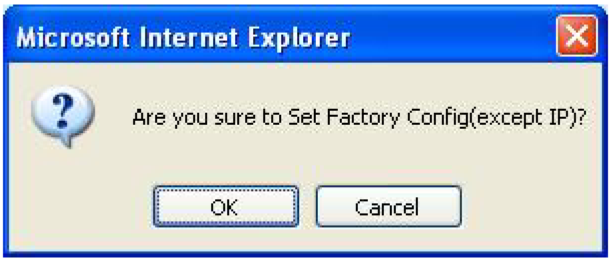


Microsoft Internet Explorer

Are you sure to Reboot?

4.13.2 Factory Reset

The Factory Reset button can reset the GSW-1602SF/2404SF back to the factory default mode. Be aware that the entire configuration will be reset; expect the IP address of the GSW-1602SF/2404SF. Once the Factory Reset item be pressed, the screen in Figure 4-50 appears.



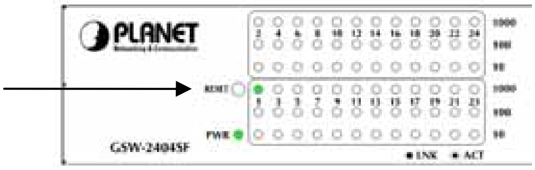
Microsoft Internet Explorer

Are you sure to Set Factory Config(except IP)?

Figure 4-50 Factory Reset screen

✍ *Note:* To reset the IP address to the default IP Address "192.168.0.100". Press the hardware reset button at the front panel about 5 seconds. After the device be rebooted. You can login the management WEB interface within the same subnet of 192.168.0.xx.

Hardware Reset button

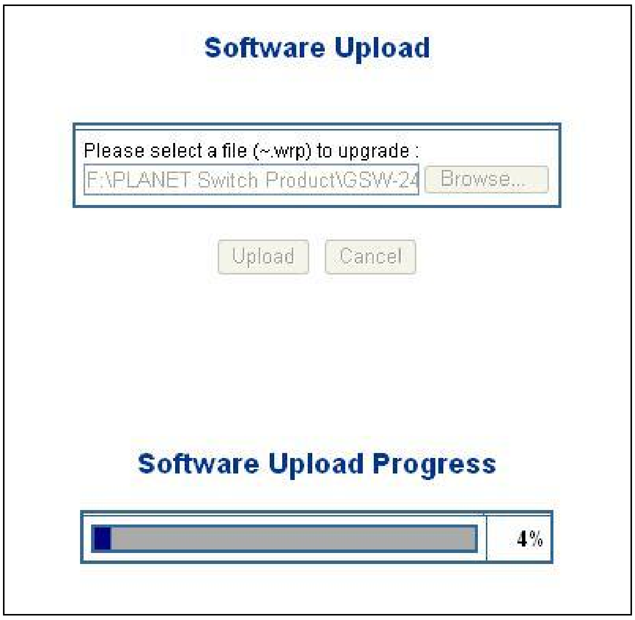


4.13.3 Firmware Upgrade

The **Firmware Upgrade** page contains fields for downloading system image files from the Local File browser to the device.

To open **Firmware Upgrade** screen perform the folling:

1. Click **Tools** -> **Firmware Upgrade**
2. The Firmware Upgrade screen is displayed as in Figure 4-51.
3. Click the "**Browse**" button of the main page, the system would pop up the file selection menu to choose firmware.
4. Select on the firmware then click "**Upload**", the **Software Upload Progress** would show the file upload status.



Software Upload

Please select a file (~.wrp) to upgrade :

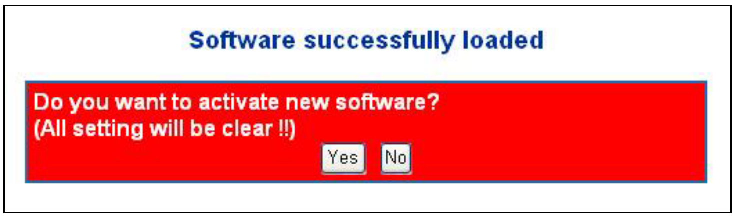
F:\PLANET Switch Product\GSW-24

Software Upload Progress

4%

Figure 4-51 Firmware Upgrade screen

5. 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.



Software successfully loaded

Do you want to activate new software?
(All setting will be clear !!)

Figure 4-52 Software successfully loaded notice screen

✍ ***Note:*** Do not power off the switch until the update progress is complete.

✍ ***Note:*** Do not quit the Firmware Upgrade page without press the "Yes" button - after the image be loaded. Or the system won't apply the new firmware. User have to repeat the firmware upgrade processes again.

4.13.4 Configuration Upload

This function allows backup and reload the current configuration of GSW-1602SF /2404SF to the local management station. The screen in Figure 4-53 appears.

- **Configuration Upload:** Upload the existed configuration file to the GSW-1602SF/2404SF. The configuration file had been saved at the local machine already.
- **Configuration Download:** Download the current configuration file of the switch to the local machine.

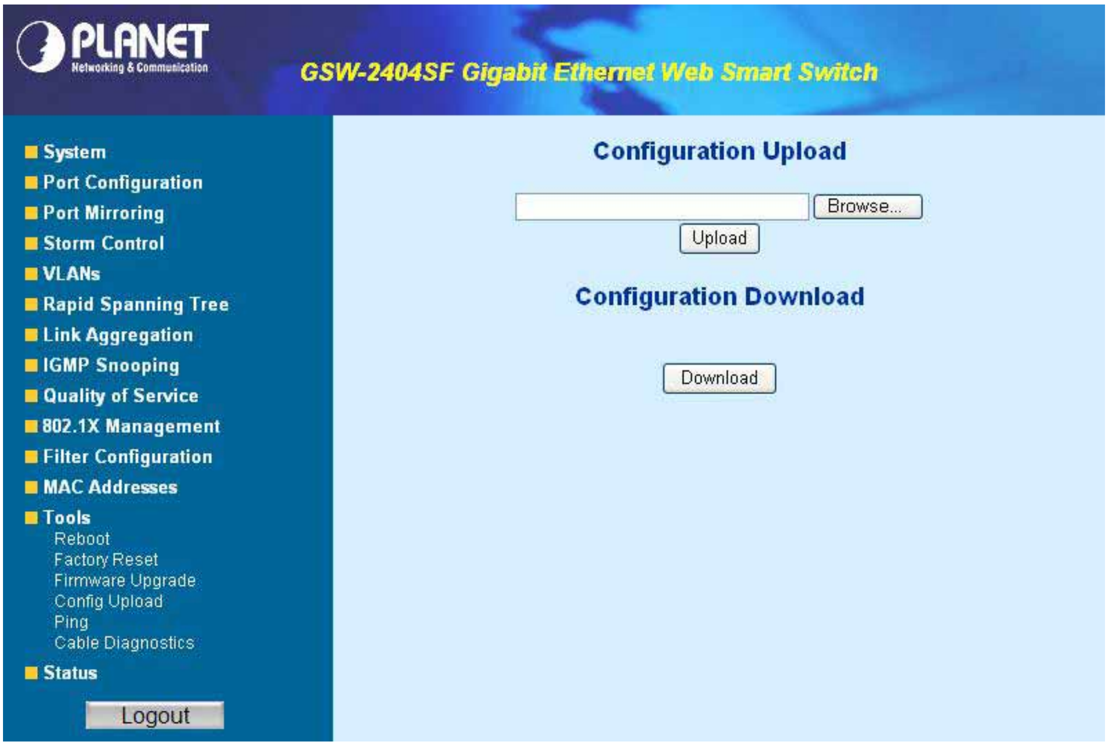
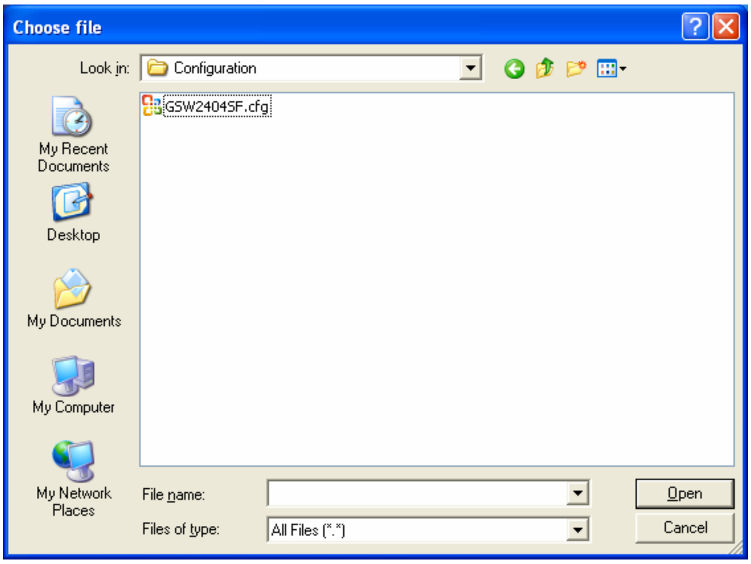


Figure 4-53 Configuration Upload/Download screen

- **Configuration Upload**

1. Click the "**Browse**" button of the main page, the system would pop up the file selection menu to choose saved configuration.



Look in: Configuration

File name:

Files of type: All Files (*.*)

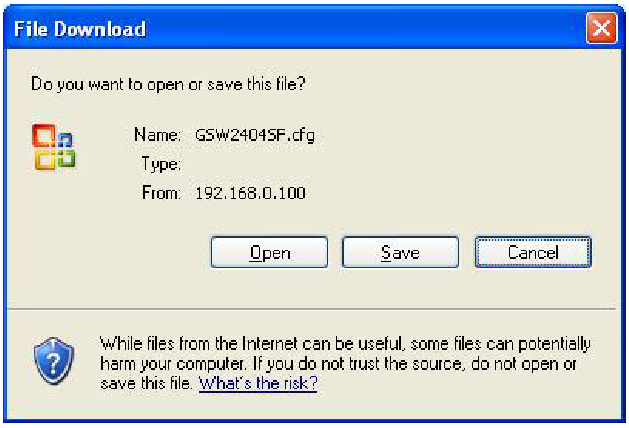
Figure 4-54 Windows file selection menu popup

2. Select on the configuration file then click “**Upload**”, the bottom of the browser shows the upload status.

3. After down, the main screen appears “**Transfer Completed**”.

- **Configuration Download**

1. Press the **“Download”** button to save the current configuration in manager workstation. The following screens in Figure 4-55 and 4-56 appear



File Download

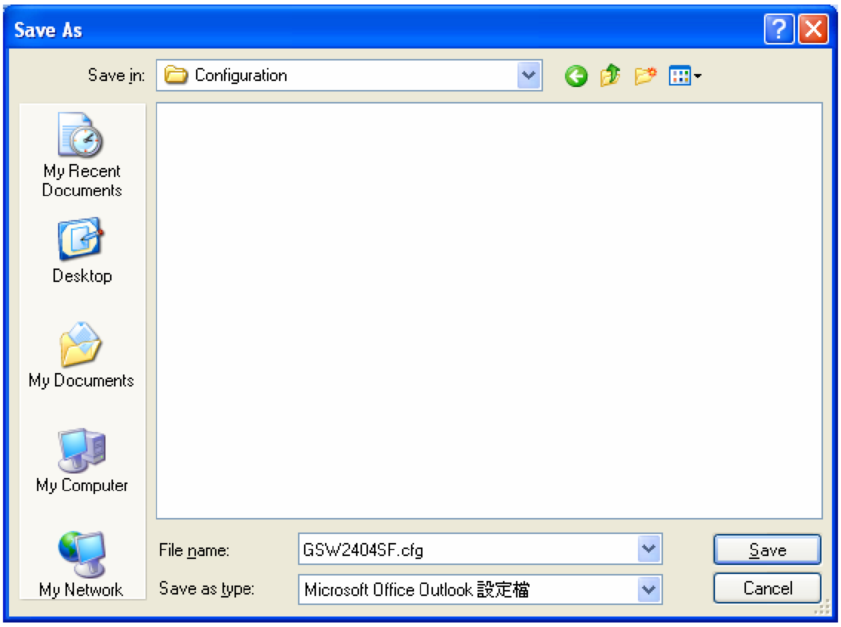
Do you want to open or save this file?

Name: GSW2404SF.cfg
Type:
From: 192.168.0.100

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 4-55 File Download screen

2. Chose the file save path in management workstation.



Save As

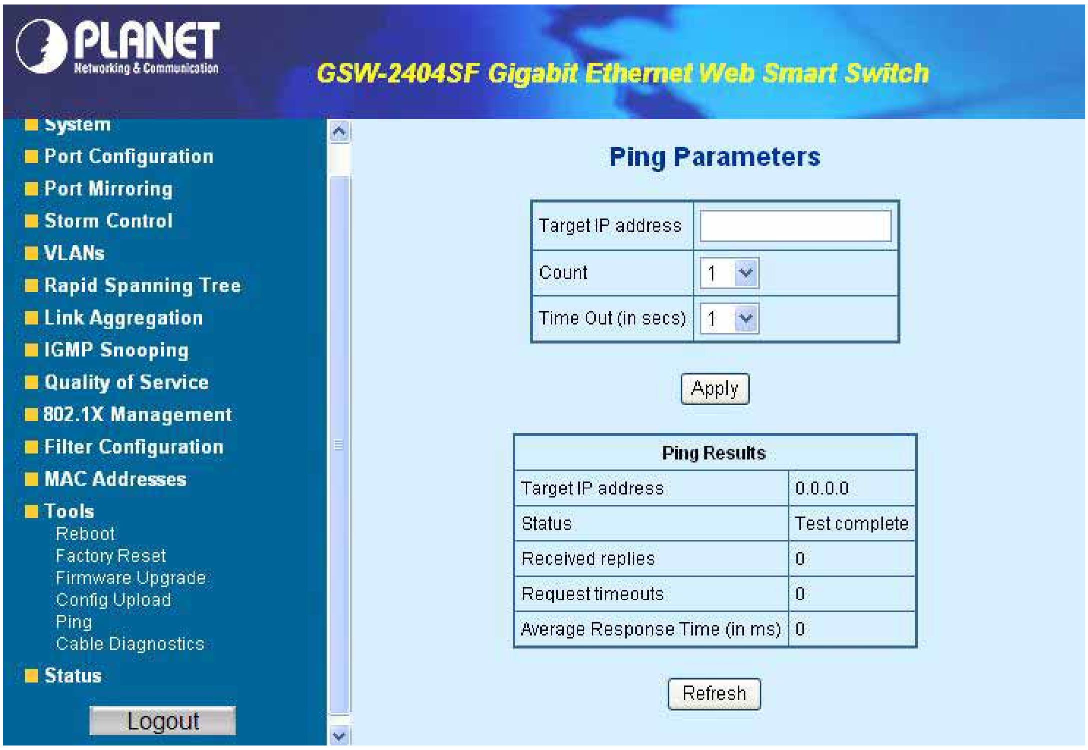
Save in: Configuration

File name: GSW2404SF.cfg
Save as type: Microsoft Office Outlook 設定檔

Figure 4-56 File save screen

4.13.5 Ping

Use this screen to tell the switch to send a Ping request to a specified IP address. You can use this to check whether the 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.



Ping Parameters

Target IP address	
Count	1
Time Out (in secs)	1

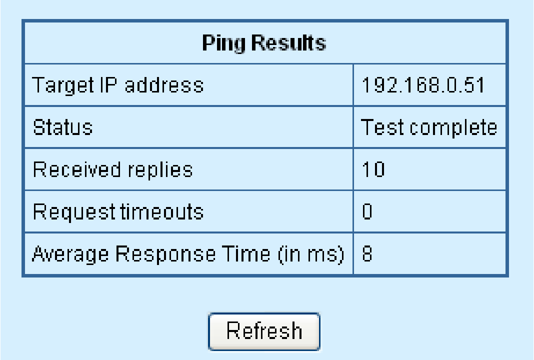
Ping Results	
Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Figure 4-57 Ping function screen

The Ping Parameters includes the following fields:

- **Target IP Address** Enter the IP address of the station you want the 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.

After field the parameter and press “**Apply**” to execute the Ping function. The Ping result shows at the next table. As the Figure 4-58 screen appears.



Ping Results	
Target IP address	192.168.0.51
Status	Test complete
Received replies	10
Request timeouts	0
Average Response Time (in ms)	8

Figure 4-58 Ping Result screen

✍ **Note:** Be sure the target IP Address is within the same network subnet of the switch, or you had setup the correct gateway IP address.

4.13.6 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:

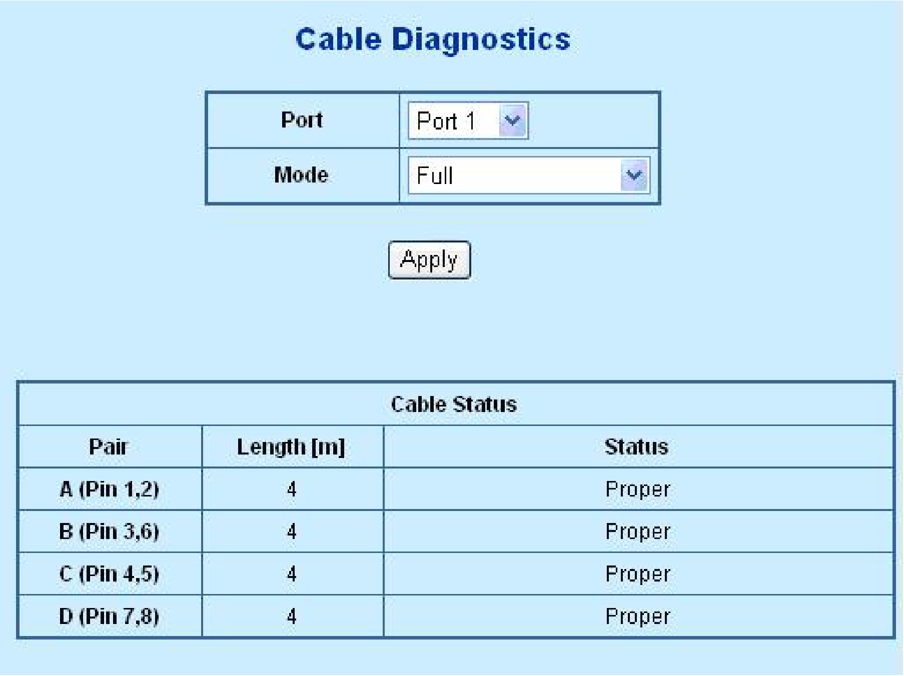
■ If the link is established on the twisted-pair interface in 1000BASE-T mode, the Cable Diagnostics can run without disruption of the link or of any data transfer.

■ 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 4-59 appears.



Cable Diagnostics

Port	Port 1
Mode	Full

Cable Status		
Pair	Length [m]	Status
A (Pin 1,2)	4	Proper
B (Pin 3,6)	4	Proper
C (Pin 4,5)	4	Proper
D (Pin 7,8)	4	Proper

Figure 4-59 Cable Diagnostics

The Cable Diagnostics includes the following fields:

• **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

The Cable status includes the following items:

- **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 a 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.

✍ **Note:** 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 link down after the cable diagnostics.

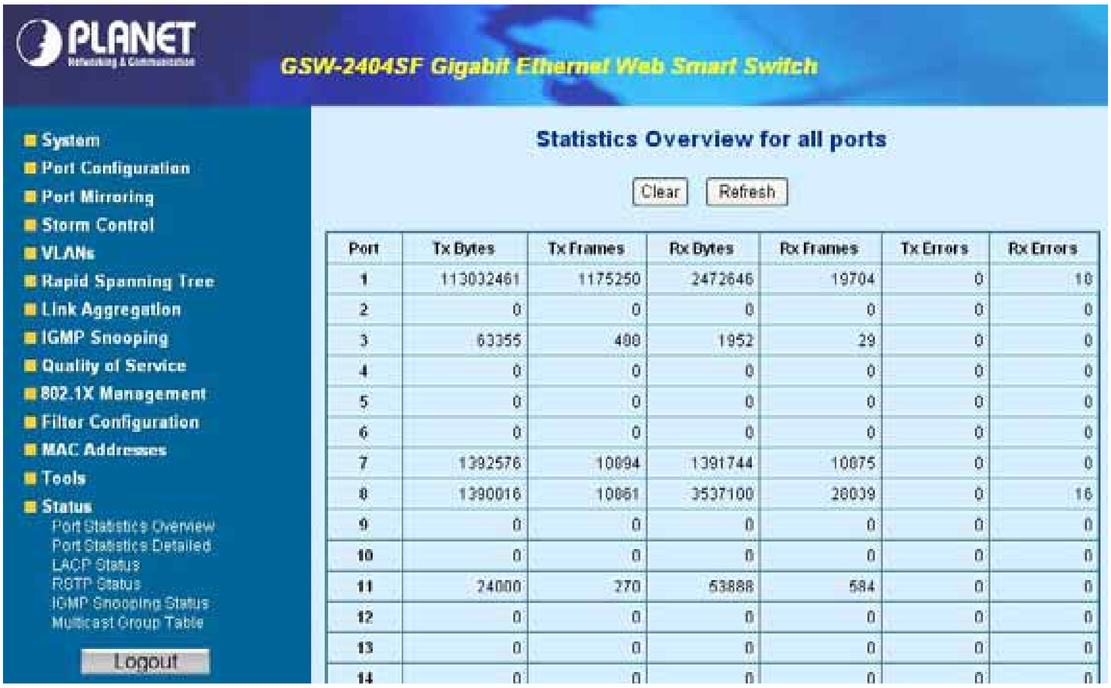
4.14 Status

Click on the ***"Status"*** to present the Switch status on this screen, it displays the following status:

- **Port Statistics Overview**
- **Port Statistics Detail**
- **LACP Status**
- **RSTP Status**
- **IGMP Snooping Status**
- **Multicast Group Table**

4.14.1 Port Statistics Overview

The Port Statistic Overview page displays the status of packet count from each port. The Port statistics overview screen in Figure 4-60 appears.



Statistics Overview for all ports

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	113032461	1175250	2472646	19704	0	10
2	0	0	0	0	0	0
3	63355	400	1952	29	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	1392576	10094	1391744	10075	0	0
8	1390016	10061	3537100	28039	0	16
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	24000	270	53888	584	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0

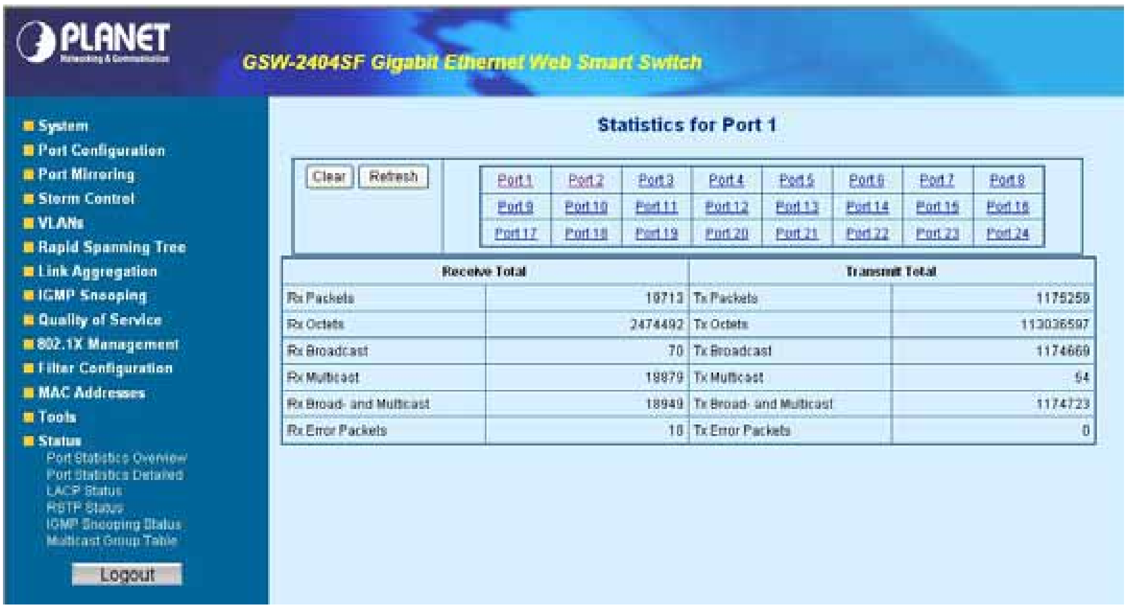
Figure 4-60 Port Statistics Overview screen

The page includes the following fields:

- **Port** The Port number
- **TX Bytes** Number of octets of data (including those in bad packets) transmitted on the port. This object can be used as a reasonable estimate of Ethernet utilization
- **TX Frames** Number of packets transmitted on the port. Include the Unicast , broadcast and multicast packets.
- **RX Bytes** Number of octets of data (including those in bad packets) received on the port. This object can be used as a reasonable estimate of Ethernet utilization
- **RX Frames** Number of packets received on the port. Include the Unicast , broadcast and multicast packets.
- **TX Errors** The number of error packets transmit from the port.
- **RX Errors** The number of error packets received on the port.

4.14.2 Port Statistics Detail

The Port Statistic detail page displays the status of packet count from each port. Press the port ID for detail packet information on each port. The screen in Figure 4-61 appears.



Statistics for Port 1

Receive Total		Transmit Total	
Rx Packets	19713	Tx Packets	1175259
Rx Octets	2474492	Tx Octets	113036597
Rx Broadcast	70	Tx Broadcast	1174669
Rx Multicast	18879	Tx Multicast	54
Rx Broad- and Multicast	18949	Tx Broad- and Multicast	1174723
Rx Error Packets	10	Tx Error Packets	0

Figure 4-61 Per port detail Statistics screen

The page includes the following fields:

- **Port ID** The Port number. Press the port ID for detail packet information on the selected port.
- **RX Packets** Number of total packets received on the selected port. Include the Unicast , broadcast and multicast packets.
- **RX Octets** Number of total octets of data (including those in bad packets) received on the selected port.
- **RX Broadcast** Number of **Broadcast** packets received on the selected port.
- **RX Multicast** Number of **Multicast** packets received on the selected port.
- **RX Broad and Multicast** Subtotal number of **Broadcast** and **Multicast** packets received on the selected port.
- **RX Errors Packets** The number of **error** packets received on the selected port.
- **TX Packets** Number of total packets transmitted from the selected port. Include the Unicast , broadcast and multicast packets.
- **TX Octets** Number of total octets of data (including those in bad packets) transmitted from the selected port.
- **TX Broadcast** Number of **Broadcast** packets transmitted from the selected port.
- **TX Multicast** Number of **Multicast** packets transmitted from the selected port.
- **TX Broad and Multicast** Subtotal number of **Broadcast** and **Multicast** packets transmitted from the selected port.

- **TX Errors Packets** The number of **error** packets transmitted from the selected port.

4.14.3 LACP Status

The LACP Status page display the current LACP aggregation Groups and LACP Port status.

Please refer to Chapter 4.7.3 at page-39 for more detail.

4.14.4 RSTP Status

The RSTP Status page display the current STP bridge , roor bridge and per port stp status.
Please refer to Chapter 4.6.3 at page-33 for more detail.

4.14.5 IGMP Snooping Status

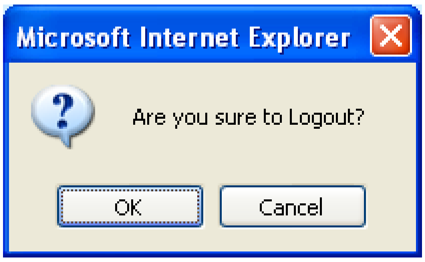
The IGMP Snooping page display the current IGMP Status and the statistics of received Query / report packets.
Please refer to Chapter 4.8.2 at page-43 for more detail.

4.14.6 Multicast Group Status

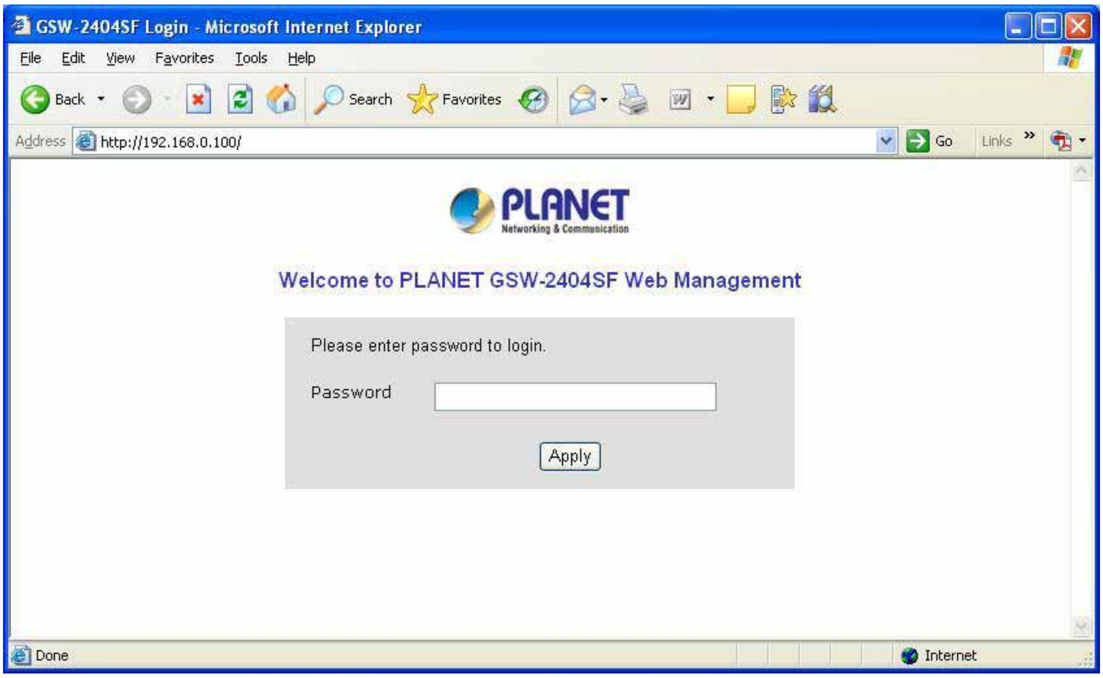
The Multicast Group page displays the ports attached to the Multicast service group in the Ports tables. The Port a tables also reflect the manner in which the port joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. The Bridge Multicast Group page permits new Multicast service groups to be created. The Bridge Multicast Group page also assigns ports to a specific Multicast service address group.
Please refer to Chapter 4.8.3 at page-44 for more detail

Logout

Press this function, the web interface will go back to login screen. The screen in Figure 4-62 appears.



Are you sure to Logout?


GSW-2404SF Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
PLANET
Networking & Communication
Apply
Done
Internet

http://192.168.0.100/

Welcome to PLANET GSW-2404SF Web Management

Please enter password to login.

Password

Figure 4-62 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. Thereby 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

<table>
<tr><td>Type</td><td>Response Time</td><td>Checksum</td></tr>
<tr><td colspan="3">Group Address (all zeros if this is a query)</td></tr>
</table>

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).

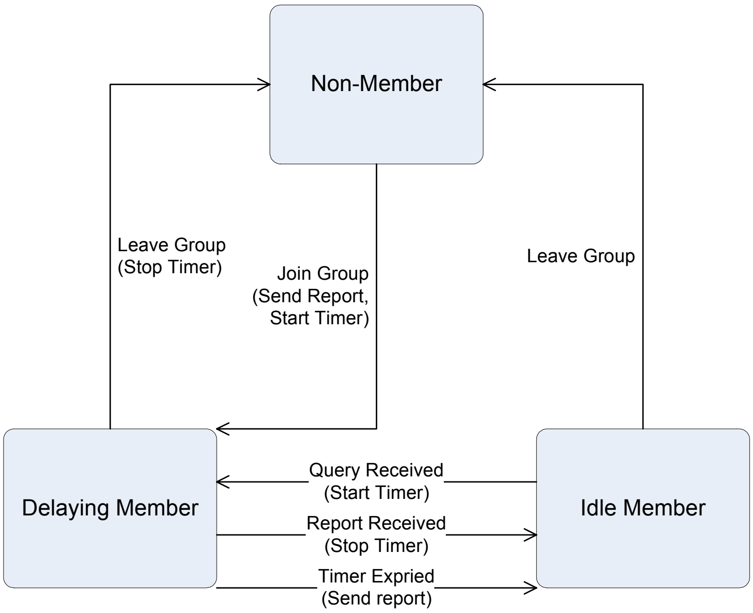
A host will send a **"leave"** report when it wants to leave a group (for version 2).

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

7. 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.

How to deal forgotten password situation of switch?

Solution:

1. Please contact Planet switch support team and the mail address is **support_switch@planet.com.tw**

APPENDIX A

A.1 Switch's RJ-45 Pin Assignments

1000Mbps, 1000Base T

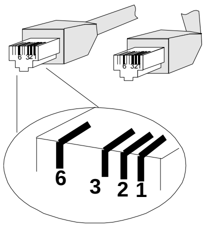
Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

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.

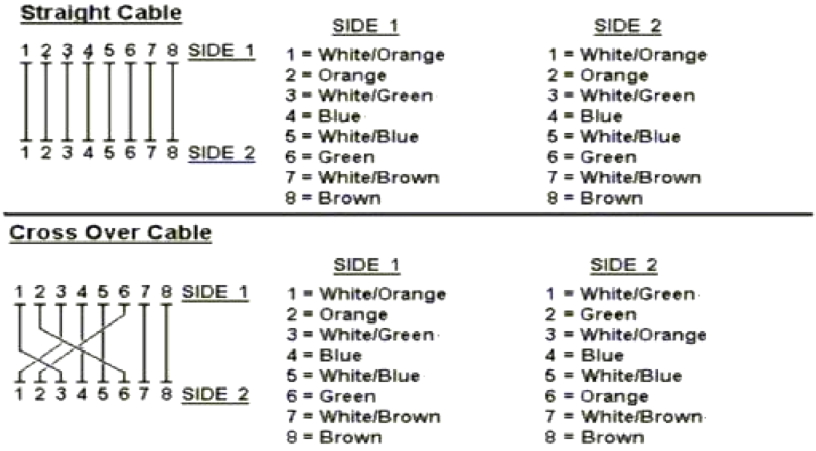
A.2 10/100Mbps, 10/100Base-TX

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:



Straight Cable

SIDE 1	SIDE 2
1 = White/Orange	1 = White/Orange
2 = Orange	2 = Orange
3 = White/Green	3 = White/Green
4 = Blue	4 = Blue
5 = White/Blue	5 = White/Blue
6 = Green	6 = Green
7 = White/Brown	7 = White/Brown
8 = Brown	8 = Brown

Cross Over Cable

SIDE 1	SIDE 2
1 = White/Orange	1 = White/Green
2 = Orange	2 = Green
3 = White/Green	3 = White/Orange
4 = Blue	4 = Blue
5 = White/Blue	5 = White/Blue
6 = Green	6 = Orange
7 = White/Brown	7 = White/Brown
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-A82070-000