User's Manual

Gigabit Ethernet L2 Web Smart Switch with 10GbE Uplink

► GS-2240-24T4X/GS-2240-48T4X

www.PLANET.com.tw

Trademarks

Disclaimer

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

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

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

FCC Warning

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

CE Mark Warning

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

Energy Saving Note of the Device

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

WEEE Warning

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

Revision

PLANET GS-2240 Series User's Manual

Model: GS-2240 Series

Revision: 1.0 (Jan, 2016)

Part No: EM-GS-2240-series _v1.0

TABLE OF CONTENTS

1. INTRODUCTION

Thank you for purchasing PLANET GS-2240 Managed Switch series, which comes with multiple Gigabit Ethernet copper and SFP/SFP+ fiber optic connectibility and robust layer 2. The description of this model is shown below:

Model Name	Gigabit RJ45 Ports	SFP/SFP+ Slots	RJ45 Console Port
GS-2240-24T4X	24	4	1
GS-2240-48T4X	48	4	1

"**Managed Switch**" is used as an alternative name in this user's manual.

1.1 Packet Contents

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

- **The Managed Switch**
- **Quick Installation Guide**
- **RJ45 to RS232 Cable**
- **Rubber Feet**
- **Two Rack-mounting Brackets with Attachment Screws**
- **Power Cord**
- **SFP Dust-proof Caps**

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 again to repack the product in case there is a need to return it to us for repair.

1.2 Product Description

High-Density, Resilient Deployment Switch Solution for Gigabit Networking of Enterprise, Campus and Data Center

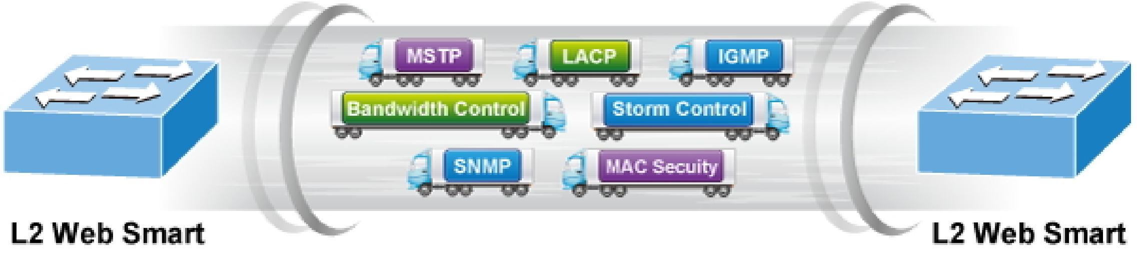
For the growing Gigabit network and IoT (Internet of Things) demand, PLANET has launched a new-generation **Web Smart 1/10Gigabit Switch solution**, the GS-2240 switch series, to meet the needs of enterprises, telecoms and campuses for a large-scale network deployment. The GS-2240 switch series provides a quick, safe and cost-effective 1/10G network solution for small businesses and enterprises.

Cost-effective 10Gbps Uplink Capacity

PLANET has made a big leap in the evolution of Ethernet with its launch of the GS-2240-24T4X whose four 10G SFP+ slots support **dual-speed, 10GBASE-SR/LR** or **1000BASE-SX/LX**, meaning the administrator now can flexibly choose a suitable SFP/SFP+ transceiver according to the transmission distance or speed required to extend the network efficiently. They greatly support an SMB network to achieve 10Gbps high performance in a cost-effective way because 10GbE interface usually could be available in Layer 3 Switch, which could be too expensive to SMBs.

Robust Layer 2 Features

The GS-2240 switch series can be programmed for advanced switch management functions such as **dynamic port link aggregation (LACP)**, **Spanning Tree Protocol (STP)**, **SNMP**, **bandwidth control**, **LLDP**, **DHCP snooping**, **IGMP snooping** and **L2 MAC security control**. The GS-2240 switch series provides **IEEE 802.1Q** tagged VLAN and **private VLAN**. With the supporting port aggregation, they allow the operation of a high-speed trunk by combining multiple ports and support fail-over as well.

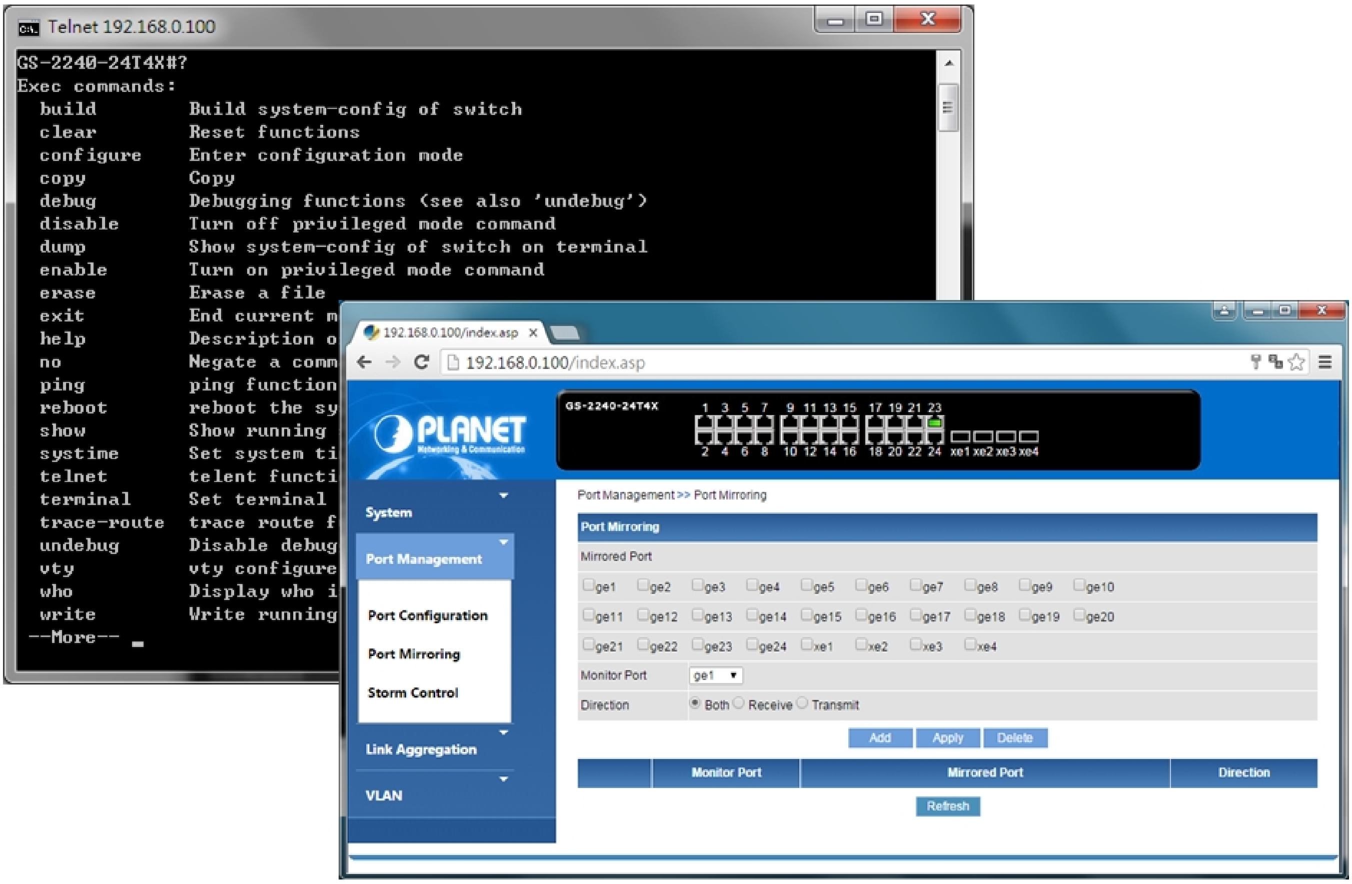


Efficient Traffic Control

The GS-2240 switch series is loaded with powerful traffic management to enhance services to business-class data, voice, and video solutions. The functionality includes **broadcast, multicast and unknown unicast storm control**, and per port **bandwidth control.** It guarantees the best performance for VoIP and video stream transmission, and empowers the enterprises to take full advantage of the limited network resources.

Friendly and Secure Management

For efficient management, the GS-2240 switch series is equipped with **web**, **console**, **Telnet** and **SNMP** management interfaces. With the built-in web-based management interface, the GS-2240 switch series offers an easy-to-use, platform-independent management and configuration facility. By supporting the standard SNMP, the switch can be managed via any standard management software. For text-based management, the switch can be accessed via Telnet.



```
GS-2240-24T4X#?
Exec commands:
  build        Build system-config of switch
  clear        Reset functions
  configure    Enter configuration mode
  copy         Copy
  debug        Debugging functions (see also 'undebug')
  disable      Turn off privileged mode command
  dump         Show system-config of switch on terminal
  enable       Turn on privileged mode command
  erase        Erase a file
  exit         End current m
  help         Description o
  no           Negate a comm
  ping         ping function
  reboot       reboot the sy
  show         Show running
  systime      Set system ti
  telnet       telent functi
  terminal     Set terminal
  trace-route  trace route f
  undebug      Disable debug
  vty          vty configure
  who          Display who i
  write        Write running
 --More--
```

Port Management >> Port Mirroring

Port Mirroring

Mirrored Port

□ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10
□ge11 □ge12 □ge13 □ge14 □ge15 □ge16 □ge17 □ge18 □ge19 □ge20
□ge21 □ge22 □ge23 □ge24 □xe1 □xe2 □xe3 □xe4

Monitor Port: ge1

Direction: ● Both ○ Receive ○ Transmit

Add | Apply | Delete

	Monitor Port	Mirrored Port	Direction

Refresh

1.3 How to Use This Manual

This User's Manual is structured as follows:

Section 2, INSTALLATION

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

Section 3, SWITCH MANAGEMENT

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

Section 4, WEB CONFIGURATION

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

Section 5, SWITCH OPERATION

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

Section 6, TROUBLESHOOTING

The chapter explains how to do troubleshooting of the Managed Switch.

Appendix A

The section contains cable information of the Managed Switch.

1.4 Product Features

- **Physical Port**
  - **10/100/1000BASE-T** Gigabit RJ45 copper ports
  - **4 10GBASE-SR/LR SFP+ slots,** compatible with 1000BASE-SX/LX/BX SFP
  - RJ45 to RS232 DB9 console interface for basic management and setup

- **Layer 2 Features**
  - Prevents packet loss with back pressure (half-duplex) and IEEE 802.3x pause frame flow control (full-duplex)
  - Supports **VLAN**
    - IEEE 802.1Q tagged VLAN
    - IP subnet-based VLAN
    - MAC-based VLAN
    - Protocol-based VLAN
    - Private VLAN
  - Supports **Spanning Tree Protocol**
    - STP (Spanning Tree Protocol)
    - RSTP (Rapid Spanning Tree Protocol)
    - MSTP (Multiple Spanning Tree Protocol)
  - Supports **Link Aggregation**
    - IEEE 802.3ad Link Aggregation Control Protocol (LACP)
    - Cisco ether-channel (static trunk)
  - Provides port mirror (many-to-1)
  - Supports Ingress/Egress Rate Limit per port bandwidth control

- **Multicast**
  - Supports IGMP snooping v1, v2 and v3
  - Querier mode support
  - IGMP router port

- **Security**
  - DHCP snooping to filter distrusted DHCP messages
  - MAC security
    - Static MAC address
    - MAC binding
    - MAC auto binding
    - Per port MAC address entries limitation
  - Storm control
    - Broadcast, multicast, unknown-unicast

Management

- IPv4 management
- Switch management interface
  - Web switch management
  - Telnet command line interface
  - Console command line interface
  - SNMP v1, v2c
- System maintenance
  - Firmware upload/download via HTTP
  - Configuration upload/download through web interface
  - Hardware reset button for system reboot or reset to factory default
- Link Layer Discovery Protocol (LLDP)
- Ping diagnostics
- Trace-route
- SNMP trap for interface linkup and linkdown notification
- Log management

1.5 Product Specifications

GS-2240-24T4X

Product	GS-2240-24T4X	GS-2240-48T4X
Hardware Specifications		
Copper Ports	24 x 10/100/1000BASE-T RJ45 auto-MDI/MDI-X port	48 x 10/100/1000BASE-T RJ45 auto-MDI/MDI-X port
SFP/mini-GBIC Slots	4 10GBASE-SR/LR SFP+ interface (XE1 to XE4) Compatible with 1000BASE-SX/LX/BX SFP transceiver	
Switch Architecture	Store-and-Forward	Store-and-Forward
Switch Fabric	128Gbps/non-blocking	176Gbps/non-blocking
Switch Throughput@64Bytes	95.24Mpps	130.95Mpps
Address Table	16K entries	16K entries
Shared Data Buffer	1.5Mbytes	1.5Mbytes
Jumbo Frame	13K bytes	13K bytes
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex	
Reset Button	< 5 sec: System reboot > 5 sec: Factory default	
LED	PWR, SYS, 10/100, 1000, 10G	
Power Requirements	100~240V AC, 50/60Hz, auto-sensing	
Dimensions (W x D x H)	440 x 230 x 44 mm, 1U height	440 x 270 x 44 mm, 1U height
ESD Protection	Contact Discharge 4KV DC Air Discharge 8KV DC	Contact Discharge 4KV DC Air Discharge 8KV DC
Enclosure	Metal	Metal
Weight	2865g	3969g
Power Consumption/ Dissipation	31 watts (max.)/106 BTU	45 watts (max.)/154 BTU
Layer 2 Functions		
Port Mirroring	TX/RX/both Many-to-1 monitor	
VLAN	802.1Q tagged-based VLAN Up to 4000 VLAN groups, out of 4094 VLAN IDs IP subnet-based VLAN MAC-based VLAN Protocol-based VLAN Private VLAN	
Link Aggregation	IEEE 802.3ad LACP and static trunk Supports 32 groups with 8 ports per trunk group	
Spanning Tree Protocol	IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)	

IGMP Snooping	IGMP snooping v1, v2, v3, up to 255 multicast groups IGMP querier mode support
Security	DHCP snooping Static MAC address MAC binding MAC auto binding Per port MAC address entries limitation Broadcast, multicast, unknown unicast storm control
Management Functions	
Basic Management Interfaces	Web browser, Telnet, console SNMP v1, v2c Firmware upgrade by HTTP protocol through Ethernet network System log
SNMP MIBs	RFC 1213 MIB-II RFC 1215 Generic Traps
Standards Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE, LVD
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3ae 10 Gigabit Ethernet IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1ab LLDP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1Q VLAN tagging RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP v1 RFC 2236 IGMP v2 RFC 3376 IGMP v3
Environment	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -20 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

2. INSTALLATION

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

2.1 Hardware Description

2.1.1 Switch Front Panel

The front panel provides a simple interface monitoring the Managed Switch. Figures 2-1-1 to 2-1-2 show the front panel of the Managed Switch.

GS-2240-24T4X Front Panel

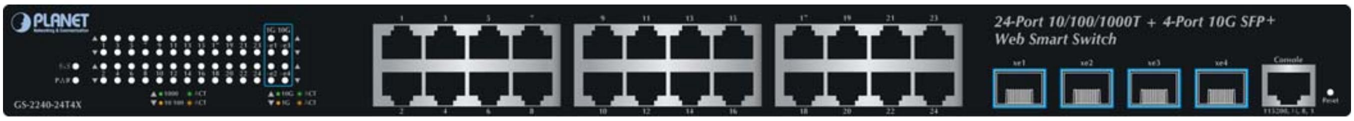


Figure 2-1-1: Front Panel of GS-2240-24T4X

GS-2240-48T4X Front Panel

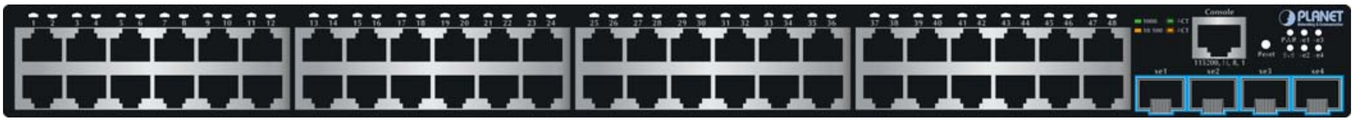


Figure 2-1-2: Front Panel of GS-2240-48T4X

- **Gigabit TP interface**

  10/100/1000BASE-T copper, RJ45 twisted-pair: Up to 100 meters.

- **10 Gigabit SFP+ slot**

  10GBASE-SR/LR mini-GBIC slot, SFP+ (Small Factor Pluggable Plus) Transceiver module supports from 300 meters (multi-mode fiber) up to 10 kilometers (single mode fiber)

- **Console port**

  The console port is a RJ45 port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP address setting, factory reset, port management, link status and system setting. Users can use the attached DB9 to RJ45 console cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

- **Reset button**

The front panel of the GS-2240-24T4X/GS-2240-48T4X comes with a reset button designed for rebooting the Managed Switch without turning off and on the power. The following is the summary table of reset button functions:

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

2.1.2 LED Indications

The front panel LEDs indicate instant status of power and system status, fan status, port links/PoE-in-use and data activity; they help monitor and troubleshoot when needed. Figures 2-1-3 to 2-1-4 show the LED indications of the Managed Switch.

GS-2240-24T4X LED Indication

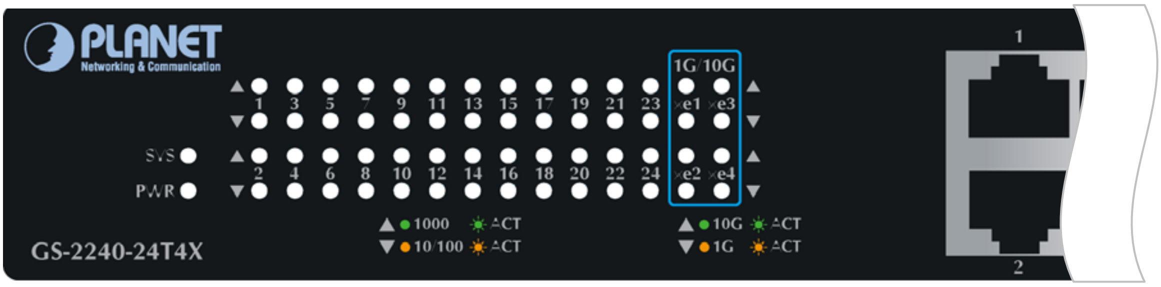


Figure 2-1-3: GS-2240-24T4X LED on Front Panel

- **System**

LED	Color	Function
PWR	Green	**Lights** to indicate that the Switch has power.
SYS	Green	**Blinks** to indicate that the Switch boots successfully.
		Off to indicate that the Switch is booting.

- **Per 10/100/1000Mbps RJ45 port (Port-1 to Port-24)**

LED	Color	Function	
10/100	Orange	**Lights**	Indicates the link through that port is successfully established at 10/100Mbps.
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.
1G	Green	**Lights**	Indicates the link through that port is successfully established at 1000Mbps.
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.

- **Per 1/10G SFP+ Interface (Port-25 to Port-28)**

LED	Color	Function	
1G	Orange	**Lights**	Indicates the link through that port is successfully established at 1Gbps.
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.
10G	Green	**Lights**	Indicates the link through that port is successfully established at 10Gbps.
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.

GS-2240-48T4X LED Indication

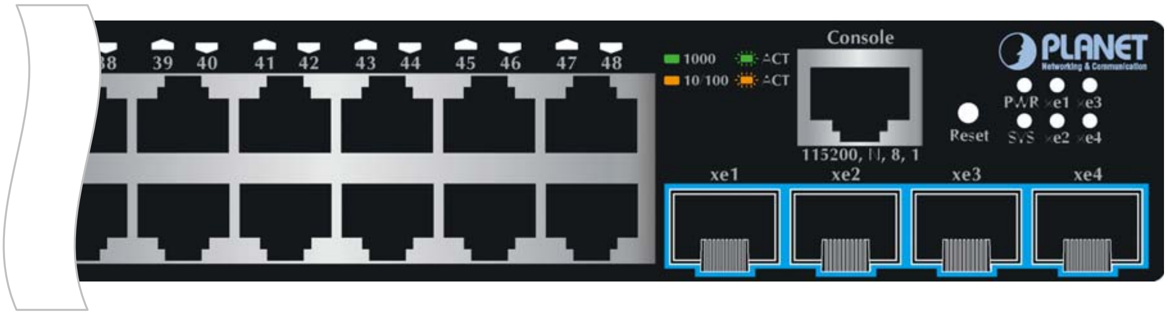


Figure 2-1-4: GS-2240-48T4X LED on Front Panel

- **System**

LED	Color	Function
PWR	Green	**Lights** to indicate that the Switch has power.
SYS	Green	**Blinks** to indicate that the Switch boots successfully.
		Off to indicate that the Switch is booting.

- **Per 10/100/1000Mbps RJ45 port (Port-1 to Port-48)**

LED	Color	Function	
10/100	Orange	**Lights**	Indicates the link through that port is successfully established at 10/100Mbps.
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.
1G	Green	**Lights**	Indicates the link through that port is successfully established at 1000Mbps.
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.

- **Per 1/10G SFP+ Interface (Port-49 to Port-52)**

LED	Color	Function	
1/10G	Green	**Lights**	Indicates the link through that port is successfully established at 1/10Gbps.
		Blinks	Indicates that the Switch is actively sending or receiving data over that port.

2.1.3 Switch Rear Panel

The rear panel of the Managed Switch consists of the AC/DC inlet power socket. Figures 2-1-5 to 2-1-6 show the rear panel of the Managed Switch.

GS-2240-24T4X Rear Panel

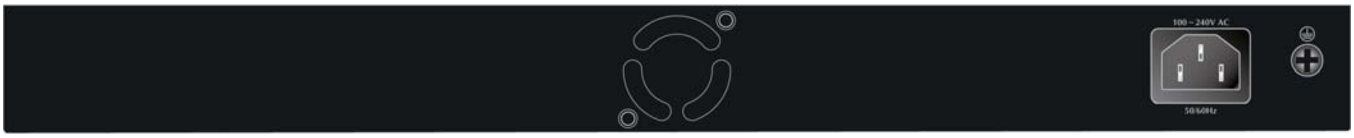


Figure 2-1-5: Rear Panel of GS-2240-24T4X

GS-2240-48T4X Rear Panel

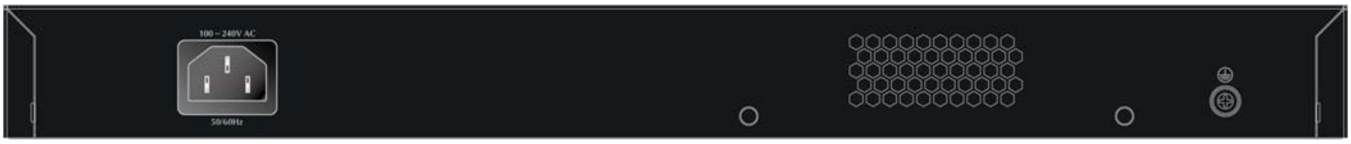


Figure 2-1-6: Rear Panel of GS-2240-48T4X

- **AC Power Receptacle**

  For compatibility with electrical voltages in most areas of the world, the Managed Switch's power supply can automatically adjust line power in the range of 100-240V AC and 50/60 Hz.

  Plug the female end of the power cord firmly into the receptacle on the rear panel of the Managed Switch and the other end of the power cord into an electrical outlet and the power will be ready.

Power Notice: The device is a power-required device, which means it will not work till it is powered. If your networks should be active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime. In some areas, installing a surge suppression device may also help to protect your Managed Switch from being damaged by unregulated surge or current to the Switch or the power adapter.

2.2 Installing the Switch

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

2.2.1 Desktop Installation

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

Step 1: Attach the rubber feet to the recessed areas on the bottom of the Managed Switch.

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

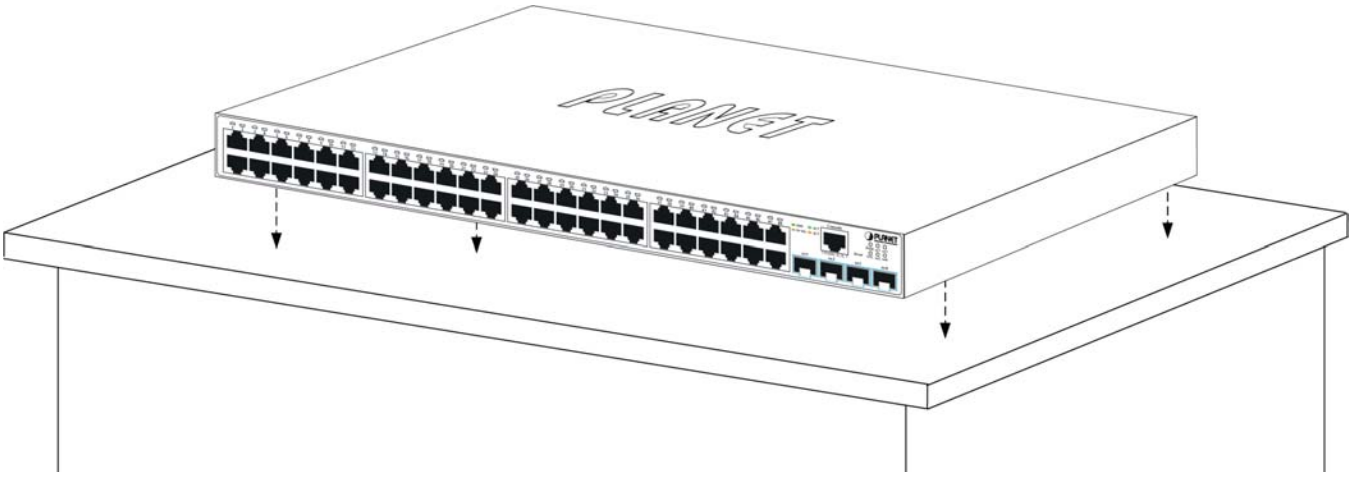


Figure 2-2-1: Place the Managed Switch on the Desktop

Step 3: Keep enough ventilation space between the Managed Switch and the surrounding objects.

Note

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

Step 4: Connect the Managed Switch to network devices.

Connect one end of a standard network cable to the 10/100/1000 RJ45 ports on the front of the Managed Switch.

Connect the other end of the cable to the network devices such as printer server, workstation or router.

Note

Connection to the Managed Switch requires UTP Category 5e network cabling with RJ45 tips. For more information, please see the Cabling Specification in Appendix A.

Step 5: Supply power to the Managed Switch.

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

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

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

2.2.2 Rack Mounting

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

Step 1: Place the Managed Switch on a hard flat surface, with the front panel positioned towards the front side.

Step 2: Attach the rack-mount bracket to each side of the Managed Switch with supplied screws attached to the package.

Figure 2-2-2 shows how to attach brackets to one side of the Managed Switch.

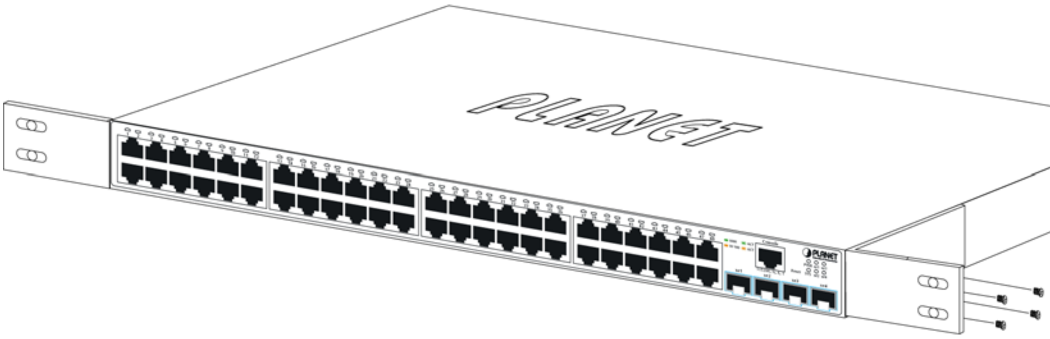


Figure 2-2-2: Attach Brackets to the Managed Switch.

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

Step 3: Secure the brackets tightly.

Step 4: Follow the same steps to attach the second bracket to the opposite side.

Step 5: After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-2-3.

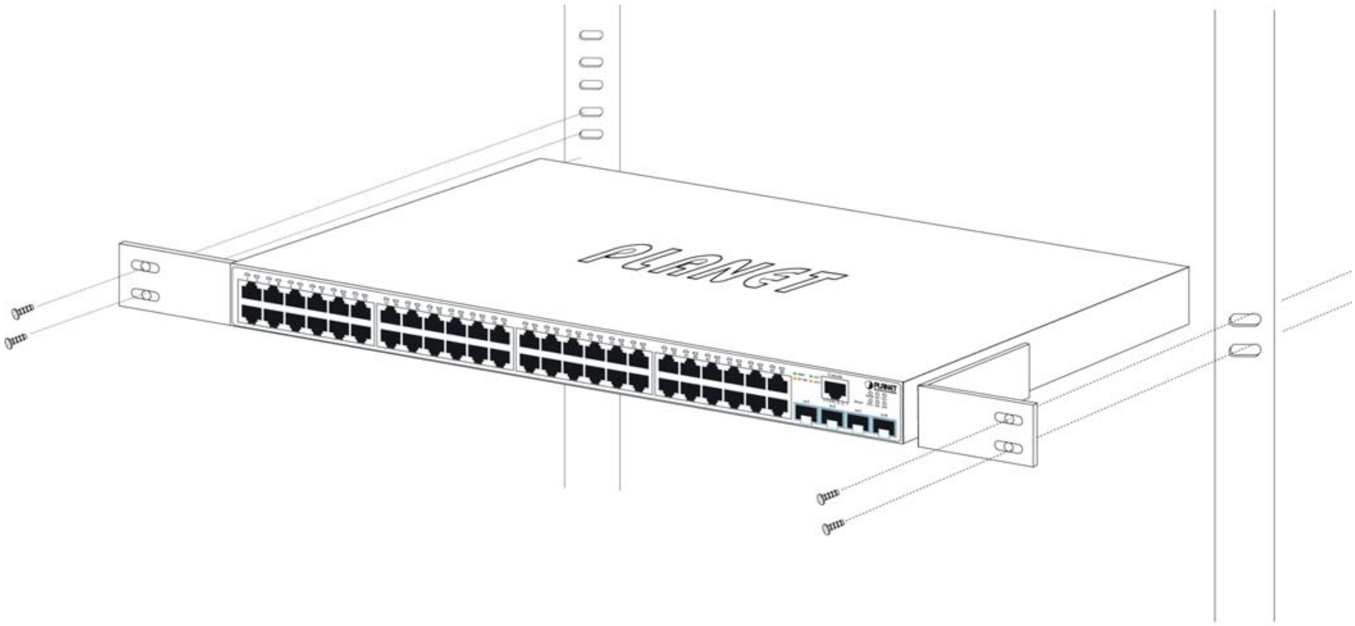


Figure 2-2-3: Mounting Managed Switch in a Rack

Step 6: Proceed with Steps 4 and 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Managed Switch.

2.2.3 Installing the SFP/SFP+ Transceiver

The sections describe how to insert an SFP/SFP+ transceiver into an SFP/SFP+ slot. The SFP/SFP+ transceivers are hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP/SFP+ port without having to power down the Managed Switch, as the Figure 2-2-4 shows..

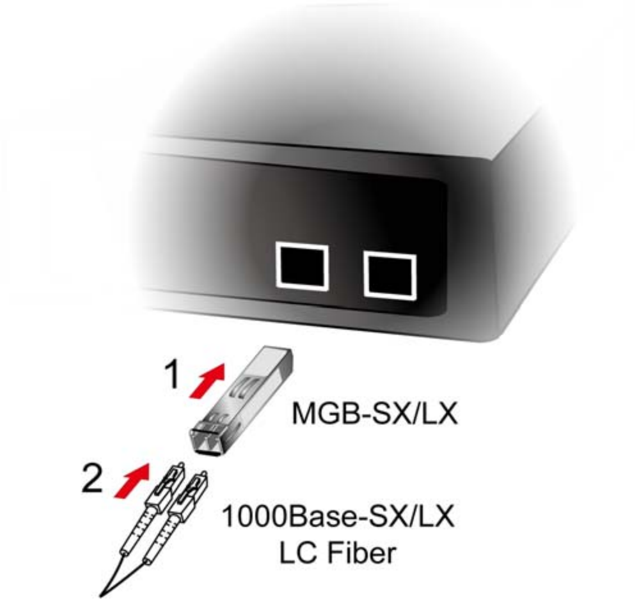


Figure 2-2-4: Plug-in the SFP/SFP+ Transceiver

- **Approved PLANET SFP/SFP+ Transceivers**

PLANET Managed Switch supports both single mode and multi-mode SFP/SFP+ transceivers. The following list of approved PLANET SFP/SFP+ transceivers is correct at the time of publication:

Gigabit Ethernet Transceiver (1000BASE-X SFP)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (nm)	Operating Temp.
MGB-GT	1000	Copper	--	100m	--	0 ~ 60 degrees C
MGB-SX	1000	LC	Multi Mode	550m	850nm	0 ~ 60 degrees C
MGB-SX2	1000	LC	Multi Mode	2km	1310nm	0 ~ 60 degrees C
MGB-LX	1000	LC	Single Mode	10km	1310nm	0 ~ 60 degrees C
MGB-L30	1000	LC	Single Mode	30km	1310nm	0 ~ 60 degrees C
MGB-L50	1000	LC	Single Mode	50km	1550nm	0 ~ 60 degrees C
MGB-L70	1000	LC	Single Mode	70km	1550nm	0 ~ 60 degrees C
MGB-L120	1000	LC	Single Mode	120km	1550nm	0 ~ 60 degrees C
MGB-TSX	1000	LC	Multi Mode	550m	850nm	-40 ~ 75 degrees C
MGB-TLX	1000	LC	Single Mode	10km	1310nm	-40 ~ 75 degrees C
MGB-TL30	1000	LC	Single Mode	30km	1310nm	-40 ~ 75 degrees C
MGB-TL70	1000	LC	Single Mode	70km	1550nm	-40 ~ 75 degrees C

Gigabit Ethernet Transceiver (1000BASE-BX, Single Fiber Bi-directional SFP)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (TX/RX)	Operating Temp.
MGB-LA10	1000	WDM(LC)	Single Mode	10km	1310nm/1550nm	0 ~ 60 degrees C
MGB-LB10	1000	WDM(LC)	Single Mode	10km	1550nm/1310nm	0 ~ 60 degrees C
MGB-LA20	1000	WDM(LC)	Single Mode	20km	1310nm/1550nm	0 ~ 60 degrees C
MGB-LB20	1000	WDM(LC)	Single Mode	20km	1550nm/1310nm	0 ~ 60 degrees C
MGB-LA40	1000	WDM(LC)	Single Mode	40km	1310nm/1550nm	0 ~ 60 degrees C
MGB-LB40	1000	WDM(LC)	Single Mode	40km	1550nm/1310nm	0 ~ 60 degrees C
MGB-LA60	1000	WDM(LC)	Single Mode	60km	1310nm/1550nm	0 ~ 60 degrees C
MGB-LB60	1000	WDM(LC)	Single Mode	60km	1550nm/1310nm	0 ~ 60 degrees C
MGB-TLA10	1000	WDM(LC)	Single Mode	10km	1310nm/1550nm	-40 ~ 75 degrees C
MGB-TLB10	1000	WDM(LC)	Single Mode	10km	1550nm/1310nm	-40 ~ 75 degrees C
MGB-TLA20	1000	WDM(LC)	Single Mode	20km	1310nm/1550nm	-40 ~ 75 degrees C
MGB-TLB20	1000	WDM(LC)	Single Mode	20km	1550nm/1310nm	-40 ~ 75 degrees C
MGB-TLA40	1000	WDM(LC)	Single Mode	40km	1310nm/1550nm	-40 ~ 75 degrees C
MGB-TLB40	1000	WDM(LC)	Single Mode	40km	1550nm/1310nm	-40 ~ 75 degrees C
MGB-TLA60	1000	WDM(LC)	Single Mode	60km	1310nm/1550nm	-40 ~ 75 degrees C
MGB-TLB60	1000	WDM(LC)	Single Mode	60km	1550nm/1310nm	-40 ~ 75 degrees C

10Gbps SFP+ (10G Ethernet/10GBASE)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (nm)	Operating Temp.
MTB-SR	10G	LC	Multi Mode	Up to 300m	850nm	0 ~ 60 degrees C
MTB-LR	10G	LC	Single Mode	10km	1310nm	0 ~ 60 degrees C

10Gbps SFP+ (10GBASE-BX, Single Fiber Bi-directional SFP)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (TX)	Wavelength (RX)	Operating Temp.
MTB-LA20	10G	WDM(LC)	Single Mode	20km	1270nm	1330nm	0 ~ 60 degrees C
MTB-LB20	10G	WDM(LC)	Single Mode	20km	1330nm	1270nm	0 ~ 60 degrees C
MTB-LA40	10G	WDM(LC)	Single Mode	40km	1270nm	1330nm	0 ~ 60 degrees C
MTB-LB40	10G	WDM(LC)	Single Mode	40km	1330nm	1270nm	0 ~ 60 degrees C
MTB-LA60	10G	WDM(LC)	Single Mode	60km	1270nm	1330nm	0 ~ 60 degrees C
MTB-LB60	10G	WDM(LC)	Single Mode	60km	1330nm	1270nm	0 ~ 60 degrees C

Note

It is recommended to use PLANET SFP/SFP+ on the Managed Switch. If you insert an SFP/SFP+ transceiver that is not supported, the Managed Switch will not recognize it.

1. Before we connect the GS-2240 series to the other network device, we have to make sure both sides of the SFP transceivers are with the same media type, for example: 1000BASE-SX to 1000BASE-SX, 1000Bas-LX to 1000BASE-LX.
2. Check whether the fiber-optic cable type matches with the SFP transceiver requirement.
   - To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
   - To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

Connect the Fiber Cable

1. Insert the duplex LC connector into the SFP/SFP+ transceiver.
2. Connect the other end of the cable to a device with SFP/SFP+ transceiver installed.
3. Check the LNK/ACT LED of the SFP/SFP+ slot on the front of the Managed Switch. Ensure that the SFP/SFP+ transceiver is operating correctly.
4. Check the Link mode of the SFP/SFP+ port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to "**10G Force**", "**1000M Force**".

Remove the Transceiver Module

1. Make sure there is no network activity anymore.
2. Remove the Fiber-Optic Cable gently.
3. Lift up the lever of the MGB module and turn it to a horizontal position.
4. Pull out the module gently through the lever.

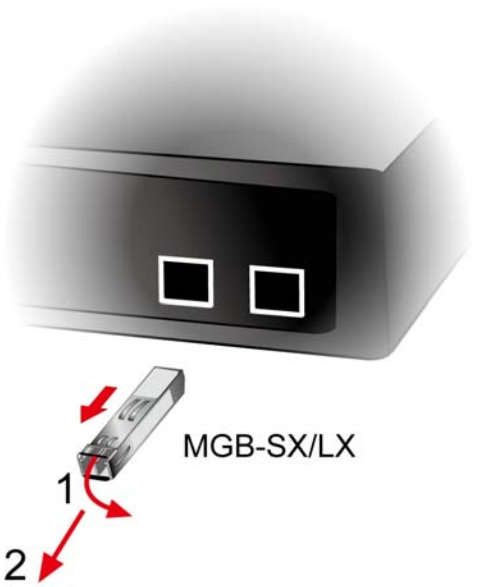


Figure 2-2-5: How to Pull Out the SFP/SFP+ Transceiver

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

3. SWITCH MANAGEMENT

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

This chapter covers the following topics:

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

3.1 Requirements

- **Workstations** running Windows 2000/XP, 2003, Vista/7/8/10, 2008, MAC OS9 or later, or Linux, UNIX , or other platforms compatible with **TCP/IP** protocols.
- **Workstation** is installed with **Ethernet NIC** (Network Interface Card)
- **Serial Port** connect (Terminal)
  - The above PC with COM Port (DB9/RS232) or USB-to-RS232 converter
- Ethernet Port connect
  - Network cables - Use standard network (UTP) cables with RJ45 connectors.
- The above workstation is installed with **Web Browser** and **JAVA runtime environment** plug-in

Note

It is recommended to use Internet Explore 7.0 or above to access Managed Switch.

3.2 Management Access Overview

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

- An administration **console**
- **Web browser** interface
- An external **SNMP-based network management application**

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

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

Table 3-1 Comparison of Management Methods

3.3 Administration Console

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

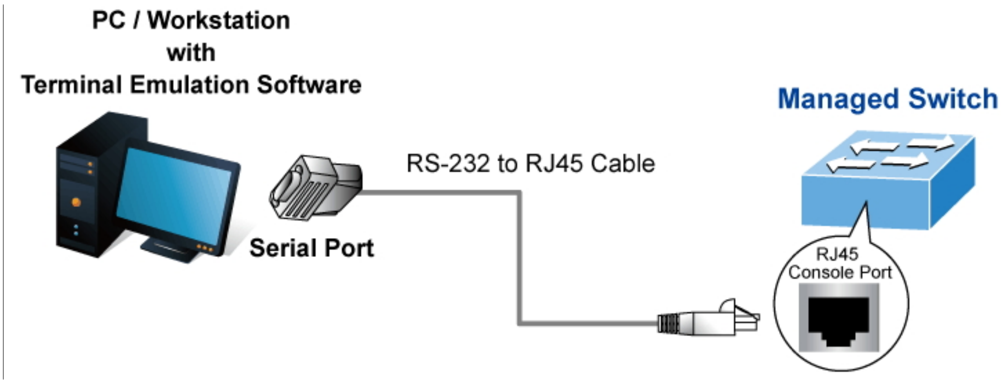


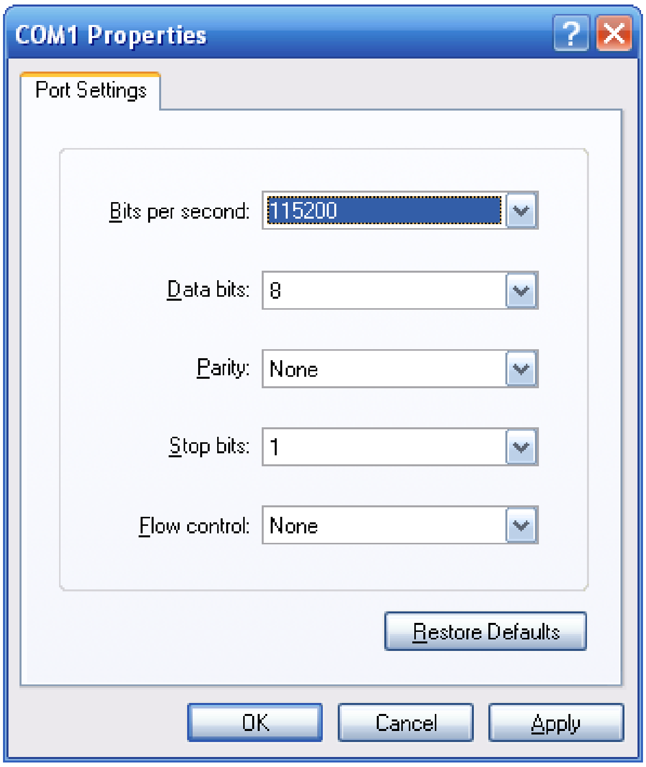
Figure 3-1-1: Console Management

Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as **HyperTerminal, PuTTY**) to the Managed Switch console (serial) port. When using this management method, a **straight DB9 RS232 cable** is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:

The default parameters are:

- **115200 bps**
- **8 data bits**
- **No parity**
- **1 stop bit**



Bits per second: 115200
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

Figure 3-1-2: Terminal Parameter Settings

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

3.4 Web Management

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

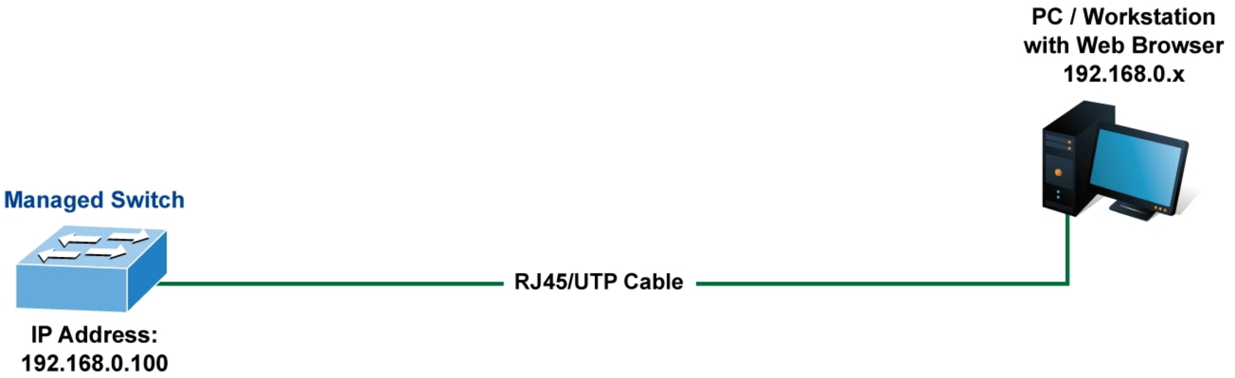
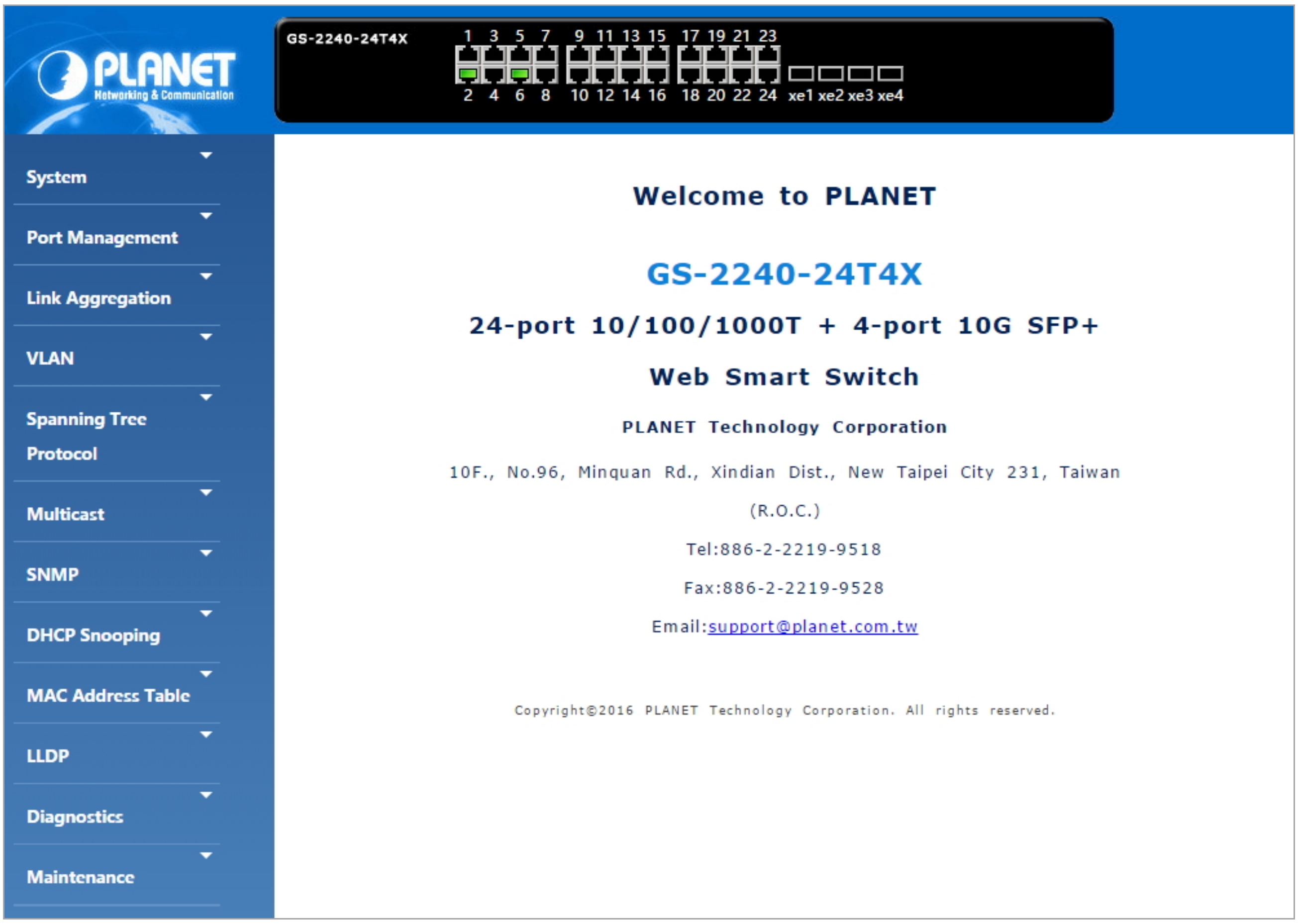


Figure 3-1-3: Web Management

You can then use your Web browser to list and manage the Managed Switch configuration parameters from one central location, just as if you were directly connected to the Managed Switch's console port. Web Management requires either **Microsoft Internet Explorer 7.0** or later, **Safari** or **Mozilla Firefox 1.5** or later.



Welcome to PLANET

GS-2240-24T4X

24-port 10/100/1000T + 4-port 10G SFP+

Web Smart Switch

PLANET Technology Corporation

10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)

Tel:886-2-2219-9518

Fax:886-2-2219-9528

Email:support@planet.com.tw

Copyright©2016 PLANET Technology Corporation. All rights reserved.

Figure 3-1-4: Web Main Screen of Managed Switch

3.5 SNMP-based Network Management

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

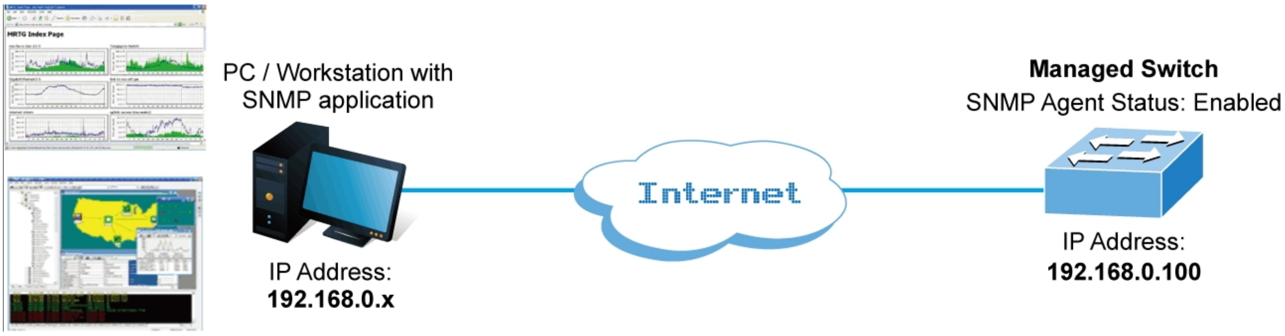


Figure 3-1-5: SNMP Management

4. WEB CONFIGURATION

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

About Web-based Management

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

The Web-based Management supports Internet Explorer 7.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

> Note
>
> By default, IE7.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

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

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

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

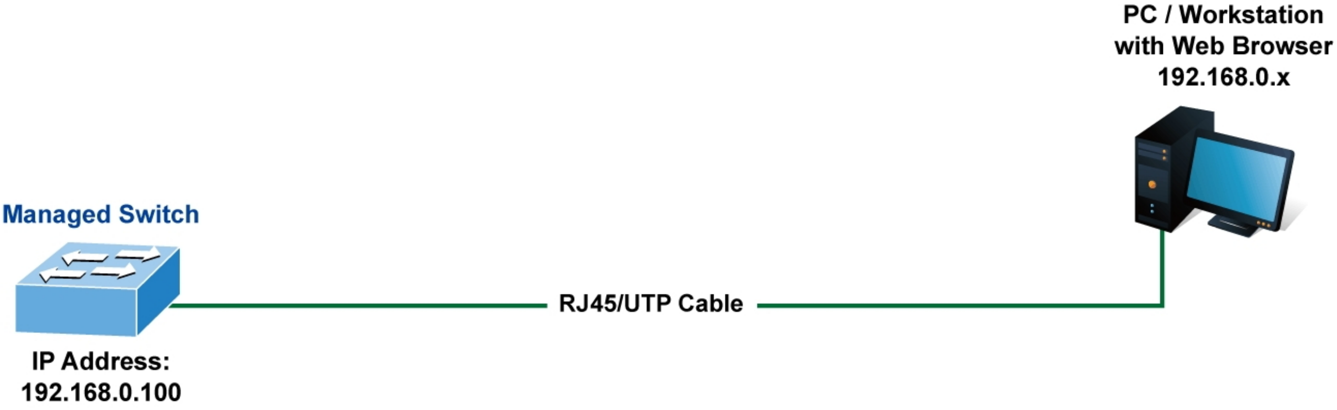


Figure 4-1-1: Web Management

- **Logging on the Managed Switch**

1. Use Internet Explorer 7.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address is shown as follows:

http://192.168.0.100

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

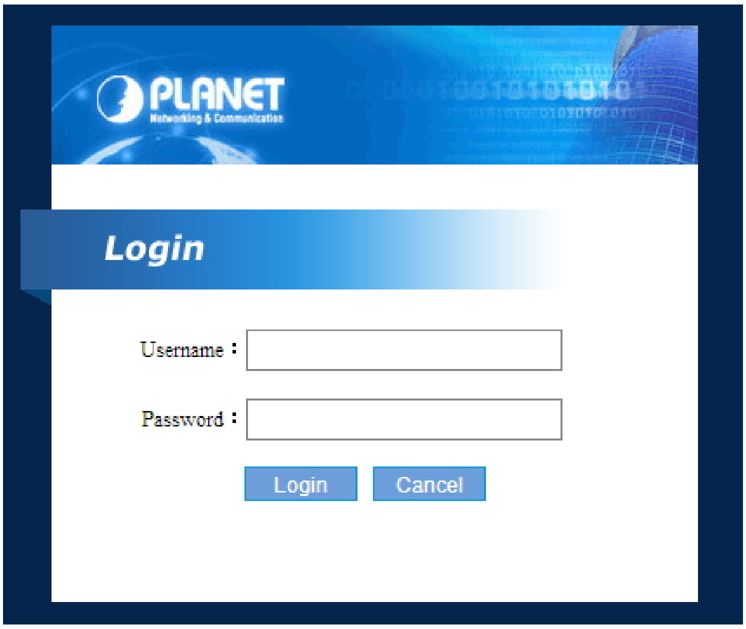
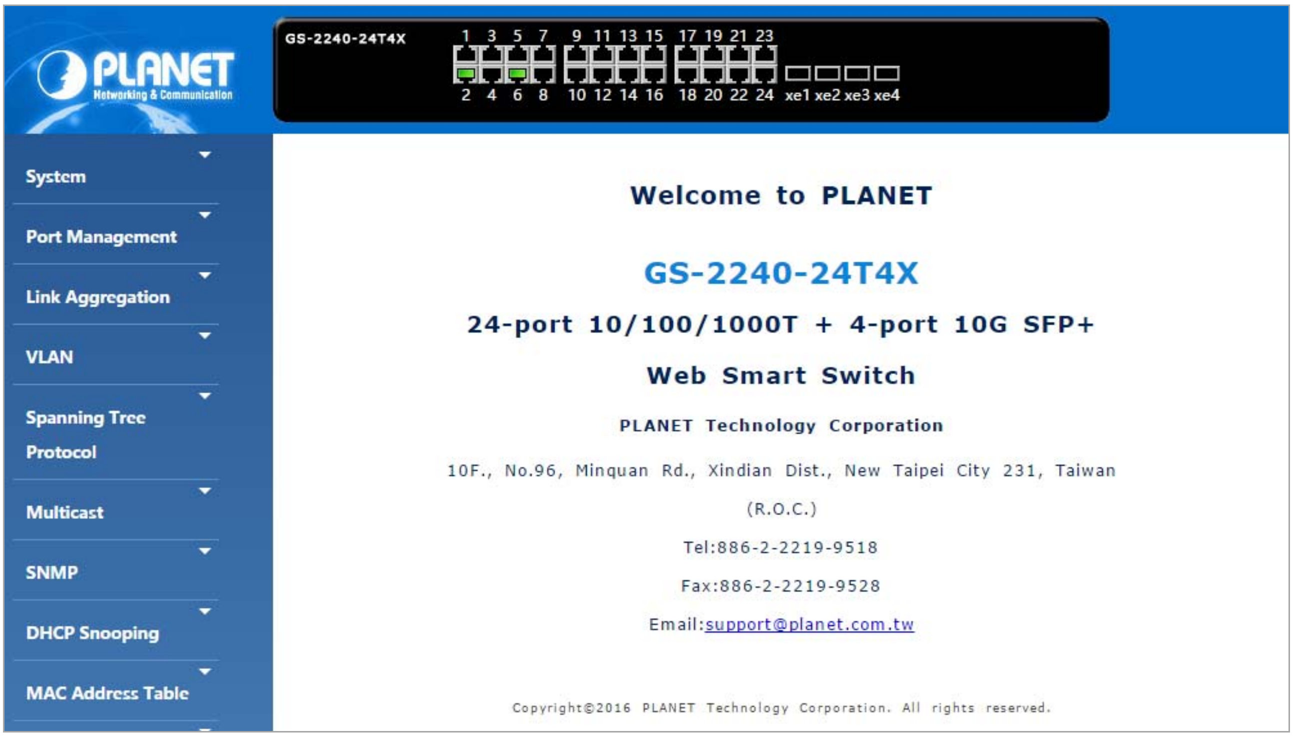


Figure 4-1-2: Login Screen

Default User name: **admin**

Default Password: **admin**

After entering the username and password, the main screen appears as shown in Figure 4-1-3.



Welcome to PLANET

GS-2240-24T4X

24-port 10/100/1000T + 4-port 10G SFP+

Web Smart Switch

PLANET Technology Corporation

10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)

Tel:886-2-2219-9518

Fax:886-2-2219-9528

Email:support@planet.com.tw

Copyright©2016 PLANET Technology Corporation. All rights reserved.

Figure 4-1-3: Web Main Page

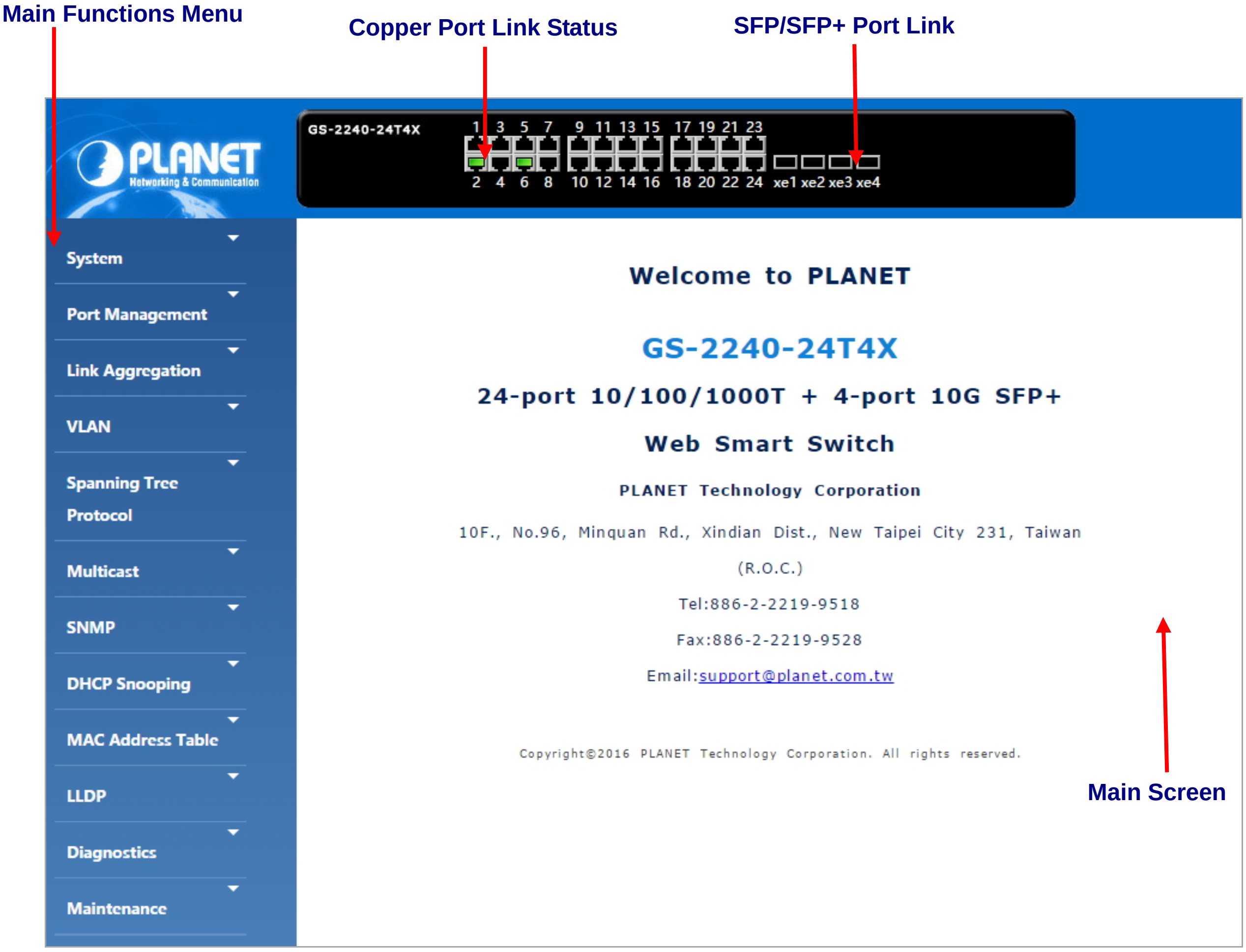
Now, you can use the Web management interface to continue the switch management or manage the Managed Switch by Web interface. The Switch Menu on the left of the web page lets you access all the commands and statistics the Managed Switch provides.

Note

1. It is recommended to use Internet Explore 7.0 or above to access Managed Switch.
2. The changed IP address takes effect immediately after clicking on the **Save** button from Maintainance >> Backup/Upgrade Manager. You need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.
4. Only accept command in lowercase letter under web interface.

4.1 Main Web Page

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



Welcome to PLANET

GS-2240-24T4X

24-port 10/100/1000T + 4-port 10G SFP+

Web Smart Switch

PLANET Technology Corporation

10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)

Tel:886-2-2219-9518

Fax:886-2-2219-9528

Email:support@planet.com.tw

Copyright©2016 PLANET Technology Corporation. All rights reserved.

Figure 4-1-4: Web Main Page

Panel Display

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

The port status are illustrated as follows:

State	Disabled	Down	Link
RJ45 Ports	🟥	⬛	🟩
SFP Ports	🟥	⬛	🟩

Main Menu

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

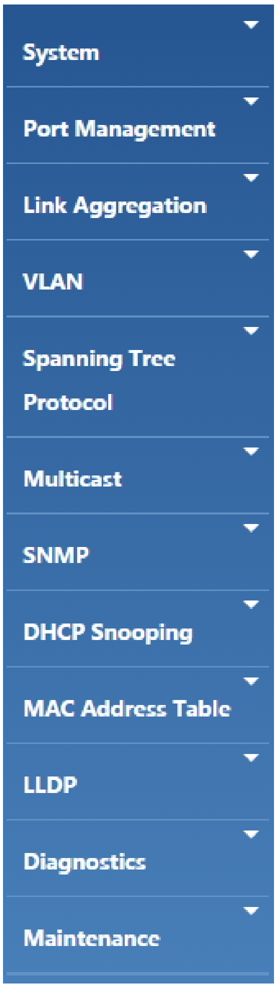


Figure 4-1-5: Managed Switch Main Functions Menu

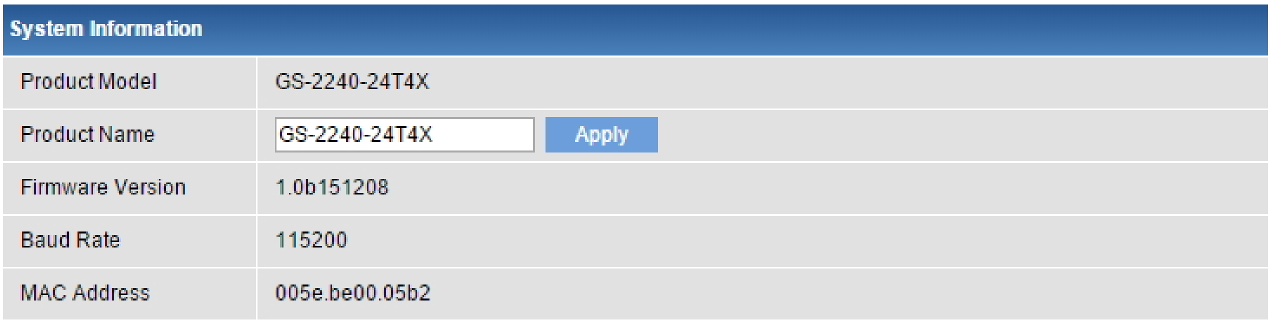
4.2 System

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

- **System Information** The Managed Switch system information is provided here.
- **System Status** This page displays the CPU load, memory load aand running time
- **IP Configuration** Configure the switch-managed IP information on this page.
- **Static Route** Configure static routing on this page.
- **ARP Table** This page displays the status of the neighbour cache (ARP cache).
- **User Configuration** Configure new user password on this page.
- **Time Settings** Configure time parameter on this page.
- **Log Management** The switch log information is provided here.
- **Logout** Log out the switch

4.2.1 System Information

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



System Information

Product Model	GS-2240-24T4X
Product Name	GS-2240-24T4X Apply
Firmware Version	1.0b151208
Baud Rate	115200
MAC Address	005e.be00.05b2

Figure 4-2-1: System Information Page Screenshot

The page includes the following fields:

Object	Description
• **Product Model**	Displays the current product model
• **Product Name**	The product name configured in SNMP | System Information | System Name.
• **Firmware Version**	The firmware version of this Managed Switch.
• **Baud Rate**	The Baud Rate of this Managed Switch.
• **MAC Address**	The MAC Address of this Managed Switch.

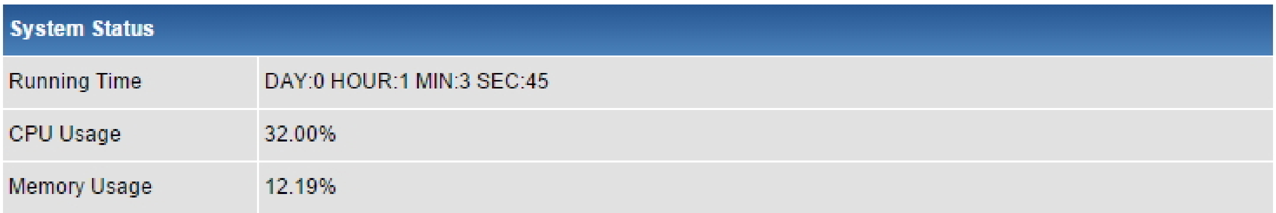
Buttons

Refresh: Click to refresh the page; any changes made locally will be undone.

Apply: Click to apply changes.

4.2.2 System Status

System Status displays the status of the System CPU, memory, running time. The screen in Figure 4-2-2 appears.



System Status

Running Time	DAY:0 HOUR:1 MIN:3 SEC:45
CPU Usage	32.00%
Memory Usage	12.19%

Figure 4-2-2: System Status Page Screenshot

The page includes the following fields:

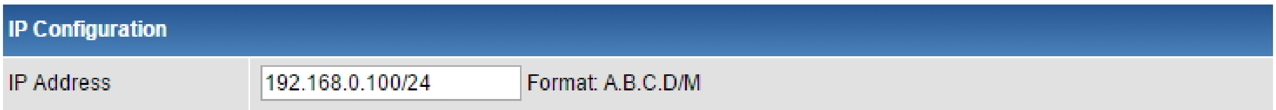
Object	Description
- **Running Time**	Displays the current running time
- **CPU Usage**	Displays the current CPU usage
- **Memory Usage**	Displays the current memory usage

Buttons

Refresh: Click to refresh the page; any changes made locally will be undone.

4.2.3 IP Configuration

The IP Configuration includes the IP Address, Subnet Mask. The configured column is used to view or change the IP configuration. Fill out the IP Address, Subnet Mask for the device. The screen in Figure 4-2-3 appears.



IP Configuration

IP Address	192.168.0.100/24	Format: A.B.C.D/M

Figure 4-2-3: IP Configuration Page Screenshot

The page includes the following fields:

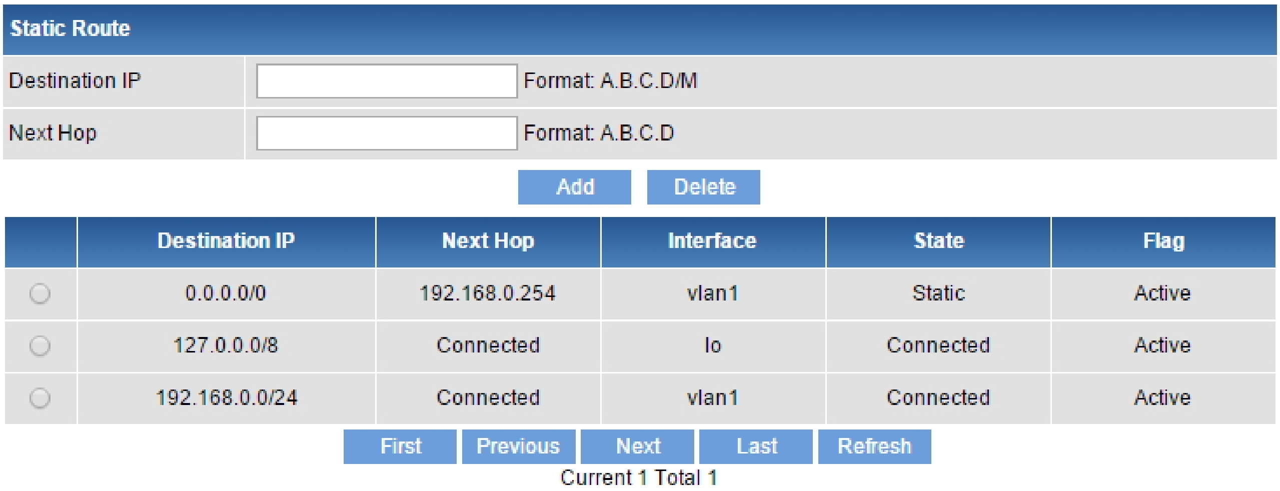
Object	Description
- **IP Address**	Provides the IP address and subnet mask of this switch in dotted decimal notation Example: 192.168.0.100/24.

Buttons

Apply: Click to apply changes.

4.2.4 Static Route

The static route includes the destination IP, next hop. The configured column is used to view or change the IP route. Fill out the destination, next hop for the device., the screen in Figure 4-2-4 appears.



Static Route

Destination IP	Format: A.B.C.D/M
Next Hop	Format: A.B.C.D

	Destination IP	Next Hop	Interface	State	Flag
○	0.0.0.0/0	192.168.0.254	vlan1	Static	Active
○	127.0.0.0/8	Connected	lo	Connected	Active
○	192.168.0.0/24	Connected	vlan1	Connected	Active

Current 1 Total 1

Figure 4-2-4: Static Route Page Screenshot

The page includes the following fields:

Object	Description
Destination IP	Provides the destination network of this switch in dotted decimal notation. Example: 0.0.0.0/0
Next Hop	Provides the next hop IP address of this switch in dotted decimal notation.

Buttons

Add: Click to add a new static route.

Delete: Click to delete a new static route.

First: Click to move to the first page.

Previous: Click to move to the previous page.

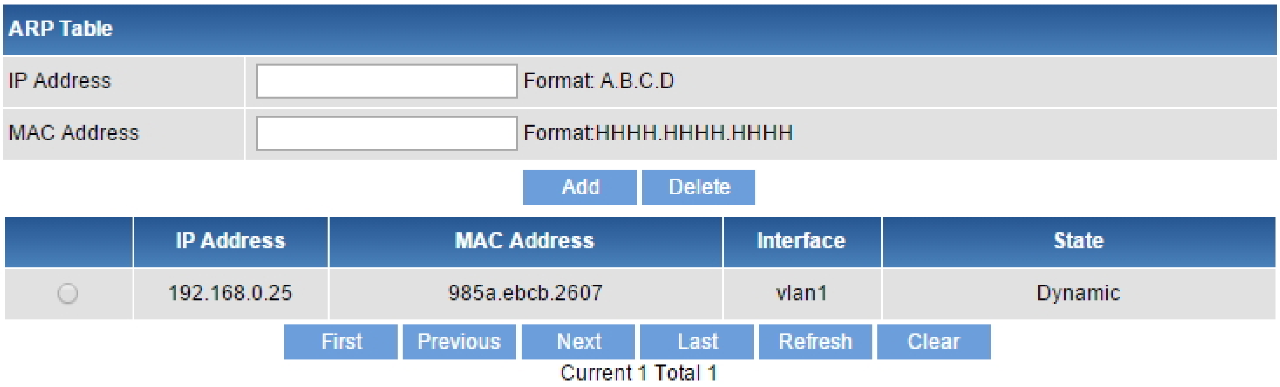
Next: Click to move to the next page.

Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.2.5 ARP Table

ARP table displays the table of the MAC address in the localhost, and the screen in Figure 4-2-5 appears.



ARP Table

IP Address		Format: A.B.C.D
MAC Address		Format:HHHH.HHHH.HHHH

	IP Address	MAC Address	Interface	State
○	192.168.0.25	985a.ebcb.2607	vlan1	Dynamic

Current 1 Total 1

Figure 4-2-5: ARP Table Page Screenshot

The page includes the following fields:

Object	Description
IP Address	Add the IP address for the specific device in dotted decimal notation Example: 192.168.0.20
MAC Address	Add the MAC address for the specific device in dotted Hexadecimal notation Example: 0030.4FAA.BBEE

Buttons

Add: Click to add a new data to the feature.

Delete: Click to delete a new data to the feature.

First: Click to move to the first page.

Previous: Click to move to the previous page.

Next: Click to move to the next page.

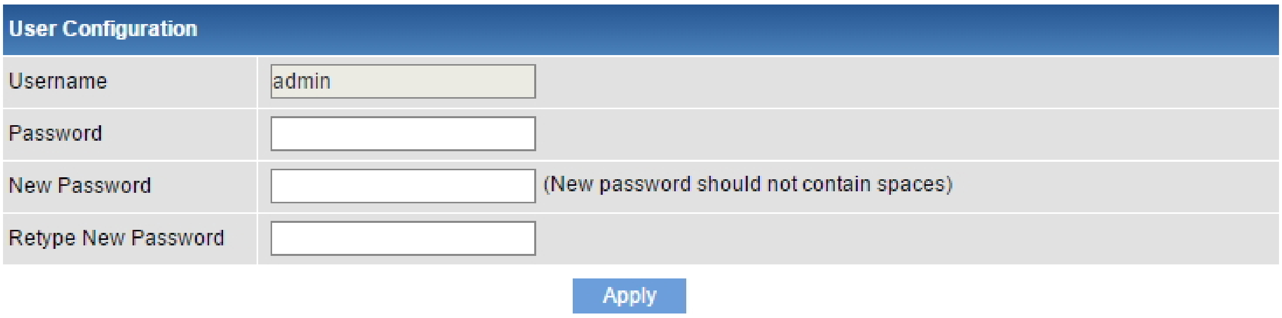
Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the table.

4.2.6 User Configuration

Configure user password in this page. After the setup is completed, please press the "**Apply**" button to take effect. Please login Web interface with a new user name and password; The User Configuration screen in Figure 4-2-6 appears.



User Configuration

Username	admin
Password	
New Password	(New password should not contain spaces)
Retype New Password	

Figure 4-2-6: User Configuration Page Screenshot

The page includes the following fields:

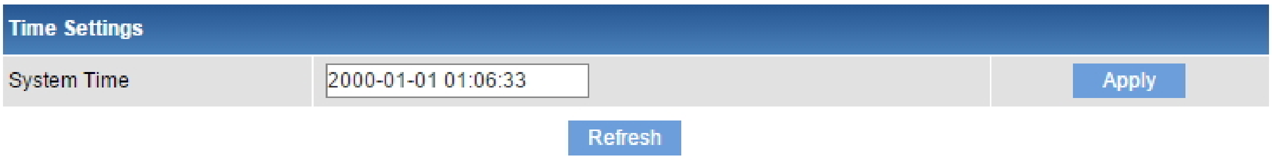
Object	Description
Password	Enter the user's current password here.
New Password	Enter the user's new password here. (Range: 0-16 characters plain text, case sensitive)
Retype New Password	Please enter the user's new password here again to confirm.

Buttons

Apply: Click to apply changes.

4.2.7 Time Settings

Configure Time Settings on this page. It is convenient for areas in close commercial or other communication to keep the same time. The Time Settings Configuration screen in Figure 4-2-7 appears



Time Settings

System Time	2000-01-01 01:06:33

Figure 4-2-7: Time Settings Page Screenshot

The page includes the following fields:

Object	Description
System Time	To set time manually. Example: 2015-01-28 14:23:05

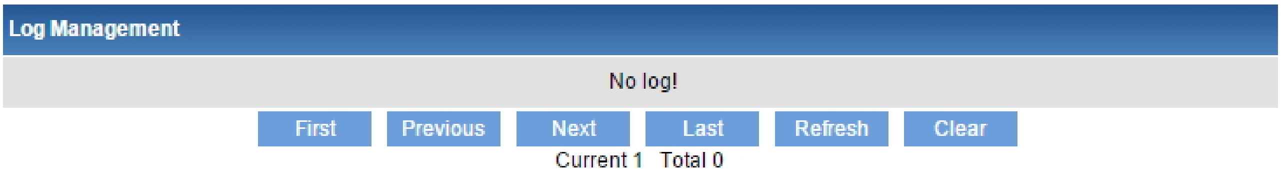
Buttons

Apply: Click to apply changes.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.2.8 Log Management

The Switch log management is provided here. The Log Management screen in Figure 4-2-8 appears.



Log Management

No log!

Current 1 Total 0

Figure 4-2-8: Log Management Page Screenshot

The page includes the following fields:

Object	Description
Log Management	Displays the current logging service status

Buttons

First: Click to move to the first page.

Previous: Click to move to the previous page.

Next: Click to move to the next page.

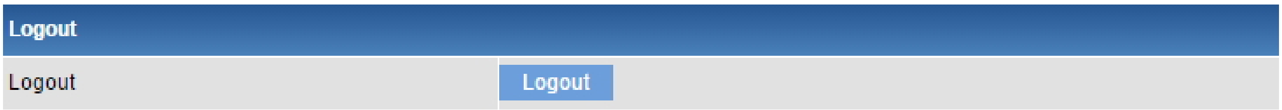
Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the table.

4.2.9 Logout

The Switch logout function is provided here. The Logout Configuration screen in Figure 4-2-9 appears.



Logout

Logout	Logout

Figure 4-2-9 Logout Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Logout**	Click to logout the Switch

Buttons

Logout: Click to log out switch.

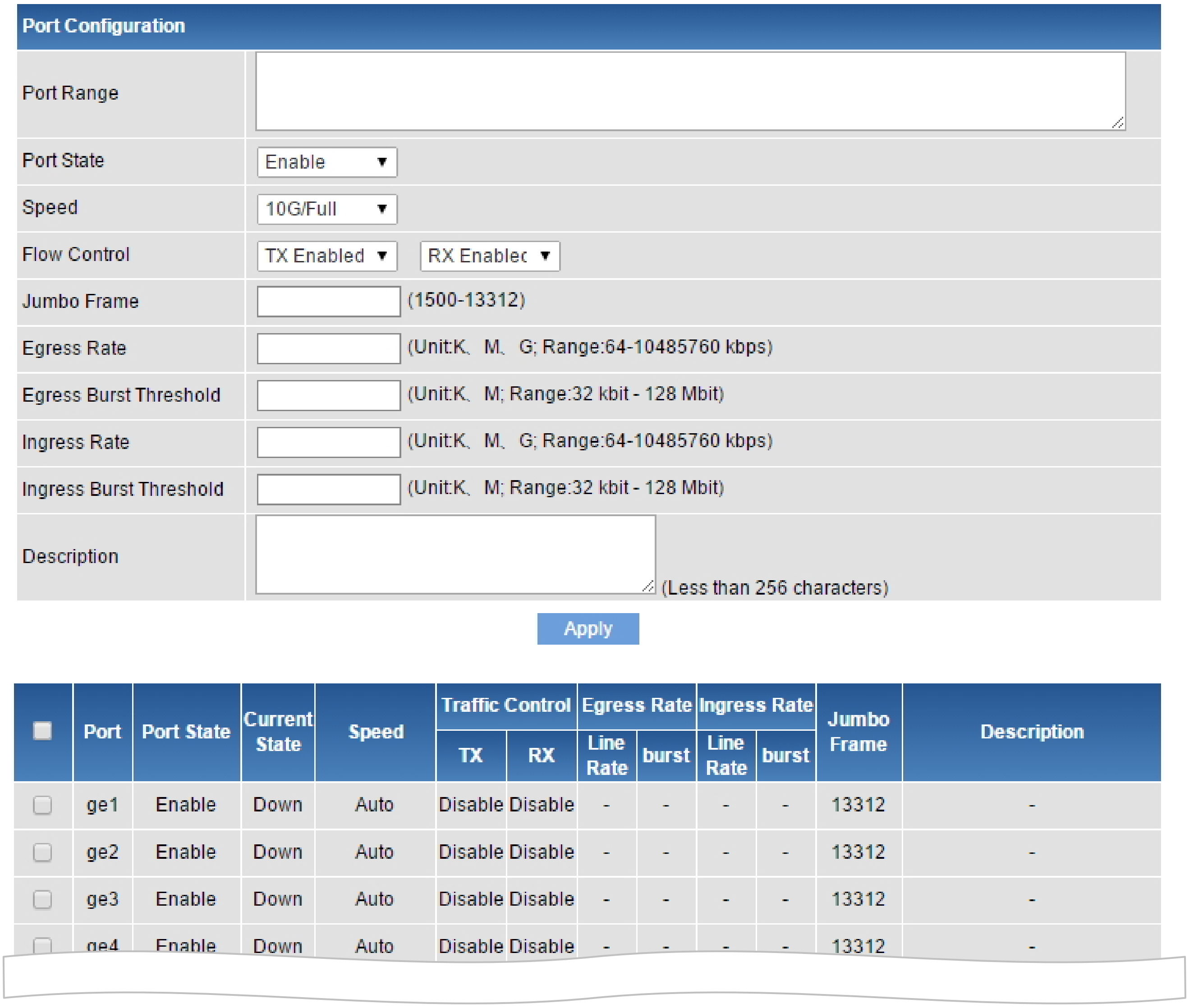
4.3 Port Management

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

■ **Port Configuration**	Configures port configuration settings
■ **Port Mirroring**	Sets the source and target ports for mirroring
■ **Storm Control**	Configures storm control settings

4.3.1 Port Configuration

This page displays and sets current port configurations and status. Ports can also be configured here. The table has one row for each port on the selected switch in a number of columns. The Port Configuration screen in Figure 4-3-1 appears.



Port Configuration

Port Range	
Port State	Enable ▼
Speed	10G/Full ▼
Flow Control	TX Enabled ▼ RX Enablec ▼
Jumbo Frame	(1500-13312)
Egress Rate	(Unit:K、M、G; Range:64-10485760 kbps)
Egress Burst Threshold	(Unit:K、M; Range:32 kbit - 128 Mbit)
Ingress Rate	(Unit:K、M、G; Range:64-10485760 kbps)
Ingress Burst Threshold	(Unit:K、M; Range:32 kbit - 128 Mbit)
Description	(Less than 256 characters)

□	Port	Port State	Current State	Speed	Traffic Control		Egress Rate		Ingress Rate		Jumbo Frame	Description
					TX	RX	Line Rate	burst	Line Rate	burst		
□	ge1	Enable	Down	Auto	Disable	Disable	-	-	-	-	13312	-
□	ge2	Enable	Down	Auto	Disable	Disable	-	-	-	-	13312	-
□	ge3	Enable	Down	Auto	Disable	Disable	-	-	-	-	13312	-
□	ge4	Enable	Down	Auto	Disable	Disable	-	-	-	-	13312	-

Figure 4-3-1: Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Range**	Select port number for below row table.
• **Port State**	Indicates the port state operation. Possible state are: **Enabled** - Start up the port manually. **Disabled** – Shut down the port manually.
• **Speed**	Select any available link speed and duplex for the given switch port. Draw the menu bar to select the mode. ■ **Auto** - Setup Auto negotiation. ■ **10G/Full** - Setup 10G Force Full-Duplex mode. ■ **1G/Full** - Setup 1G Force Full-Duplex mode. ■ **100M/Full** - Setup 100M Force Full-Duplex mode. ■ **100M/Half** - Setup 100M Force Half-Duplex mode.
• **Flow Control**	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. Current Rx column indicates whether pause frames on the port are obeyed. Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
• **Jumbo Frame**	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1500 bytes ~ 13312 bytes.
• **Egress Rate**	Configure the egress rate for the port. The default value is "unlimited". Valid values are in the range 64Kbps~10485760Kbps.
• **Egress Burst Threshold**	Configure the egress burst threshold for the port. The default value is "unlimited". Valid values are in the range 32Kbit~128Mbit.
• **Ingress Rate**	Configure the ingress rate for the port. The default value is "unlimited". Valid values are in the range 64Kbps~10485760Kbps.
• **Ingress Burst Threshold**	Configure the ingress burst threshold for the port. The default value is "unlimited". Valid values are in the range 32Kbit~128Mbit.
• **Description**	Indicate the port name

Buttons

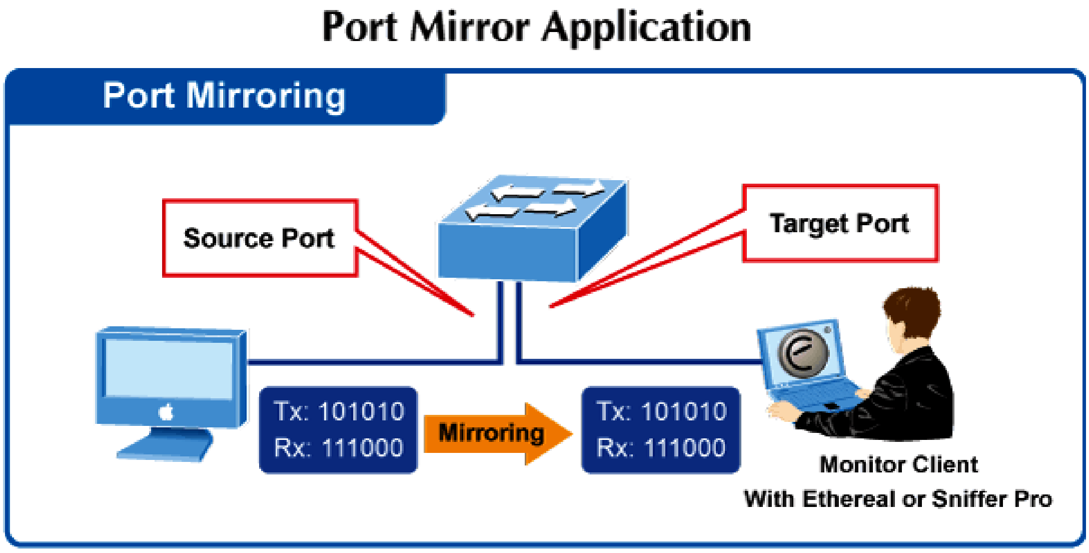
Apply: Click to apply changes.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.3.2 Port Mirroring

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

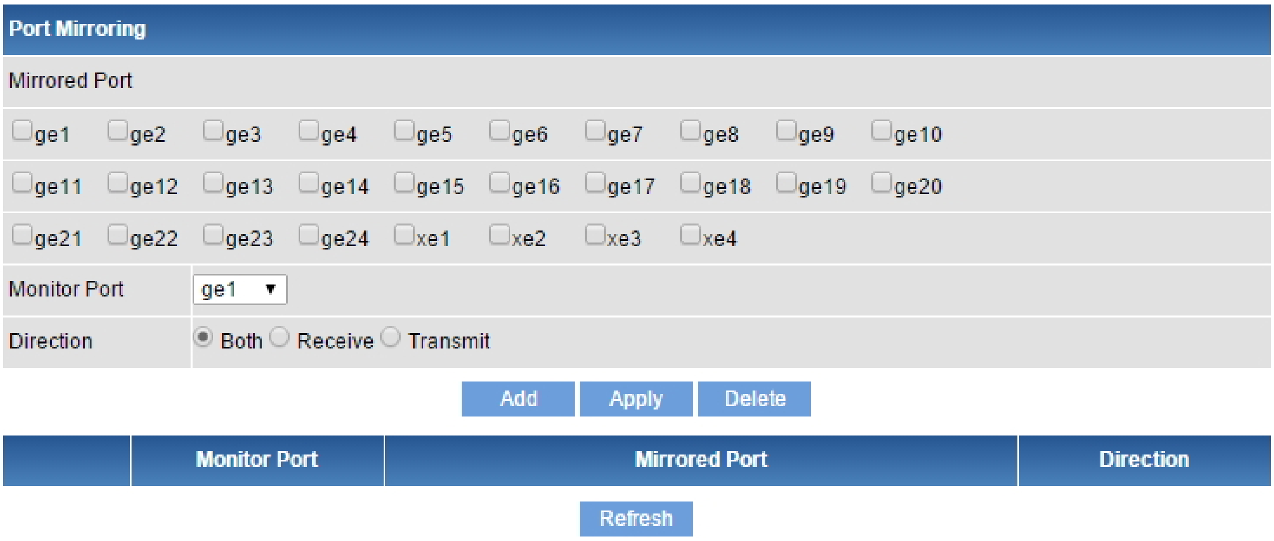
- To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.
- The Managed Switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to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



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

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

The Port Mirroring Configuration screen in Figure 4-3-2 appears.



Port Mirroring

Mirrored Port

□ge1	□ge2	□ge3	□ge4	□ge5	□ge6	□ge7	□ge8	□ge9	□ge10
□ge11	□ge12	□ge13	□ge14	□ge15	□ge16	□ge17	□ge18	□ge19	□ge20
□ge21	□ge22	□ge23	□ge24	□xe1	□xe2	□xe3	□xe4		

Monitor Port	ge1 ▾
Direction	● Both ○ Receive ○ Transmit

	Monitor Port	Mirrored Port	Direction

Figure 4-3-2: Port Mirroring Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mirrored Port**	Select mirrored port for below row table.
• **Monitor Port**	Select the port to mirror destination port.
• **Direction**	Select any available direction for the given switch port. Select the check box to select the mode. ■ **Both** - Frames received and transmitted at these ports are mirrored to the mirroring port. ■ **Receive** - Frames received at these ports are mirrored to the mirroring port. Frames transmitted are not mirrored.. ■ **Transmit** - Frames transmitted from these ports are mirrored to the mirroring port. Frames received are not mirrored.

Buttons

Add: Click to add a new data to the feature.

Delete: Click to delete a new data to the feature.

Apply: Click to apply changes.

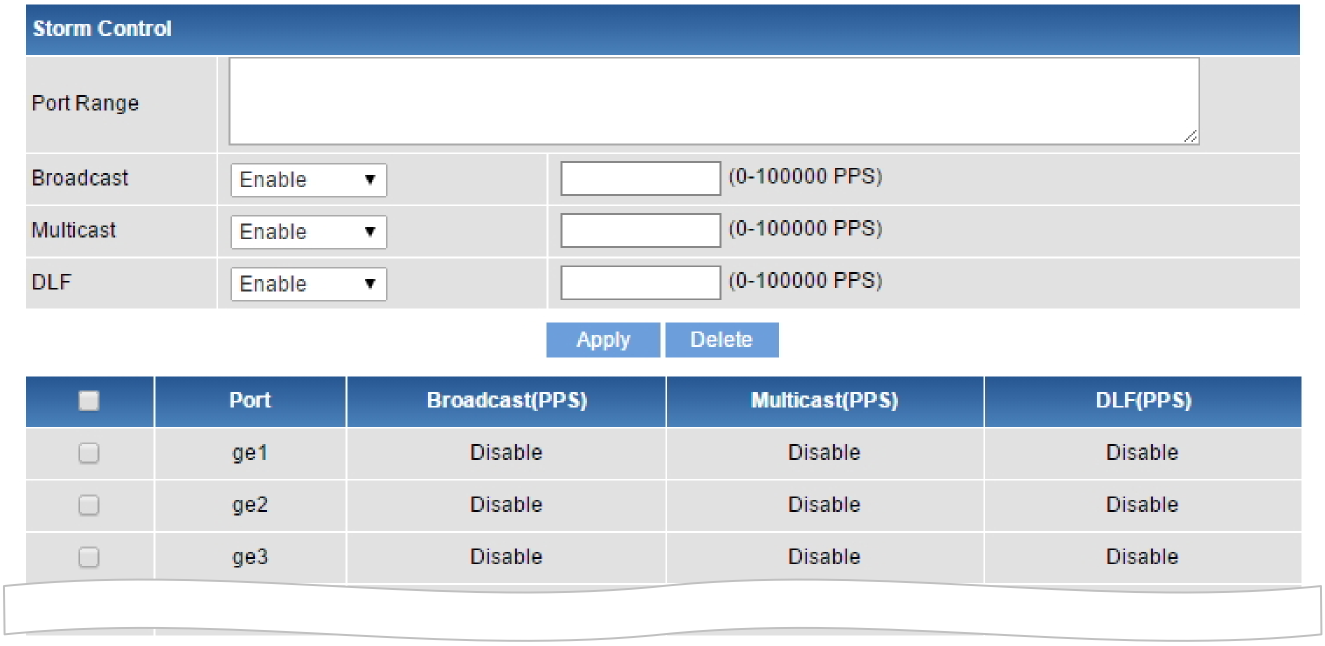
Refresh: Click to refresh the page; any changes made locally will be undone.

4.3.3 Storm Control

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

- **Broadcast** storm rate control
- **Destination Lookup Failure (DLF)** storm rate control
- **Multicast** storm rate control

The configuration indicates the permitted packet rate for unknown unicast, unknown multicast, or broadcast traffic across the switch. The Storm Control screen in Figure 4-3-3 appears.



Storm Control

Port Range		
Broadcast	Enable ▼	(0-100000 PPS)
Multicast	Enable ▼	(0-100000 PPS)
DLF	Enable ▼	(0-100000 PPS)

□	Port	Broadcast(PPS)	Multicast(PPS)	DLF(PPS)
□	ge1	Disable	Disable	Disable
□	ge2	Disable	Disable	Disable
□	ge3	Disable	Disable	Disable

Figure 4-3-3: Storm Control Configuration Page Screenshot

The page includes the following fields:

Object	Description
Port Range	Select port number for below row table.
Broadcast	Configures the Broadcast rate for the port. The default value is "unlimited". Valid values are in the range 0pps~100000pps.
Multicast	Configures the Multicast rate for the port. The default value is "unlimited". Valid values are in the range 0pps~100000pps.
DLF	Configures the Destination Lookup Failure (DLF) rate for the port. The default value is "unlimited". Valid values are in the range 0pps~100000pps.

Buttons

Delete: Click to delete a new data to the feature.

Apply: Click to apply changes.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.4 Link Aggregation

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

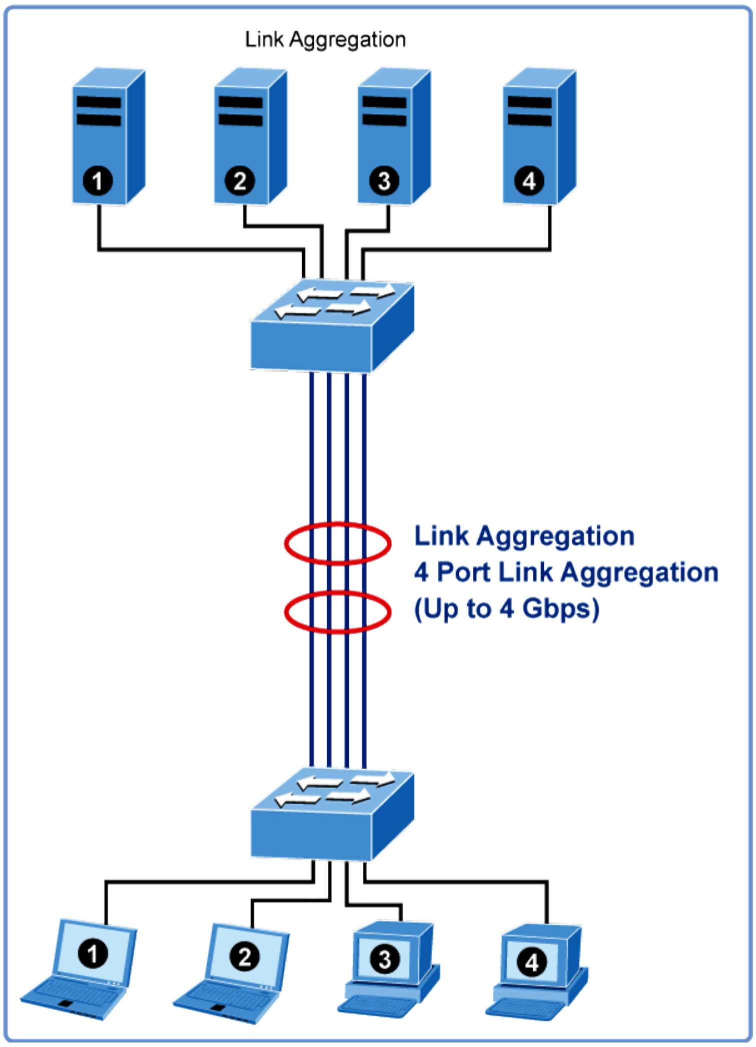
Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG can be of different media types (UTP/Fiber, or different fiber types) provided they operate at the same speed.

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

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

The device supports the following Aggregation links :

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



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

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

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

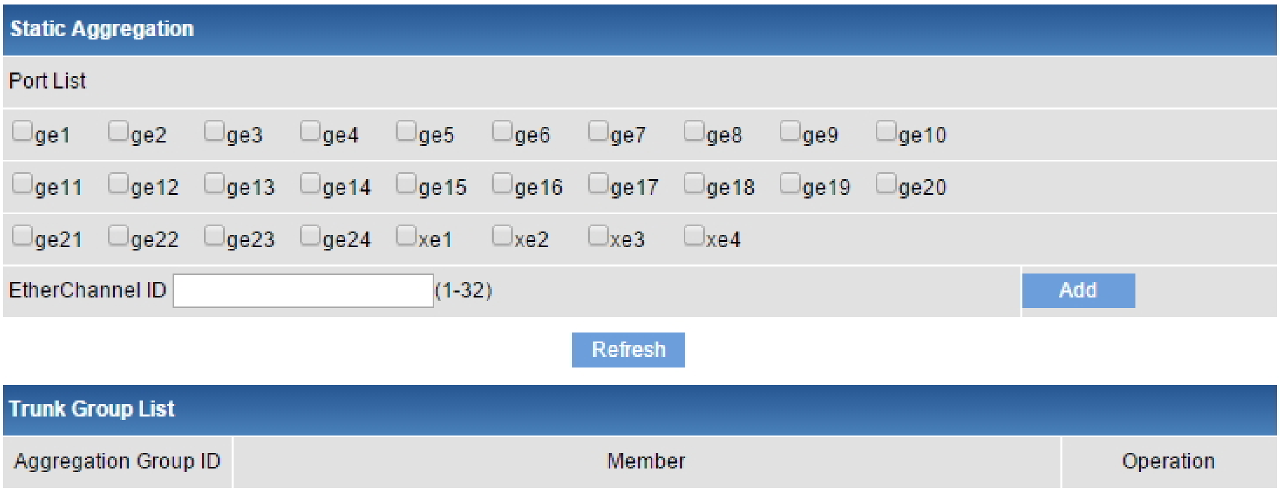
It allows a maximum of 8 ports to be aggregated at the same time. The Managed Switch supports Gigabit Ethernet ports (up to 8 groups). If the group is defined as an LACP static link aggregation group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports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

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

■ **Static Aggregation**	Configures Static Aggregation settings
■ **LACP Configuration**	Configures LACP configuration settings

4.4.1 Static Aggregation

This page displays and sets current port configurations for Static Aggregation. Ports can also be configured here. The Port Configuration screen in Figure 4-4-1 appears.



Static Aggregation

Port List

□ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10

□ge11 □ge12 □ge13 □ge14 □ge15 □ge16 □ge17 □ge18 □ge19 □ge20

□ge21 □ge22 □ge23 □ge24 □xe1 □xe2 □xe3 □xe4

EtherChannel ID ______ (1-32) Add

Refresh

Trunk Group List

Aggregation Group ID	Member	Operation

Figure 4-4-1: Static Aggregation Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number for below row table.
• **EtherChannel ID**	Indicates each static aggregation profile ID
• **Load Balancing**	Select load balancing algorithm for the given switch port. Select the check box to select the mode. ■ **Dst-ip** - The Destination IP address can be used to calculate the port for the frame. ■ **Dst-mac** – The Destination MAC address can be used to calculate the port for the frame. ■ **Src-dst-ip** - The IP address can be used to calculate the port for the frame. ■ **Src-dst-mac** - The MAC address can be used to calculate the port for the frame. ■ **Src-ip** - The Source IP address can be used to calculate the port for the frame. ■ **Src-mac** - The Source MAC address can be used to calculate the port for the frame.

Buttons

Add : Click to add a new data to the feature.

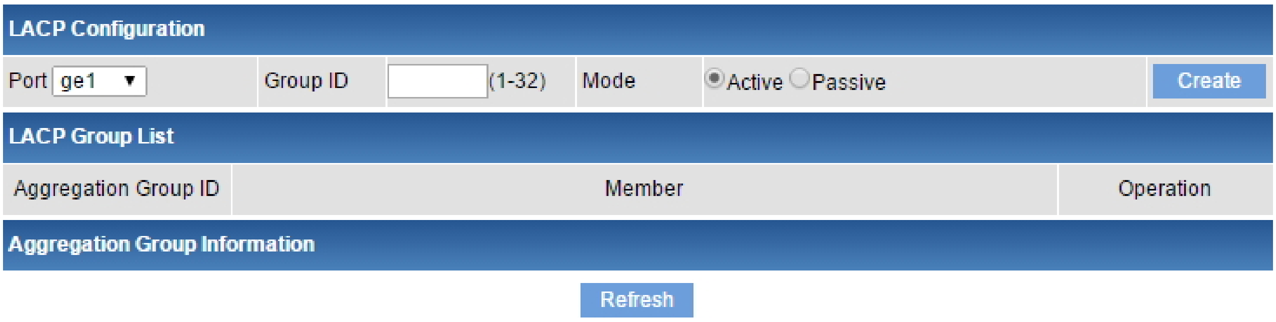
Delete : Click to delete a new data to the feature.

Apply : Click to apply changes.

Refresh : Click to refresh the page; any changes made locally will be undone.

4.4.2 LACP configuration

This page displays and sets the current port configurations for Static Aggregation. Ports can also be configured here. The LACP configuration screen in Figure 4-4-2 appears.



LACP Configuration

Port ge1 ▼ Group ID (1-32) Mode ● Active ○ Passive Create

LACP Group List

Aggregation Group ID	Member	Operation

Aggregation Group Information

Figure 4-4-2: LACP Configuration Page Screenshot

The displayed counters are:

Object	Description
• **Port**	Select port number for below row table.
• **Group ID**	Indicates each LACP profile ID
• **Mode**	Select LACP mode for the given switch port. Select the check box to select the mode. ■ **Active** - Set a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets. ■ **Passive** –Set a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.
• **Load Balancing**	Select load balancing algorithm for the given switch port. Select the check box to select the mode. ■ **Dst-ip** - The Destination IP address can be used to calculate the port for the frame. ■ **Dst-mac** – The Destination MAC address can be used to calculate the port for the frame. ■ **Src-dst-ip** - The IP address can be used to calculate the port for the frame. ■ **Src-dst-mac** - The MAC address can be used to calculate the port for the frame. ■ **Src-ip** - The Source IP address can be used to calculate the port for the frame. ■ **Src-mac** - The Source MAC address can be used to calculate the port for the frame.

Buttons

Create : Click to add a new data to the feature.

Delete : Click to delete a new data to the feature.

Apply : Click to apply changes.

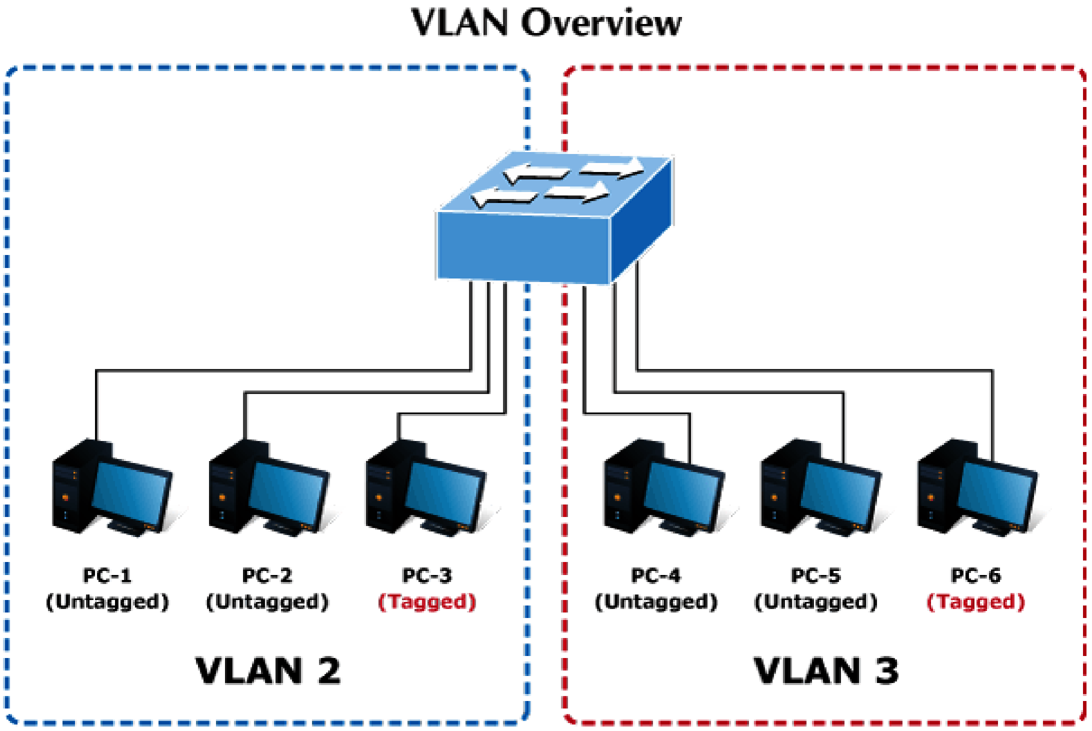
4.5 VLAN

4.5.1 VLAN Overview

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

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

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.



Note

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
2. The Managed Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

Note

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

This section has the following items:

■ **VLAN Configuration**	Configures mode and PVID on the VLAN port
■ **VLAN Membership**	Configures the VLAN membership
■ **VLAN Type Configuration**	Configures the VLAN type port setting
■ **IP Subnet-based VLAN**	Configures the IP subnet-based VLAN port setting
■ **MAC-based VLAN**	Configures the MAC-based VLAN port setting
■ **Protocol-based VLAN**	Configures the protocol VLAN port setting
■ **Private VLAN onfiguration**	Configures the private VLAN port setting

4.5.2 IEEE 802.1Q VLAN

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

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

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

This Managed Switch supports the following VLAN features:

- Up to 4000 VLANs based on the IEEE 802.1Q standard
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices

IEEE 802.1Q Standard

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

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

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

- The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.
- The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

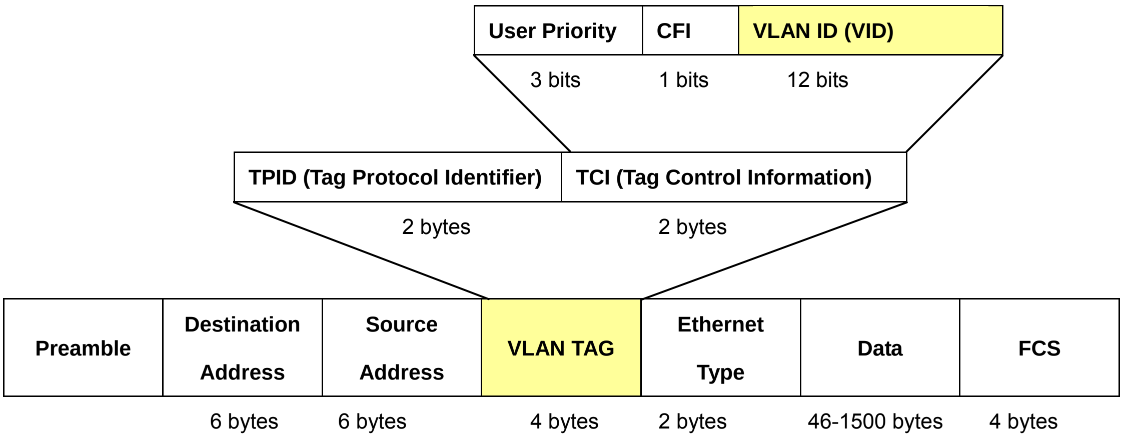
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN Tags

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

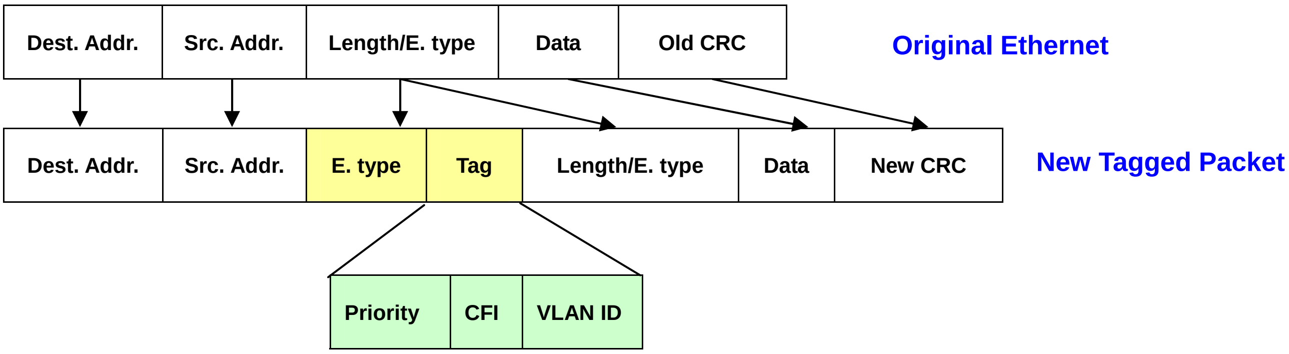
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag



Port VLAN ID

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

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

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

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

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

Default VLANs

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

Assigning Ports to VLANs

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

Note

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

VLAN Classification

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

Port Overlapping

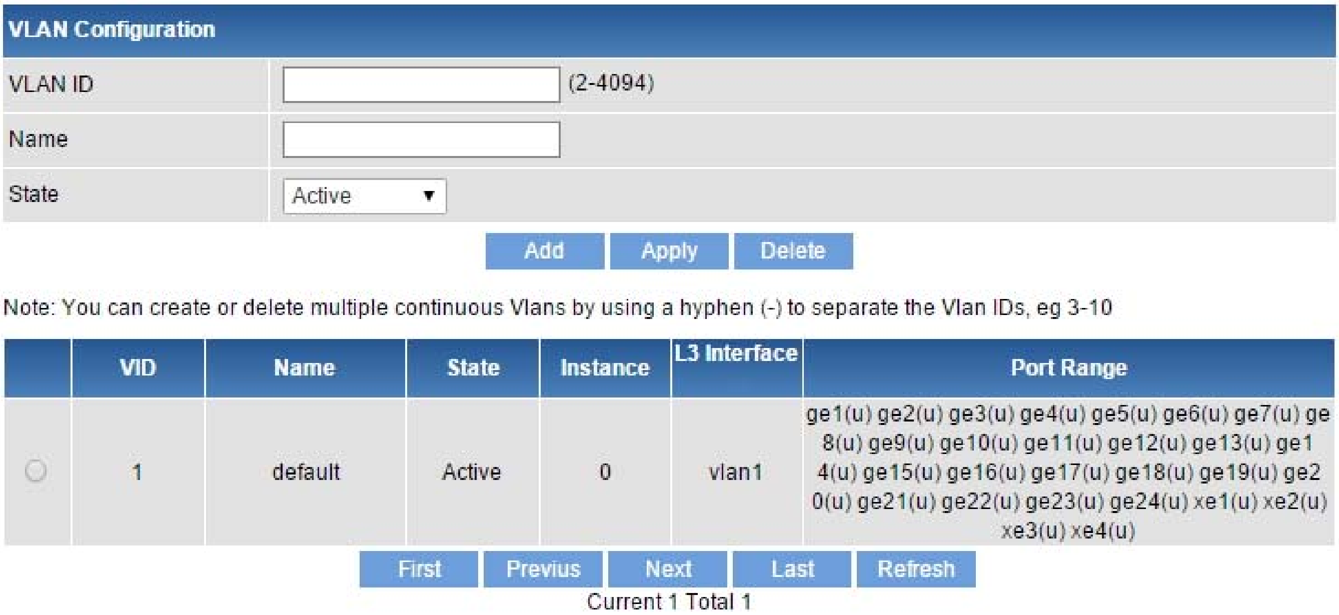
Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs

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

4.5.3 VLAN Configuration

Define VLAN ID state on this page. The VLAN Configuration screen in Figure 4-5-4 appears.



VLAN Configuration

VLAN ID	(2-4094)
Name	
State	Active ▼

Add Apply Delete

Note: You can create or delete multiple continuous Vlans by using a hyphen (-) to separate the Vlan IDs, eg 3-10

	VID	Name	State	Instance	L3 Interface	Port Range
○	1	default	Active	0	vlan1	ge1(u) ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u) xe1(u) xe2(u) xe3(u) xe4(u)

First Previus Next Last Refresh

Current 1 Total 1

Figure 4-5-4 : VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Indicates the ID of this particular VLAN.
• **Name**	Indicates the name of this particular VLAN.
• **State**	Select VLAN state for the given VLAN. Click the drop-down menu to select the mode. ■ **Active** – To active the given VLANs ■ **Suspend** – To shutdown the given VLANs

Buttons

Add : Click to add a new data to the feature.

Delete : Click to delete a new data to the feature.

First : Click to move to first page.

Previous : Click to move to previous page.

Next : Click to move to next page.

Last : Click to move to last page.

Refresh : Click to refresh the page; any changes made locally will be undone.

4.5.4 VLAN Membership

This page is used for configuring the Switch port VLAN. The VLAN per Port Configuration Page contains fields for managing ports that are part of a VLAN. The port **default VLAN ID** (**PVID**) is configured on the VLAN Port Configuration Page. All untagged packets arriving to the device are tagged by the ports PVID 1.

Understand nomenclature of the Switch

■ IEEE 802.1Q Tagged and Untagged

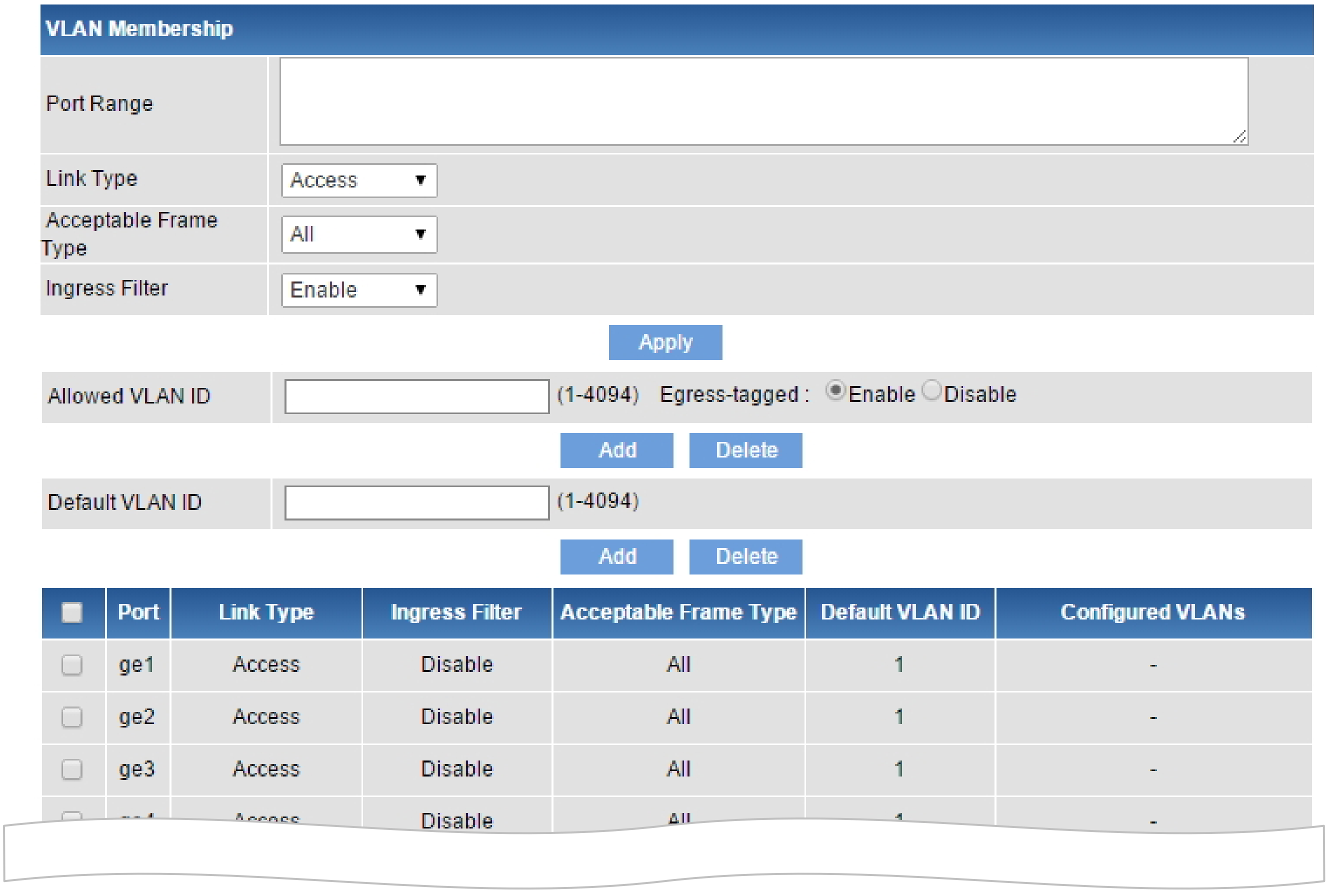
Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

- **Tagged:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
- **Untagged:** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

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

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

The VLAN membership screen in Figure 4-5-3 appears.



VLAN Membership

Port Range	
Link Type	Access ▾
Acceptable Frame Type	All ▾
Ingress Filter	Enable ▾

Allowed VLAN ID	(1-4094) Egress-tagged : ● Enable ○ Disable
Default VLAN ID	(1-4094)

□	Port	Link Type	Ingress Filter	Acceptable Frame Type	Default VLAN ID	Configured VLANs
□	ge1	Access	Disable	All	1	-
□	ge2	Access	Disable	All	1	-
□	ge3	Access	Disable	All	1	-
□	ge4	Access	Disable	All	1	-

Figure 4-5-3: VLAN Membership Page Screenshot

The page includes the following fields:

Object	Description
• **Port Range**	Select port number for below row table.
• **Link Type**	Set the port in access, trunk, hybrid and tunnel mode. ■ **Trunk** means the port allows traffic of multiple VLANs. ■ **Access** indicates the port belongs to one VLAN only. ■ **Hybrid** means the port allows the traffic of multi-VLANs to pass in tag or untag mode.
• **Acceptable Frame Type**	Determines whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. Options: ■ **All** ■ **Tag Only** By default, the field is set to **All**.
• **Ingress Filter**	• If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. • If ingress filtering is disabled, frames classified to a VLAN that the port is not a

	member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
• **Allowed VLAN ID**	Allows you to assign allowed VLAN ID to selected port.
• **Egress-tagged**	This option is only available for ports in Hybrid mode. Ports in Hybrid mode may control the tagging of frames on egress. ■ **<u>Tag All</u>** All frames, whether classified to the Port VLAN or not, are transmitted with a tag. ■ **<u>Untag All</u>** All frames, whether classified to the Port VLAN or not, are transmitted without a tag.
• **Default VLAN ID**	Allows you to assign PVID to selected port. The PVID will be inserted into all untagged frames entering the ingress port. The PVID must be the same as the VLAN ID that the port belongs to VLAN group, or the untagged traffic will be dropped. The range for the PVID is **1-4094.**

Buttons

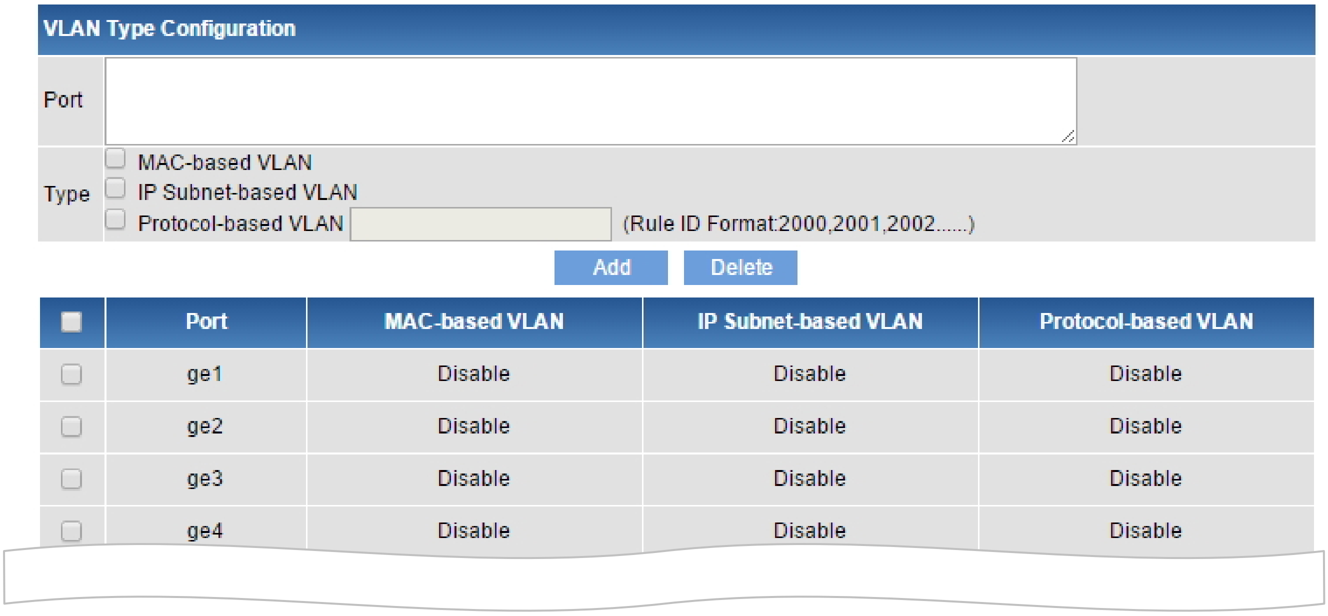
Add: Click to add a new data to the feature.

Delete: Click to delete a new data to the feature.

Apply: Click to apply changes.

4.5.5 VLAN Type Configuration

This page is used for configuring the Switch port VLAN type mode. The VLAN Type Configuration screen in Figure 4-5-4appears.



VLAN Type Configuration

Port

Type
□ MAC-based VLAN
□ IP Subnet-based VLAN
□ Protocol-based VLAN (Rule ID Format:2000,2001,2002......)

□	Port	MAC-based VLAN	IP Subnet-based VLAN	Protocol-based VLAN
□	ge1	Disable	Disable	Disable
□	ge2	Disable	Disable	Disable
□	ge3	Disable	Disable	Disable
□	ge4	Disable	Disable	Disable

Figure 4-5-4: VLAN Type Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number for below row table.
• **Type**	This type is only available for ports in the specific VLAN mode. ■ **IP Subnet-based VLAN** Any unicast IP address can be configured for the IP Subnet-based VLAN entry. No broadcast or multicast IP addresses are allowed. ■ **MAC-based VLAN** Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. ■ **Protocol-based VLAN** Add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switc.

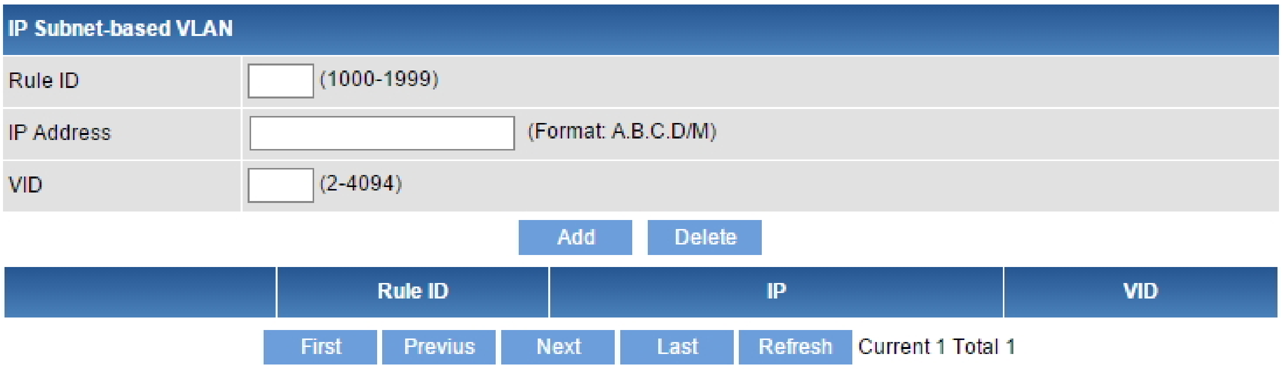
Buttons

Add : Click to add a new data to the feature.

Delete : Click to delete a new data to the feature.

4.5.6 IP Subnet-based VLAN

The IP Subnet-based VLAN entries can be configured here. The IP Subnet-based VLAN Configuration screen in Figure 4-5-5 appears.



IP Subnet-based VLAN

Rule ID	(1000-1999)
IP Address	(Format: A.B.C.D/M)
VID	(2-4094)

Add Delete

	Rule ID	IP	VID

First Previus Next Last Refresh Current 1 Total 1

Figure 4-5-5: IP Subnet-based VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Rule ID**	Indicates the VLAN rule ID. Legal values for a VLAN rule ID are 1000 through 1999.
• **IP Address**	Indicates the IP networks. Example: 10.10.10.1/24
• **VID**	Indicates the VLAN ID. Legal values for a VLAN rule ID are 2 through 4094.

Buttons

Add: Click to add a new data to the feature.

Delete: Click to delete a new data to the feature.

First: Click to move to the first page.

Previous: Click to move to the previous page.

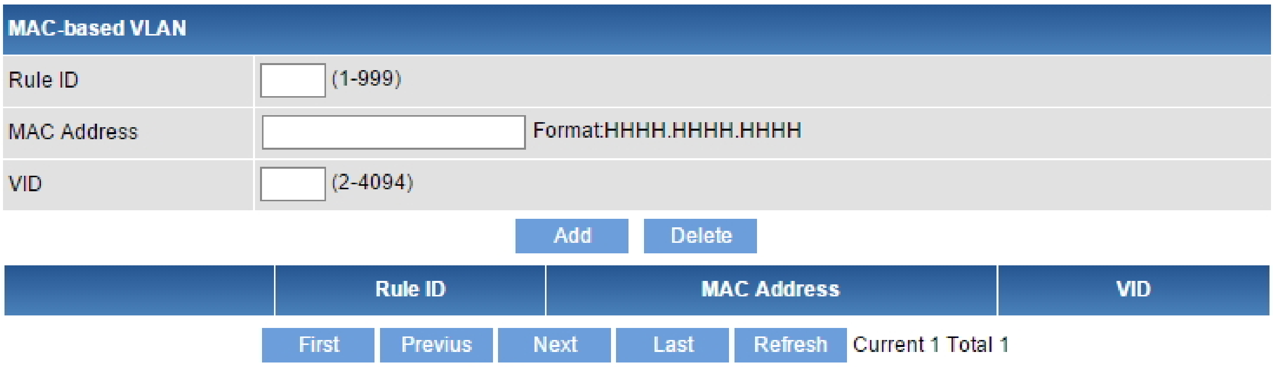
Next: Click to move to the next page.

Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.5.7 MAC-based VLAN

The MAC-based VLAN entries can be configured here. The MAC-based VLAN Configuration screen in Figure 4-5-6 appears.



MAC-based VLAN

Rule ID	(1-999)
MAC Address	Format:HHHH.HHHH.HHHH
VID	(2-4094)

	Rule ID	MAC Address	VID

Current 1 Total 1

Figure 4-5-6: MAC-based VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Rule ID**	Indicates the VLAN rule ID. Legal values for a VLAN rule ID are 1 through 999.
• **MAC Address**	Indicates the MAC address for the specific device in dotted Hexadecimal notation Example: 0030.4FAA.BBEE
• **VID**	Indicates the VLAN ID. Legal values for a VLAN rule ID are 2 through 4094.

Buttons

Add : Click to add a new data to the feature.

Delete : Click to delete a new data to the feature.

First : Click to move to the first page.

Previous : Click to move to the previous page.

Next : Click to move to the next page.

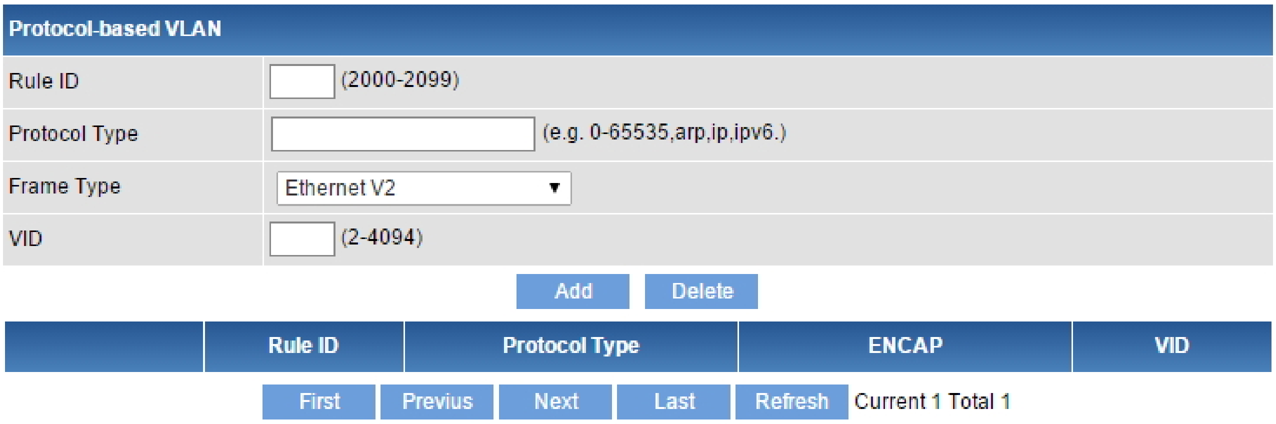
Last : Click to move to the last page.

Refresh : Click to refresh the page; any changes made locally will be undone.

4.5.8 Protocol-based VLAN

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this Managed Switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets. The Protocol-based VLAN Configuration screen in Figure 4-5-7 appears.



Protocol-based VLAN

Rule ID	(2000-2099)
Protocol Type	(e.g. 0-65535,arp,ip,ipv6.)
Frame Type	Ethernet V2 ▼
VID	(2-4094)

	Rule ID	Protocol Type	ENCAP	VID

Current 1 Total 1

Figure 4-5-7: Protocol-based VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Rule ID**	Indicates the VLAN rule ID. Legal values for a VLAN rule ID are 1000 through 1999.
• **Protocol Type**	Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Example: 0-65535, arp, ip, ipv6
• **IP Address**	Frame Type can have one of the following values: ■ **Ethernet V2** ■ **IEEE802.3 LLC** ■ **IEEE802.3 LLC + SNAP** **Note:** On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.
• **VID**	Indicates the VLAN ID. Legal values for a VLAN rule ID are 2 through 4094.

Buttons

Add: Click to add a new data to the feature.

Delete: Click to delete a new data to the feature.

First: Click to move to the first page.

Previous: Click to move to the previous page.

Next: Click to move to the next page.

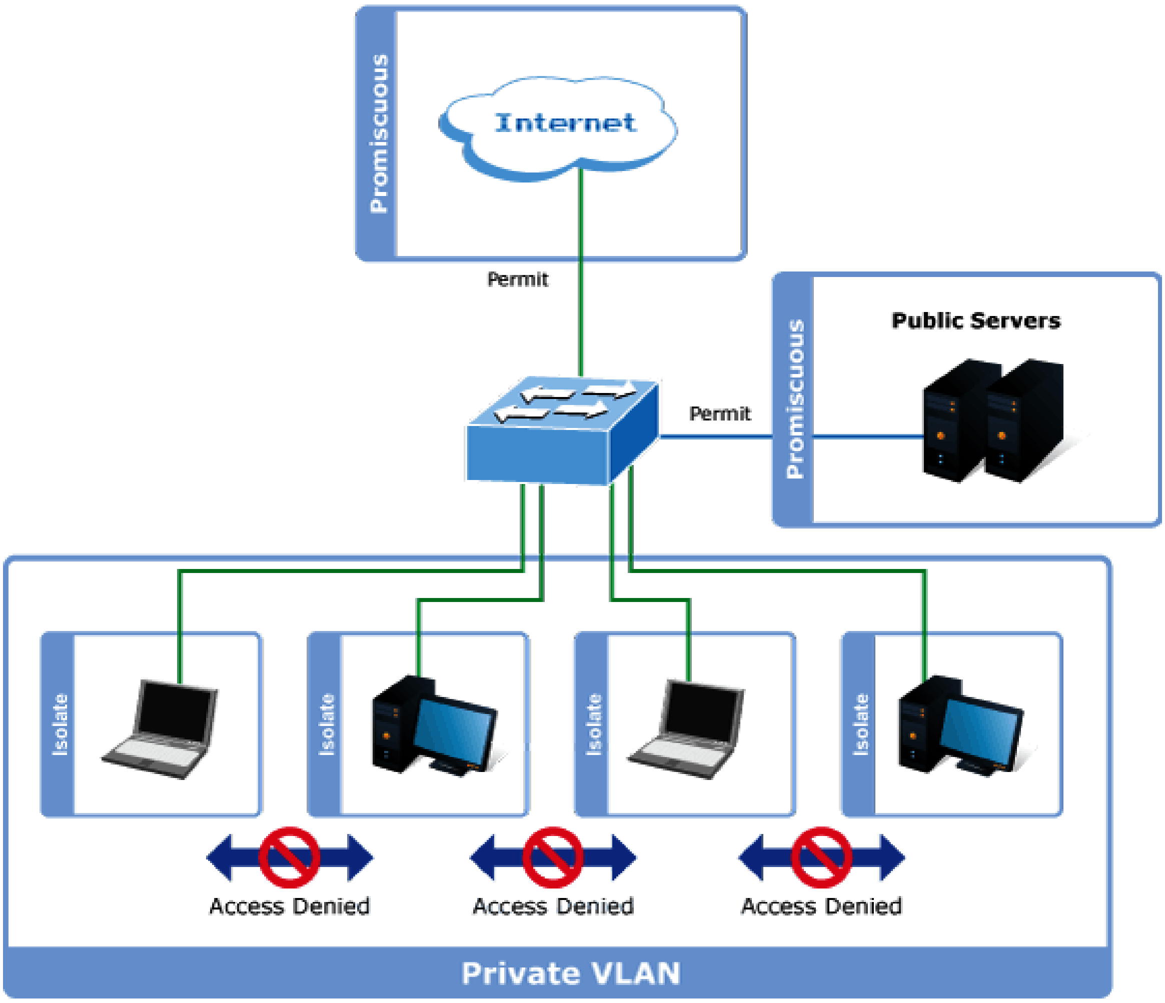
Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.5.9 Private VLAN Configuration

When a VLAN is configured to be a private VLAN, communication between ports within that VLAN can be prevented. Two application examples are provided in this section:

- Customers connected to an ISP can be members of the same VLAN, but they are not allowed to communicate with each other within that VLAN.
- Servers in a farm of web servers in a Demilitarized Zone (DMZ) are allowed to communicate with the outside world and with database servers on the inside segment, but are not allowed to communicate with each other



For private VLANs to be applied, the switch must first be configured for standard VLAN operation When this is in place, one or more of the configured VLANs can be configured as private VLAN ports. Ports in a private VLAN fall into one of these three groups:

- **Promiscuous ports**

— Ports from which traffic can be forwarded to all ports in the private VLAN

— Ports which can receive traffic from all ports in the private VLAN

- **Isolated ports**

— Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN

— Ports which can receive traffic from only promiscuous ports in the private VLAN

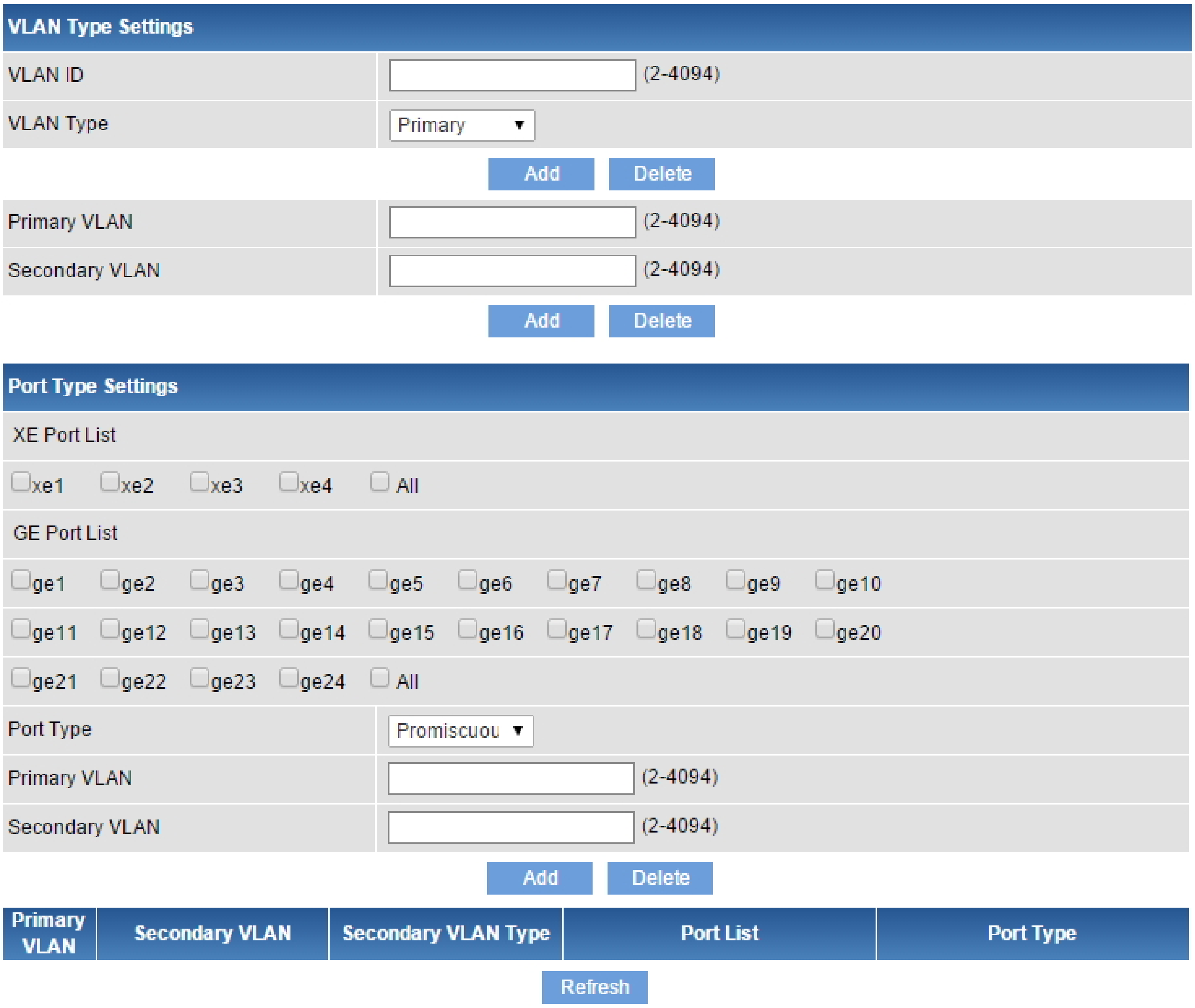
- **Commuity ports**

— Ports from which traffic can only be forwarded to same community VLAN in the private VLAN

— Ports which can receive traffic from only promiscuous ports in the private VLAN

The configuration of promiscuous and isolated ports applies to all private VLANs. When traffic comes in on a promiscuous port in a private VLAN, the VLAN mask from the VLAN table is applied. When traffic comes in on an isolated port, the private VLAN mask is applied in addition to the VLAN mask from the VLAN table. This reduces the ports to which forwarding can be done to just the promiscuous ports within the private VLAN.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN. The Private VLAN Configuration screen in Figure 4-5-8 appears.



VLAN Type Settings

VLAN ID	(2-4094)
VLAN Type	Primary ▾

Primary VLAN	(2-4094)
Secondary VLAN	(2-4094)

Port Type Settings

XE Port List

□xe1 □xe2 □xe3 □xe4 □ All

GE Port List

□ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10

□ge11 □ge12 □ge13 □ge14 □ge15 □ge16 □ge17 □ge18 □ge19 □ge20

□ge21 □ge22 □ge23 □ge24 □ All

Port Type	Promiscuou ▾
Primary VLAN	(2-4094)
Secondary VLAN	(2-4094)

Primary VLAN	Secondary VLAN	Secondary VLAN Type	Port List	Port Type

Figure 4-5-8: IP Subnet-based VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Indicates the VLAN rule ID. Legal values for a VLAN rule ID are 2 through 4094.
• **VLAN type**	This type is only available for ports in the private VLAN mode. ■ **Promiscuous** The promiscuous port can communicate with all interfaces. ■ **Isolated** It can communicate with associated promiscuous ports only ■ **Community** It can communicate with associated promiscuous ports only with same community VLAN
• **Primary VLAN**	Indicates the Primary VLAN rule ID. Legal values for a VLAN rule ID are 2 through 4094.
• **Secondary VLAN**	Indicates the Secondary VLAN rule ID. Legal values for a VLAN rule ID are 2 through 4094.
• **Port List**	Select port number for below row table.
• **Port type**	This type is only available for ports in the Primary and Secondary VLANs. ■ **Promiscuous** It can communicate with only one primary VLAN and multiple secondary VLANs ■ **Host** It can make secondary VLANs to communicate outside the private VLAN

Buttons

Add: Click to add a new data to the feature.

Delete: Click to delete a new data to the feature.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.5.10 VLAN Setting Example:

- Separate VLANs

- 802.1Q VLAN Trunk

4.5.10.1 Two Separate 802.1Q VLANs

The diagram shows how the Managed Switch handles Tagged and Untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separate VLANs. Each VLAN isolates network traffic so only members of the VLAN receive traffic from the same VLAN members. The screen in Figure 4-5-20 appears and Table 4-5-2 describes the port configuration of the Managed Switches.

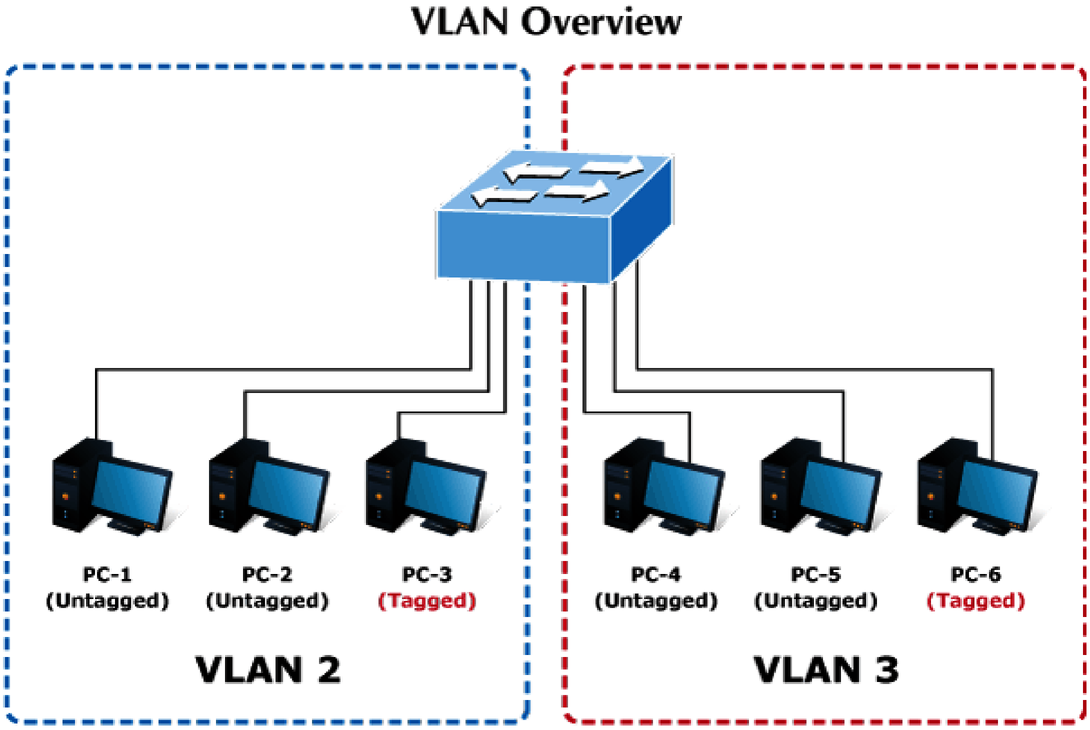


Figure 4-5-20 Two Separate VLAN Diagrams

VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 2	2	Port-1,Port-2	Port-3
VLAN Group 3	3	Port-4,Port-5	Port-6

Table 4-5-2 VLAN and Port Configuration

The scenario described as follows:

■ Untagged packet entering VLAN 2

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

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

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

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

■ Tagged packet entering VLAN 2

1. While **[PC-3]** transmits a **tagged** packet with **VLAN Tag=2** entering **Port-3**. **[PC-1]** and **[PC-2]** will receive the packet through **Port-1** and **Port-2**.
2. While the packet leaves **Port-1** and **Port-2**, it will be stripped away its tag becoming an **untagged** packet.

■ Untagged packet entering VLAN 3

1. While **[PC-4]** transmits an **untagged** packet entering **Port-4**, the switch will tag it with a **VLAN Tag=3**. **[PC-5]** and **[PC-6]** will receive the packet through **Port-5** and **Port-6**.
2. While the packet leaves **Port-5**, it will be stripped away its tag becoming an **untagged** packet.
3. While the packet leaves **Port-6**, it will keep as a **tagged** packet with **VLAN Tag=3**.

Note

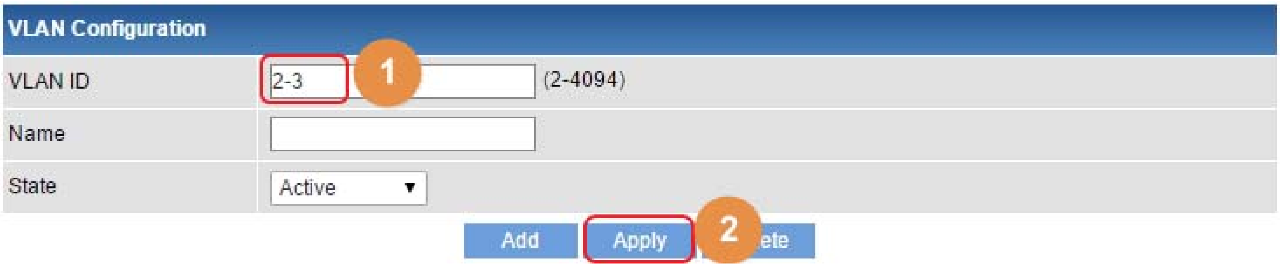
In this example, VLAN Group 1 is set as default VLAN, but only focuses on VLAN 2 and VLAN 3 traffic flow.

Setup Steps

3. Create VLAN Group 2 and 3

Step1: Add VLAN group 2 and group 3

Step2: Apply the settings



VLAN Configuration

VLAN ID	2-3 (2-4094)
Name	
State	Active ▼

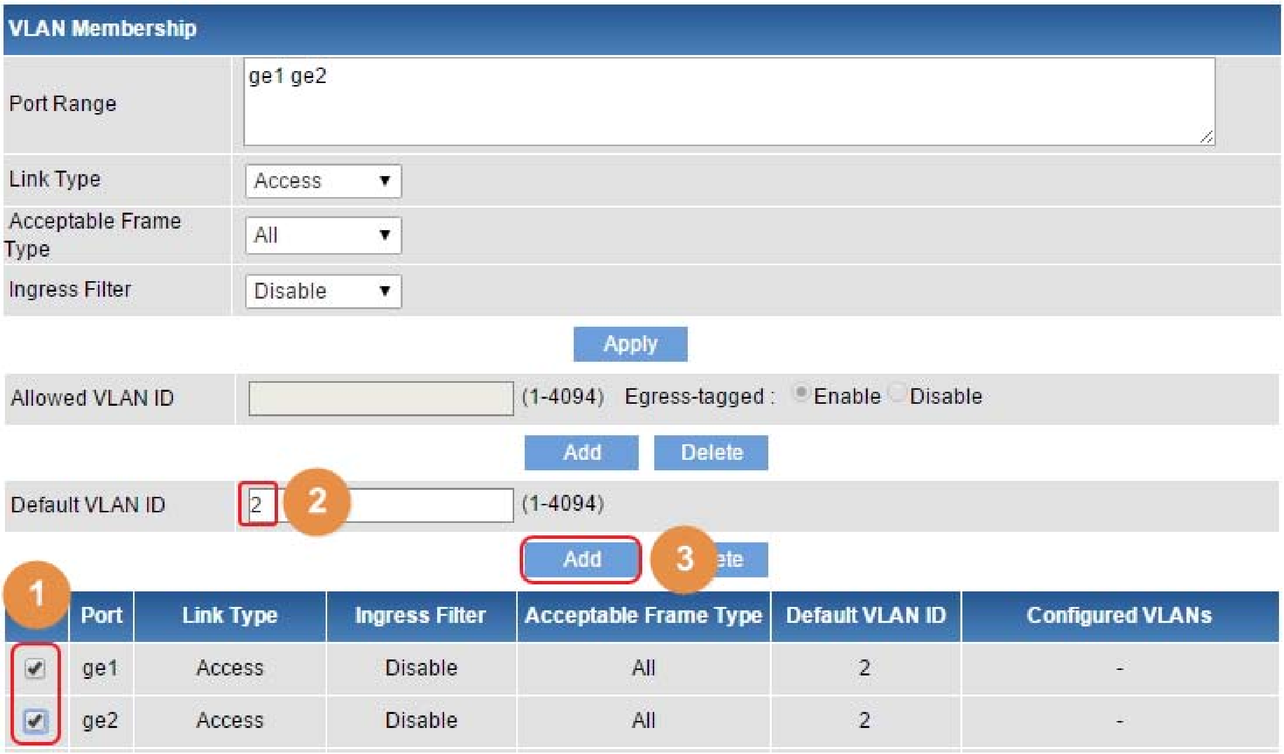
3. Assign VLAN mode, allowed VLAN ID and PVID to each port:

A. Settings of Port-1 and Port-2

Step1: Select Port-1 and Port-2

Step2: Link Type = Access, Default VLAN ID=*2*

Step3: Add the settings



VLAN Membership

Port Range: ge1 ge2

Link Type: Access

Acceptable Frame Type: All

Ingress Filter: Disable

Allowed VLAN ID: (1-4094) Egress-tagged : ● Enable ○ Disable

Default VLAN ID: 2 (1-4094)

	Port	Link Type	Ingress Filter	Acceptable Frame Type	Default VLAN ID	Configured VLANs
☑	ge1	Access	Disable	All	2	-
☑	ge2	Access	Disable	All	2	-

B. Settings of Port-3

Step1: Select Port-3

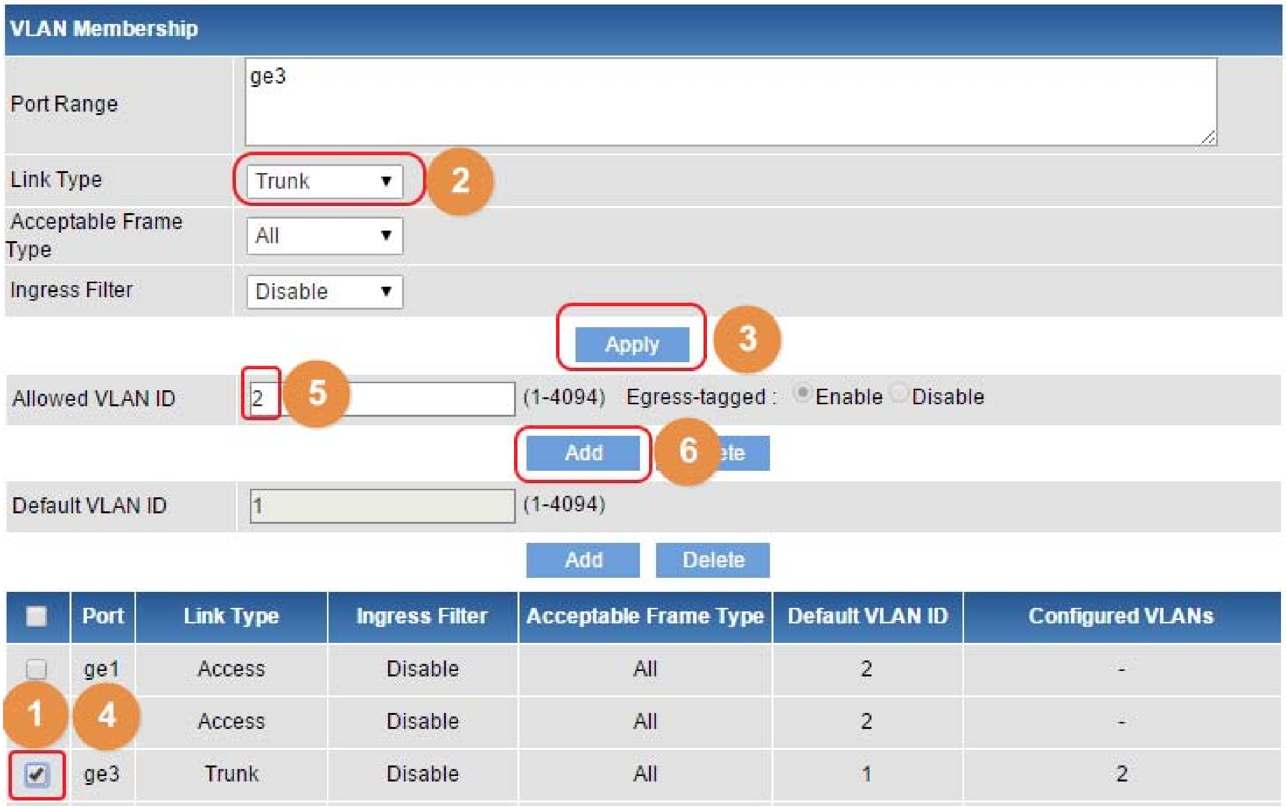
Step2: Link Type = Trunk

Step3: Apply the settings

Step4: Select Port-3

Step5: Allowed VLAN ID=*2*

Step6: Add the settings



VLAN Membership

Port Range: ge3

Link Type: Trunk

Acceptable Frame Type: All

Ingress Filter: Disable

Allowed VLAN ID: 2 (1-4094) Egress-tagged : ● Enable ○ Disable

Default VLAN ID: 1 (1-4094)

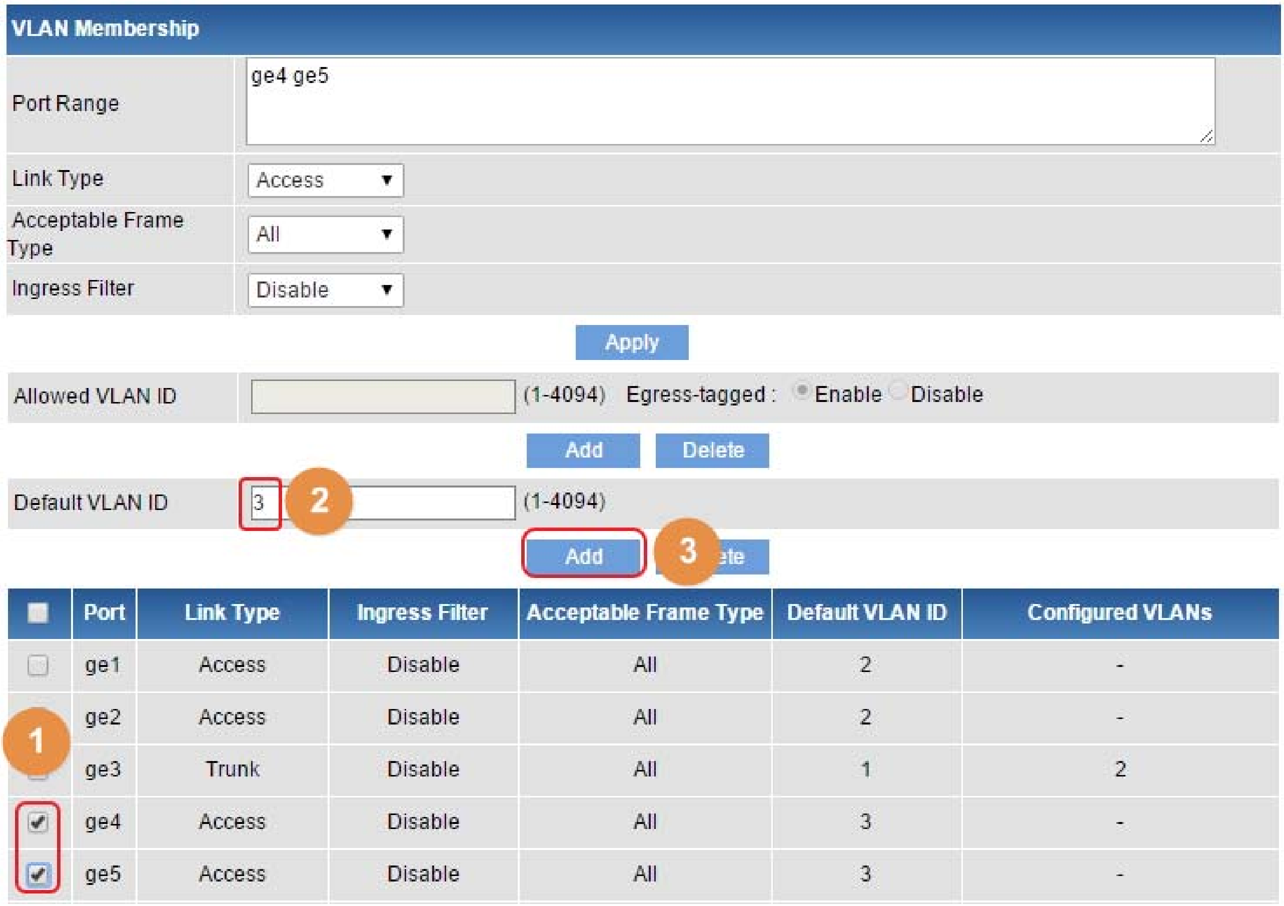
□	Port	Link Type	Ingress Filter	Acceptable Frame Type	Default VLAN ID	Configured VLANs
□	ge1	Access	Disable	All	2	-
		Access	Disable	All	2	-
☑	ge3	Trunk	Disable	All	1	2

C. Settings of Port-4 and Port-5

Step1: Select Port-4 and Port-5

Step2: Link Type = Access, Default VLAN ID=*3*

Step3: Add the settings



VLAN Membership

Port Range	ge4 ge5
Link Type	Access ▼
Acceptable Frame Type	All ▼
Ingress Filter	Disable ▼

Apply

Allowed VLAN ID: (1-4094) Egress-tagged : ● Enable ○ Disable

Add Delete

Default VLAN ID: 3 (1-4094)

Add Delete

□	Port	Link Type	Ingress Filter	Acceptable Frame Type	Default VLAN ID	Configured VLANs
□	ge1	Access	Disable	All	2	-
□	ge2	Access	Disable	All	2	-
□	ge3	Trunk	Disable	All	1	2
☑	ge4	Access	Disable	All	3	-
☑	ge5	Access	Disable	All	3	-

D. Settings of Port-6

Step1: Select Port-6

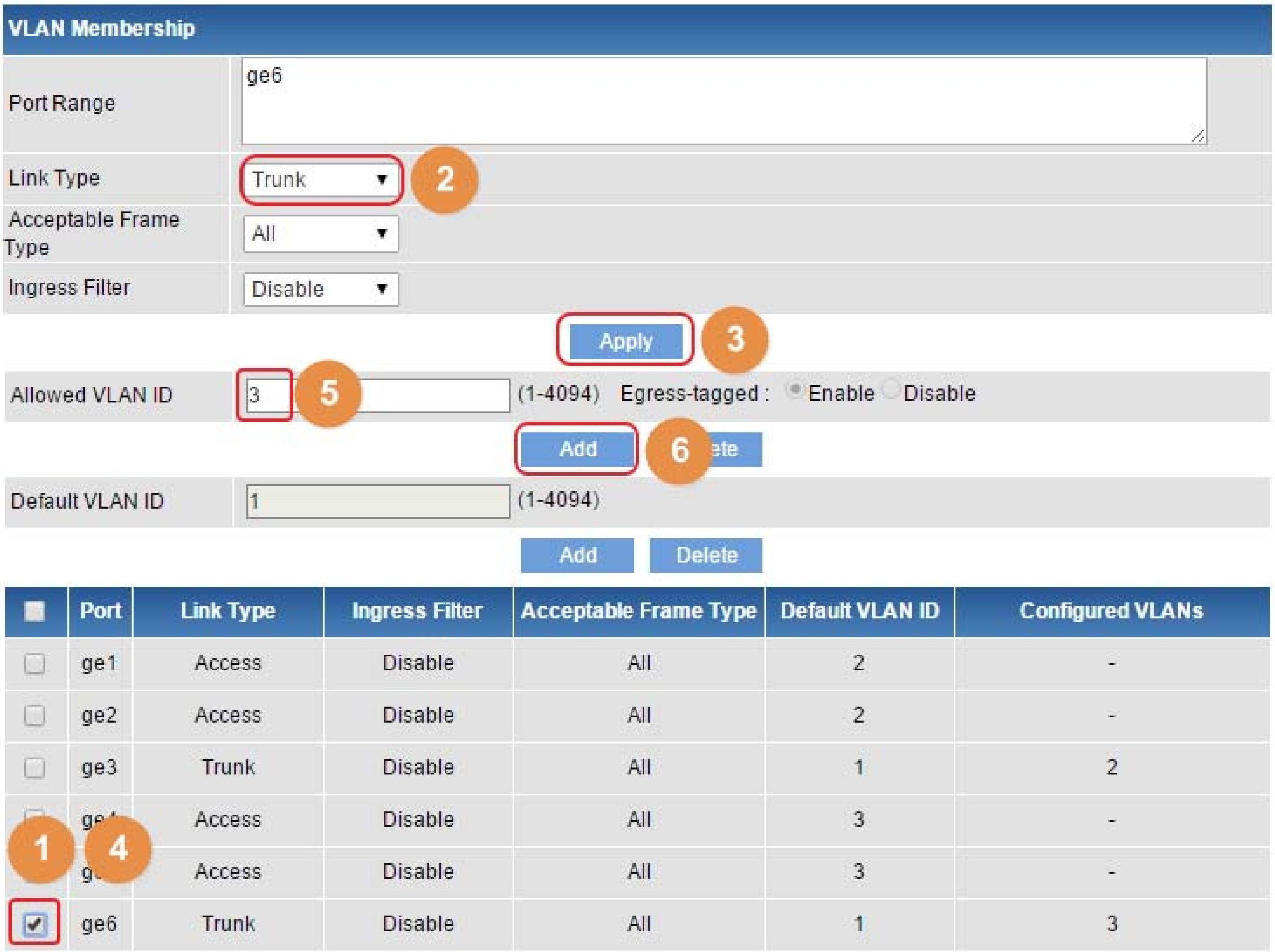
Step2: Link Type = Trunk

Step3: Apply the settings

Step4: Select Port-6

Step5: Allowed VLAN ID=*3*

Step6: Add the settings



Port Range	ge6
Link Type	Trunk
Acceptable Frame Type	All
Ingress Filter	Disable
Allowed VLAN ID	3 (1-4094) Egress-tagged : ● Enable ○ Disable
Default VLAN ID	1 (1-4094)

□	Port	Link Type	Ingress Filter	Acceptable Frame Type	Default VLAN ID	Configured VLANs
□	ge1	Access	Disable	All	2	-
□	ge2	Access	Disable	All	2	-
□	ge3	Trunk	Disable	All	1	2
□	ge4	Access	Disable	All	3	-
	ge5	Access	Disable	All	3	-
☑	ge6	Trunk	Disable	All	1	3

4.5.10.2 VLAN Trunking between two 802.1Q aware switches

In most cases, they are used for "**Uplink**" to other switches. VLANs are separated at different switches, but they need to access other switches within the same VLAN group. The screen in Figure 4-5-21 appears.

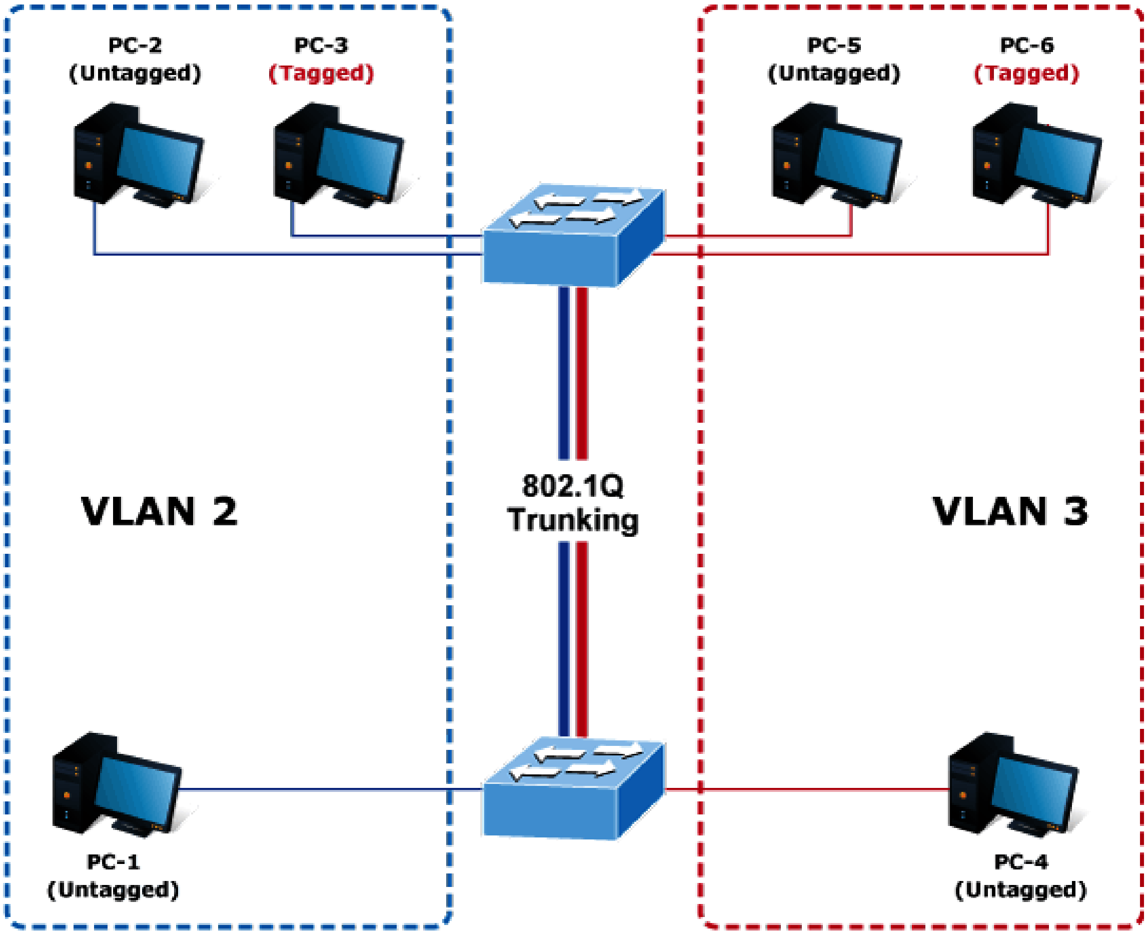


Figure 4-5-21 VLAN Trunking between Two 802.1Q Diagrams

VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 2	2	Port-1,Port-2	Port-3
VLAN Group 3	3	Port-4,Port-5	Port-6
802.1Q Trunking (VLAN Group 2, VLAN Group 3)	1	-	Port-7

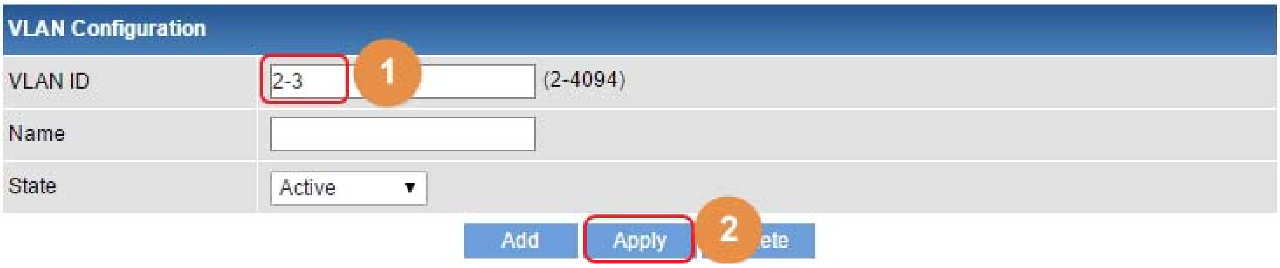
Table 4-5-3 VLAN and Port Configuration

Setup Steps

1. Create VLAN Group 2 and 3

Step1: Add VLAN group 2 and group 3

Step2: Apply the settings



VLAN Configuration

VLAN ID	2-3 (2-4094)
Name	
State	Active

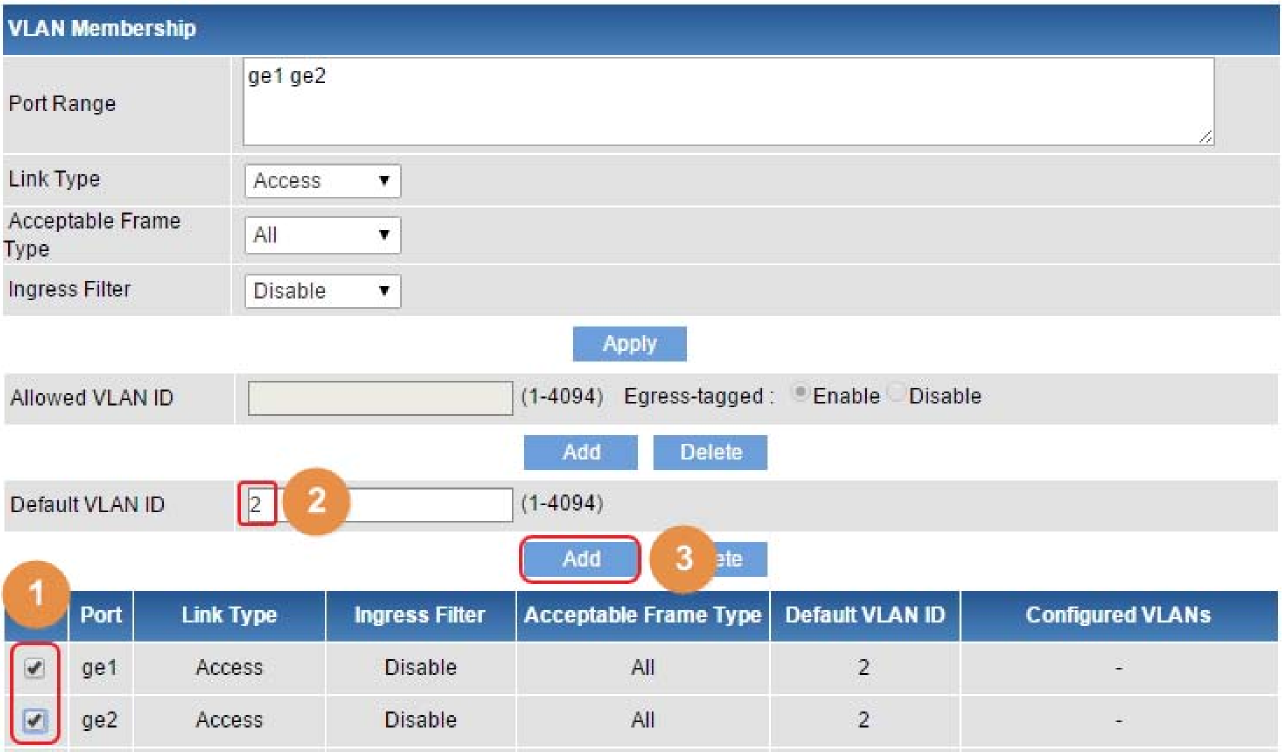
2. Assign VLAN mode, allowed VLAN ID and PVID to each port 1 ~ Port 6:

A. Settings of Port-1 and Port-2

Step1: Select Port-1 and Port-2

Step2: Link Type = Access, Default VLAN ID=*2*

Step3: Add the settings



VLAN Membership

Port Range	ge1 ge2
Link Type	Access
Acceptable Frame Type	All
Ingress Filter	Disable
Allowed VLAN ID	(1-4094) Egress-tagged : ● Enable ○ Disable
Default VLAN ID	2 (1-4094)

	Port	Link Type	Ingress Filter	Acceptable Frame Type	Default VLAN ID	Configured VLANs
☑	ge1	Access	Disable	All	2	-
☑	ge2	Access	Disable	All	2	-

B. Settings of Port-3

Step1: Select Port-3

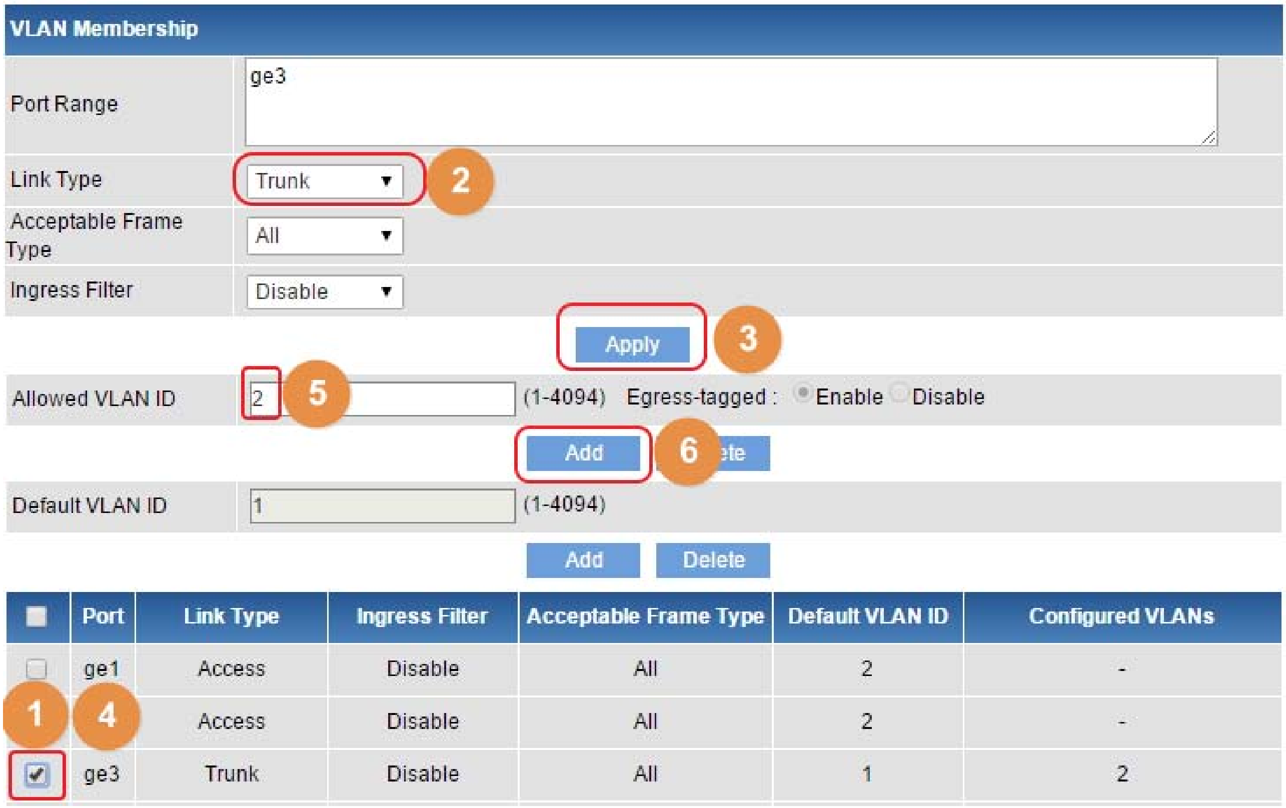
Step2: Link Type = Trunk

Step3: Apply the settings

Step4: Select Port-3

Step5: Allowed VLAN ID=*2*

Step6: Add the settings



VLAN Membership

Port Range	ge3
Link Type	Trunk ▾
Acceptable Frame Type	All ▾
Ingress Filter	Disable ▾
Allowed VLAN ID	2 (1-4094) Egress-tagged : ● Enable ○ Disable
Default VLAN ID	1 (1-4094)

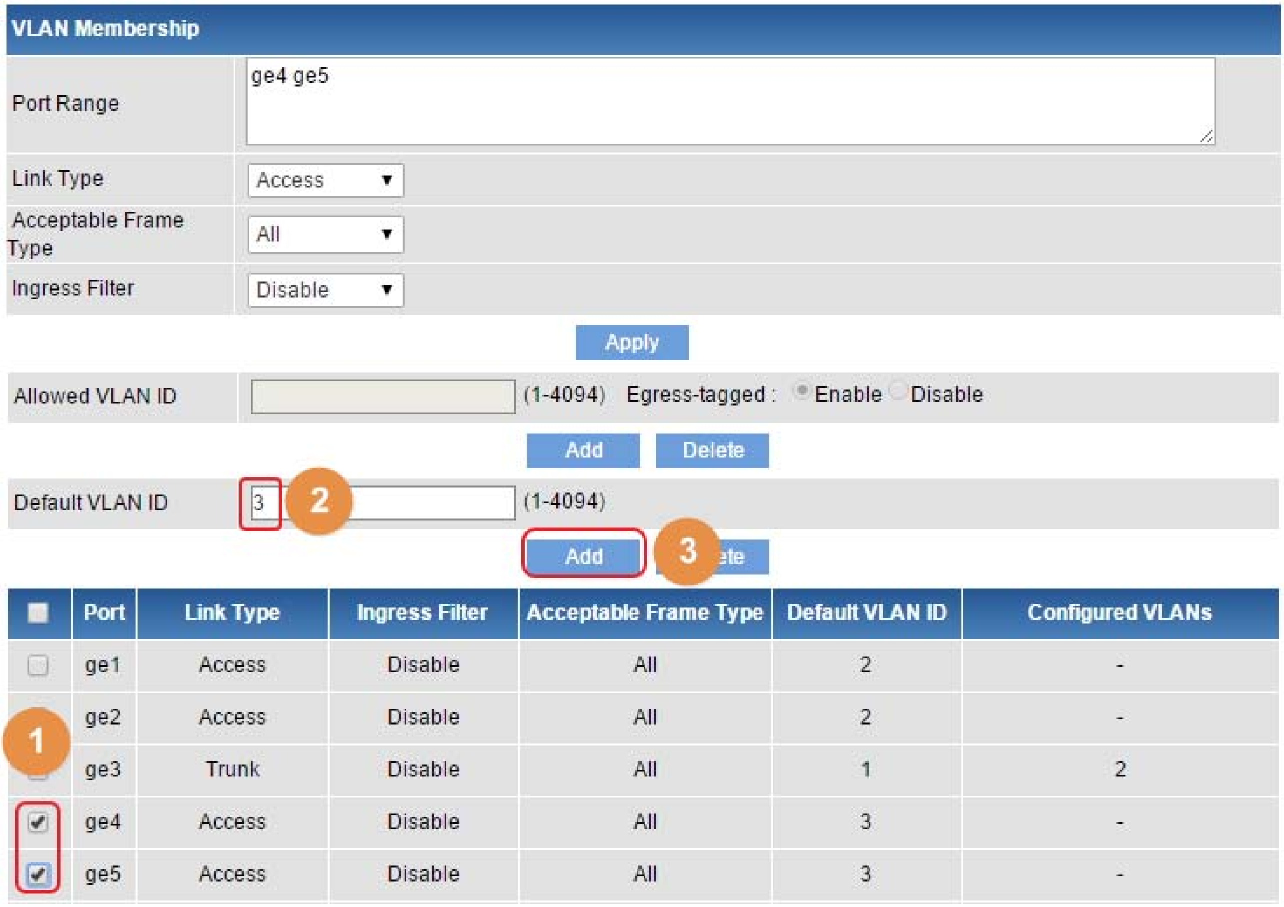
□	Port	Link Type	Ingress Filter	Acceptable Frame Type	Default VLAN ID	Configured VLANs
□	ge1	Access	Disable	All	2	-
		Access	Disable	All	2	-
☑	ge3	Trunk	Disable	All	1	2

C. Settings of Port-4 and Port-5

Step1: Select Port-4 and Port-5

Step2: Link Type = Access, Default VLAN ID=*3*

Step3: Add the settings



VLAN Membership

Port Range	ge4 ge5
Link Type	Access ▾
Acceptable Frame Type	All ▾
Ingress Filter	Disable ▾
Allowed VLAN ID	(1-4094) Egress-tagged : ● Enable ○ Disable
Default VLAN ID	3 (1-4094)

□	Port	Link Type	Ingress Filter	Acceptable Frame Type	Default VLAN ID	Configured VLANs
□	ge1	Access	Disable	All	2	-
	ge2	Access	Disable	All	2	-
	ge3	Trunk	Disable	All	1	2
☑	ge4	Access	Disable	All	3	-
☑	ge5	Access	Disable	All	3	-

D. Settings of Port-6

Step1: Select Port-6

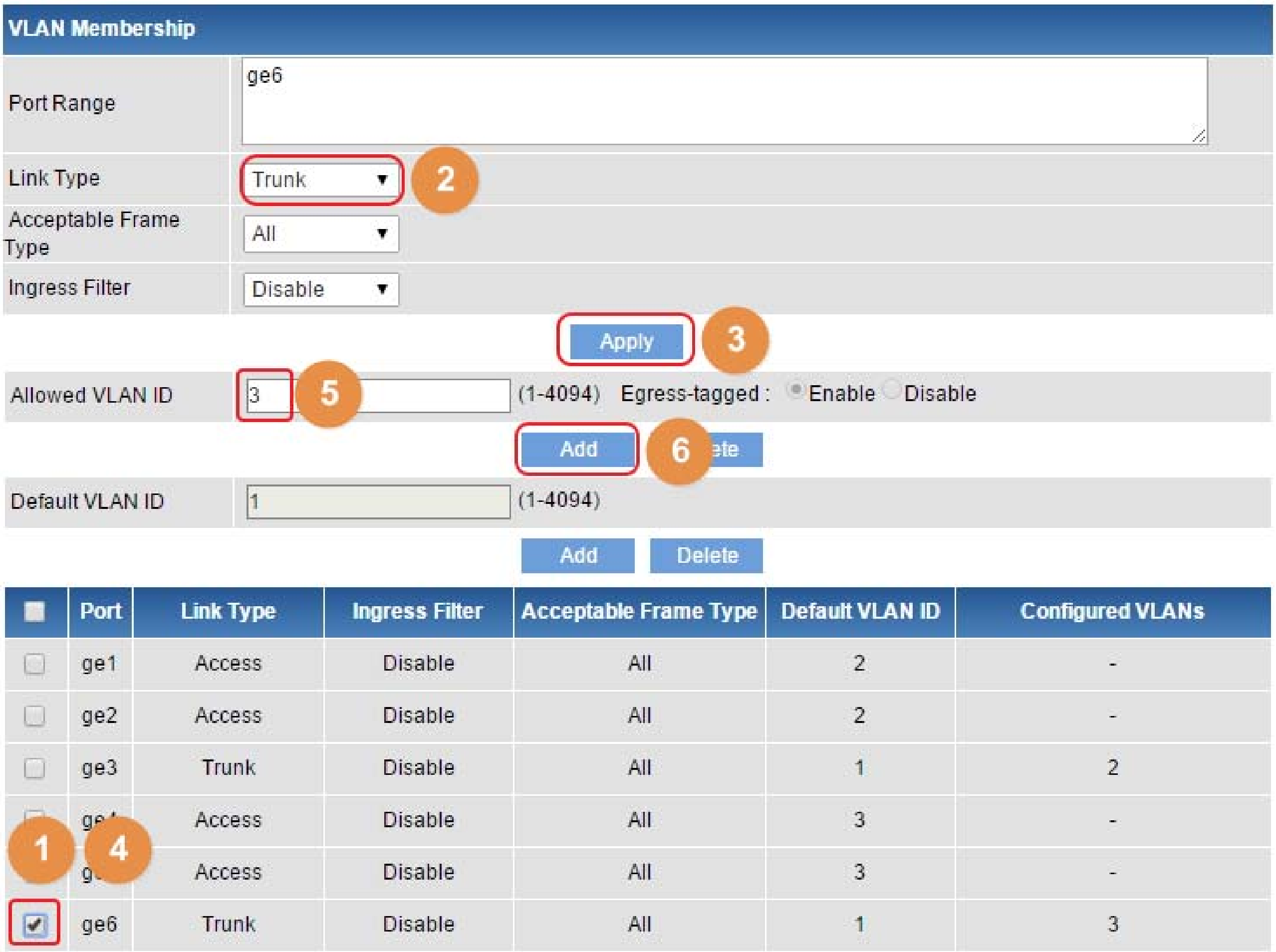
Step2: Link Type = Trunk

Step3: Apply the settings

Step4: Select Port-6

Step5: Allowed VLAN ID=*3*

Step6: Add the settings



VLAN Membership

Port Range: ge6

Link Type: Trunk

Acceptable Frame Type: All

Ingress Filter: Disable

Allowed VLAN ID: 3 (1-4094) Egress-tagged : ● Enable ○ Disable

Default VLAN ID: 1 (1-4094)

□	Port	Link Type	Ingress Filter	Acceptable Frame Type	Default VLAN ID	Configured VLANs
□	ge1	Access	Disable	All	2	-
□	ge2	Access	Disable	All	2	-
□	ge3	Trunk	Disable	All	1	2
□	ge4	Access	Disable	All	3	-
□	ge5	Access	Disable	All	3	-
☑	ge6	Trunk	Disable	All	1	3

3. Assign VLAN mode, allowed VLAN ID and PVID to each Uplink port 7:

Step1: Select Port-7

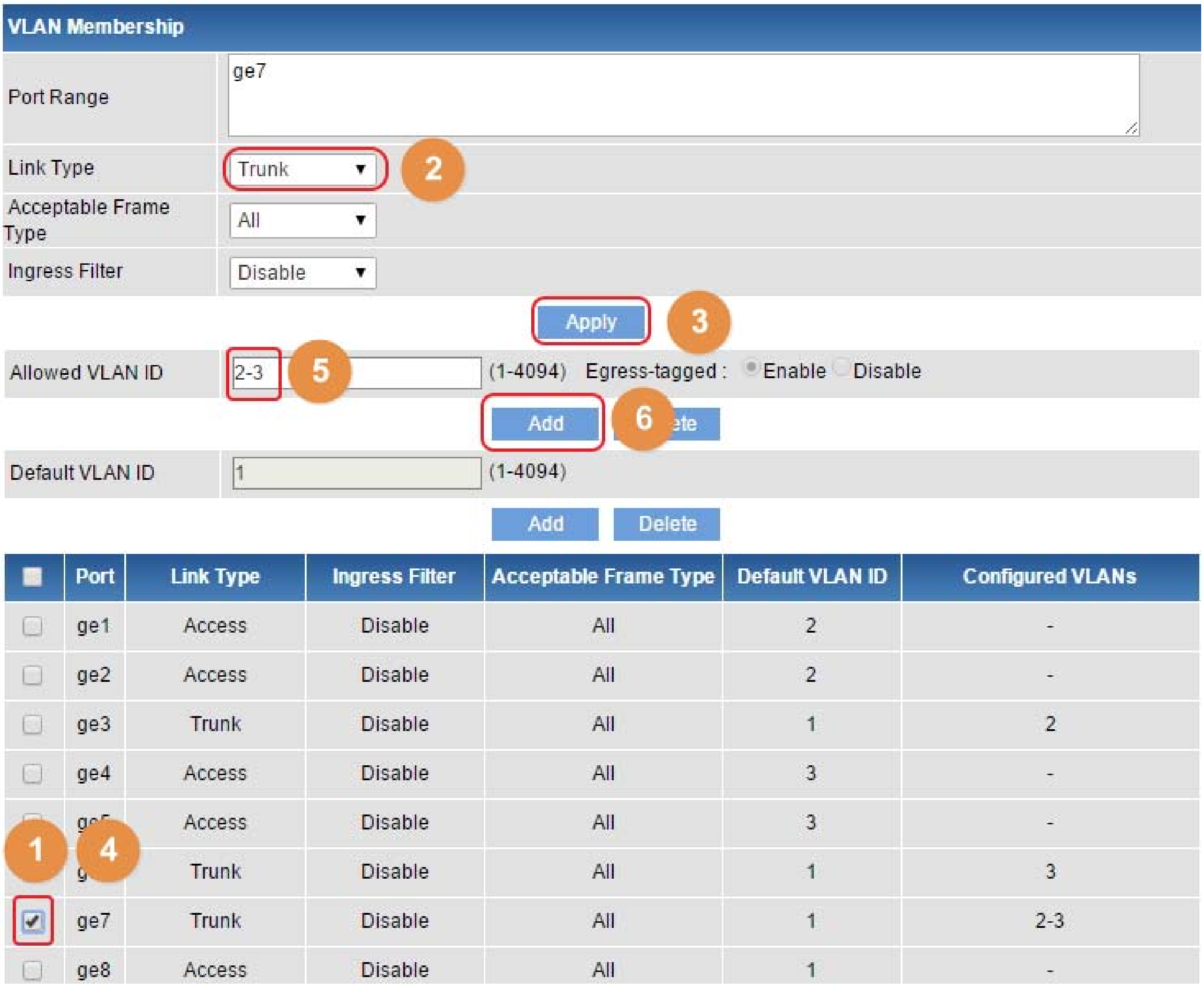
Step2: Link Type = Trunk

Step3: Apply the settings

Step4: Select Port-7

Step5: Allowed VLAN ID=*2-3*(VLAN group 2 and VLAN group 3)

Step6: Add the settings



VLAN Membership

Port Range	ge7
Link Type	Trunk ▼
Acceptable Frame Type	All ▼
Ingress Filter	Disable ▼
Allowed VLAN ID	2-3 (1-4094) Egress-tagged : ● Enable ○ Disable
Default VLAN ID	1 (1-4094)

□	Port	Link Type	Ingress Filter	Acceptable Frame Type	Default VLAN ID	Configured VLANs
□	ge1	Access	Disable	All	2	-
□	ge2	Access	Disable	All	2	-
□	ge3	Trunk	Disable	All	1	2
□	ge4	Access	Disable	All	3	-
□	ge5	Access	Disable	All	3	-
□	ge6	Trunk	Disable	All	1	3
☑	ge7	Trunk	Disable	All	1	2-3
□	ge8	Access	Disable	All	1	-

4.6 Spanning Tree Protocol

4.6.1 Spanning Tree Protocol Overview

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

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

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

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

The Switch STP performs the following functions:

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

Bridge Protocol Data Units

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

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

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

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

- The port identifier of the transmitting port

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

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

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

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

STP Port States

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

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

- **Blocking** – the port is blocked from forwarding or receiving packets
- **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- **Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets
- **Forwarding** – the port is forwarding packets
- **Disabled** – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

- From disabled to blocking

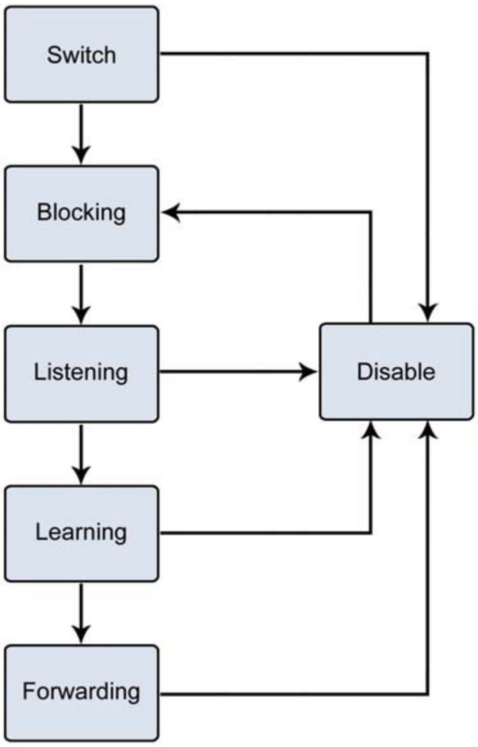


Figure 4-6-1-1 STP Port State Transitions

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

2. STP Parameters

STP Operation Levels

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

Note

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

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

Parameter	Description	Default Value
Bridge Identifier (Not user configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts:	32768 + MAC

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

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

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

Default Spanning-Tree Configuration

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

User-Changeable STA Parameters

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

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

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

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

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

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

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

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

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

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

3. Illustration of STP

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

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

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

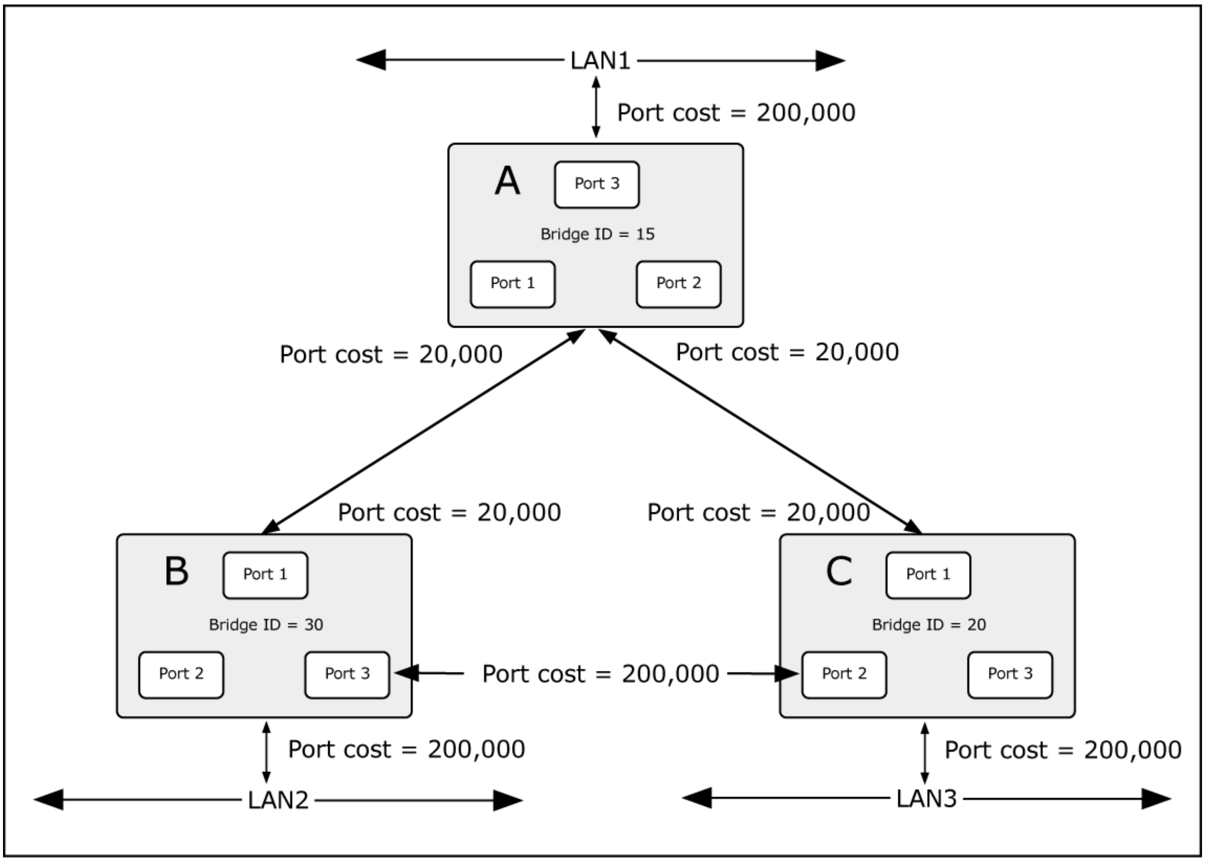


Figure 4-6-1-2 Before Applying the STA Rules

In this example, only the default STP values are used.

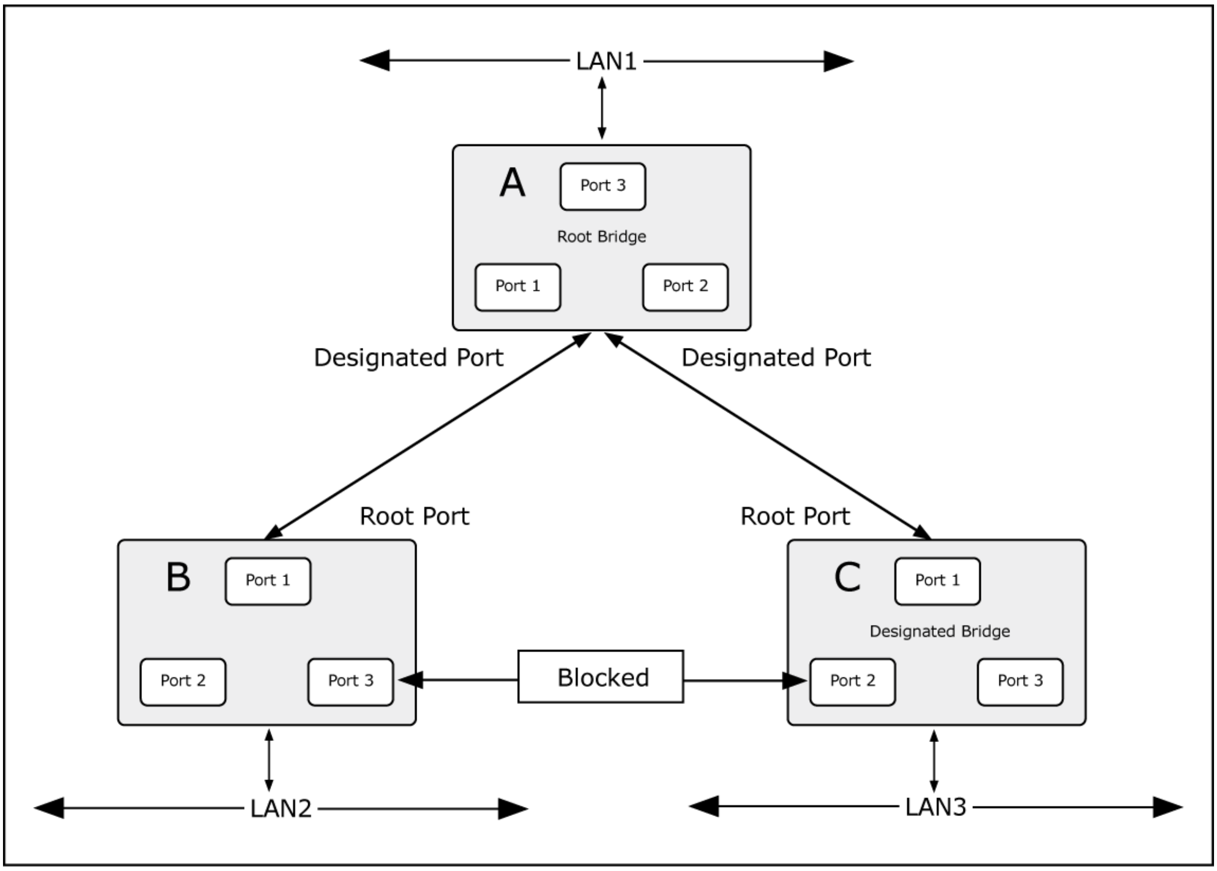


Figure 4-6-1-3 After Applying the STA Rules

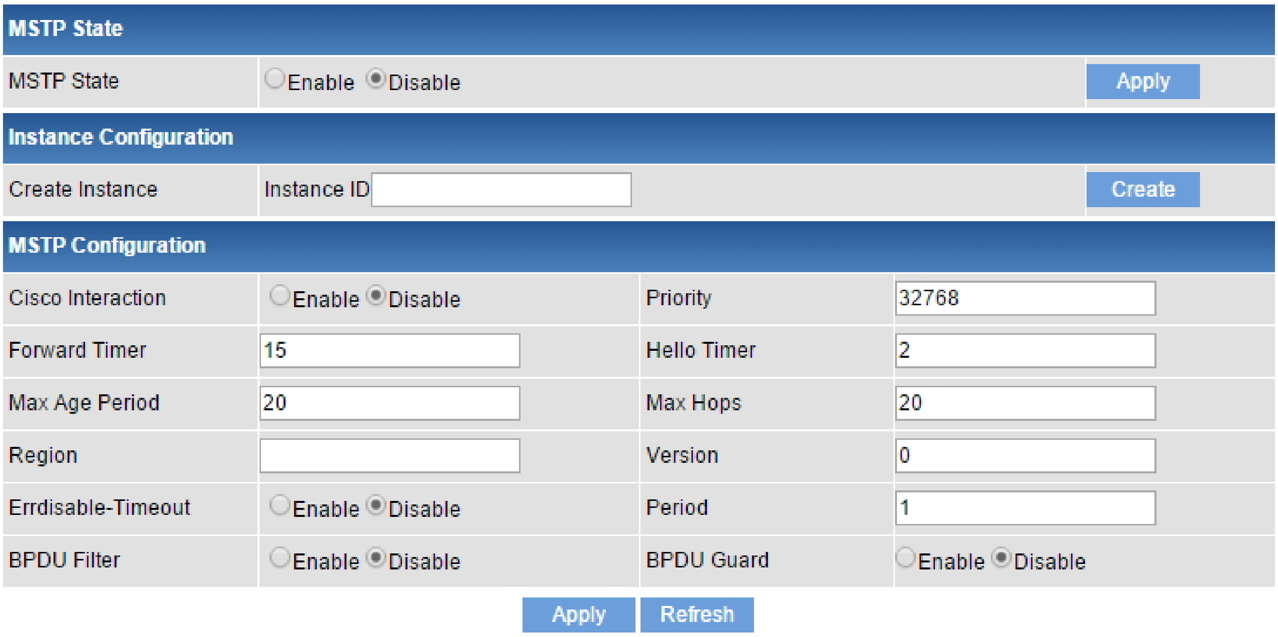
The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The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

This section has the following items:

STP Configuration	Configures STP system settings
Port Configuration	Configuration per port STP setting
STP Information	Displays the STP statistics
Port Information	Displays the per port STP statistics

4.6.2 STP Configuration

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch. The STP Configuration screen in Figure 4-6-2 appears.



MSTP State

MSTP State	○ Enable ● Disable	Apply

Instance Configuration

Create Instance	Instance ID	Create

MSTP Configuration

Cisco Interaction	○ Enable ● Disable	Priority	32768
Forward Timer	15	Hello Timer	2
Max Age Period	20	Max Hops	20
Region		Version	0
Errdisable-Timeout	○ Enable ● Disable	Period	1
BPDU Filter	○ Enable ● Disable	BPDU Guard	○ Enable ● Disable

Figure 4-6-2 : Global VLAN Configuration Screenshot

The page includes the following fields:

Object	Description
• **MSTP State**	Enable or disable the STP function. The default value is "Disabled".
• **Create Instance**	Allow to assign MSTI ID.

	The range for the MSTI ID is 1-15.
• **Cisco Interaction**	Allow to enable/disable Cisco interaction.
• **Priority**	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
• **Forward Timer**	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds -Default: 15 -Minimum: The higher of 4 or [(Max. Message Age / 2) + 1] -Maximum: 30
• **Hello Timer**	The time that controls the switch to send out the BPDU packet to check STP current status. Enter a value between 1 through 10.
• **Max Age Period**	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds. -Default: 20 -Minimum: The higher of 6 or [2 x (Hello Time + 1)]. -Maximum: The lower of 40 or [2 x (Forward Delay -1)]
• **Max Hops**	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 6 to 40 hops.
• **Region**	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 16 characters.
• **Version**	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
• **Errdisable-Timeout**	Sets the errdisable-timeout interval -Default: 400seconds

• **Period**	Configures sending STP packet period time . -Default: 1
• **BPDU Filter**	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
• **BPDU Guard**	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Buttons

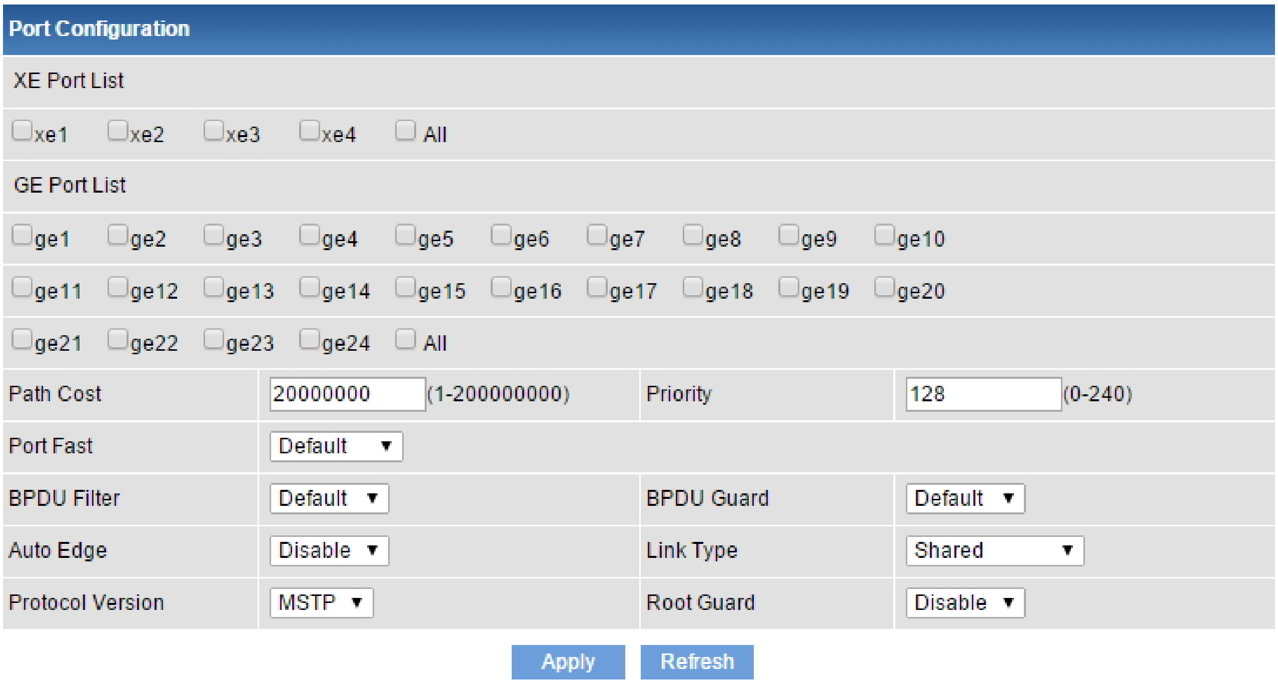
Apply : Click to apply changes.

Create : Click to add a new data to the feature.

Refresh : Click to refresh the page; any changes made locally will be undone.

4.6.3 Port Configuration

This page provides the port configuration for STP. The Port Configuration screen in Figure 4-6-3 appears.



Port Configuration

XE Port List

□xe1 □xe2 □xe3 □xe4 □ All

GE Port List

□ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10

□ge11 □ge12 □ge13 □ge14 □ge15 □ge16 □ge17 □ge18 □ge19 □ge20

□ge21 □ge22 □ge23 □ge24 □ All

Path Cost	20000000 (1-200000000)	Priority	128 (0-240)
Port Fast	Default ▼		
BPDU Filter	Default ▼	BPDU Guard	Default ▼
Auto Edge	Disable ▼	Link Type	Shared ▼
Protocol Version	MSTP ▼	Root Guard	Disable ▼

Figure 4-6-3: Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port List**	Select port number for below row table.
• **Path Cost**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Default: **128** Range: 0-240, in steps of 16
• **Port Fast**	PortFast is a Cisco network function which can be configured to resolve taking to transition ports over to the Forwarding state. ■ **Default** The vaule is disabled as default. ■ **Portfast** PortFast enabled port can transition to the blocking forwarding state ■ **Edgeport** Controls whether the operEdge flag should start as beeing set or cleared. (The initial operEdge state when a port is initialized).
• **BPDU Filter**	Control whether a port explicitly configured as Edge will transmit and receive BPDUs. ■ **Default** The vaule is disabled as default. ■ **Enable** It can enable BPDU filter ■ **Disable** It can disable BPDU filter
• **BPDU Guard**	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. ■ **Default** The vaule is disabled as default. ■ **Enable** It can enable BPDU Guard ■ **Disable**

	It can disable BPDU Guard
• **Auto Edge**	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not. The vaule is disabled as default ■ **Enable** It can enable Auto Edge ■ **Disable** It can disable Auto Edge
• **Link Type**	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transitions to the forwarding state is faster for point-to-point LANs than for shared media. The vaule is shared as default ■ **Shared** It can enable Shared mode ■ **Point to Point** It can enable Point to Point mode
• **Protocol Version**	The STP protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**. The vaule is MSTP as default
• **Root Guard**	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized). The vaule is disabled as default ■ **Enable** It can enable Root Guard ■ **Disable** It can disable Root Guard

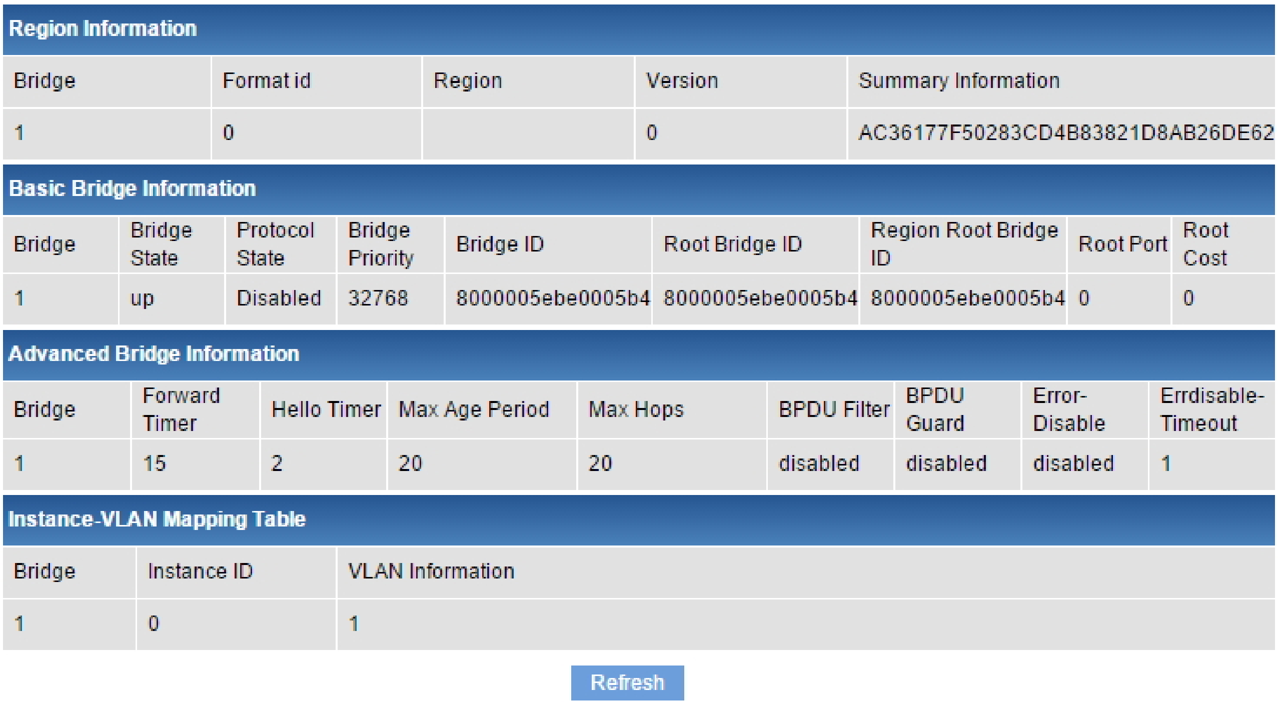
Buttons

Apply: Click to apply changes.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.6.4 STP Information

This page display STP Information. The STP Information screen in Figure 4-6-5 appears.



Region Information

Bridge	Format id	Region	Version	Summary Information
1	0		0	AC36177F50283CD4B83821D8AB26DE62

Basic Bridge Information

Bridge	Bridge State	Protocol State	Bridge Priority	Bridge ID	Root Bridge ID	Region Root Bridge ID	Root Port	Root Cost
1	up	Disabled	32768	8000005ebe0005b4	8000005ebe0005b4	8000005ebe0005b4	0	0

Advanced Bridge Information

Bridge	Forward Timer	Hello Timer	Max Age Period	Max Hops	BPDU Filter	BPDU Guard	Error-Disable	Errdisable-Timeout
1	15	2	20	20	disabled	disabled	disabled	1

Instance-VLAN Mapping Table

Bridge	Instance ID	VLAN Information
1	0	1

Figure 4-6-5: STP Information Page Screenshot

The page includes the following fields:

Object	Description
• **Bridge**	Displays the current STP Bridge of this Region
• **Format ID**	Displays the current STP Format ID of this Region
• **Region**	Displays the current STP Region of this Region
• **Version**	Displays the current STP version of this Region
• **Summary Information**	Displays the current Summary Information of this Region
• **Bridge State**	Displays the current Bridge State
• **Protocol State**	Displays the current STP state
• **Bridge Priority**	The Bridge Priority of this Bridge instance.
• **Bridge ID**	The Bridge ID of this Bridge instance.
• **Root Bridge ID**	**The Root Bridge ID of this Bridge instance.**
• **Region Root Bridge ID**	**The Region Root Bridge ID of this Bridge instance.**
• **Root Port**	**The switch port currently assigned the root port role.**

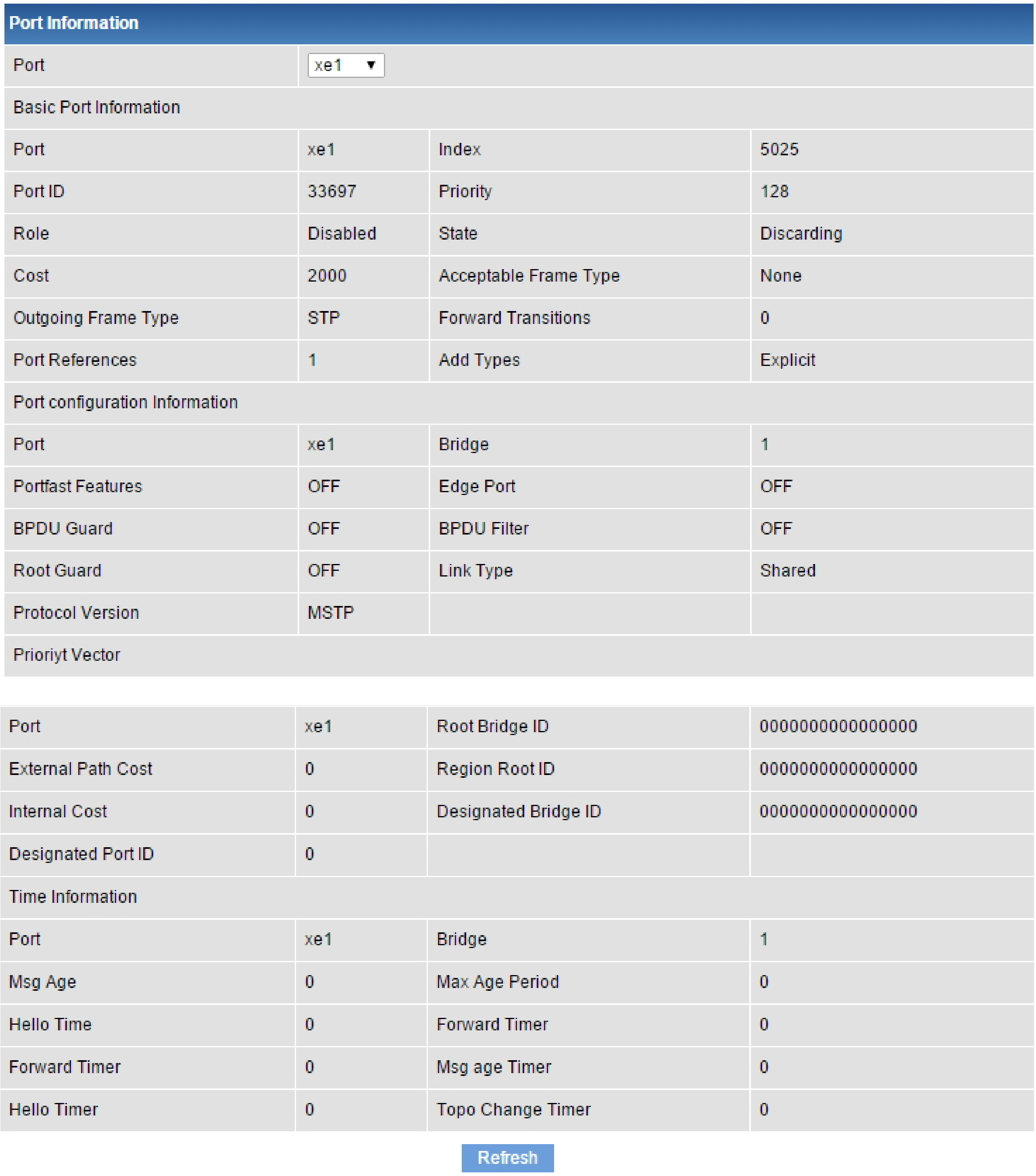
• Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
• Forward Timer	Display the current Forward Timer
• Hello Timer	Display the current Hello Timer
• Max Age Period	Display the current Max Age Period
• Max Hops	Display the current Max Hops
• BPDU Filter	Displays the current BPDU filter configuration.
• BPDU Guard	Displays the current BPDU guard configuration.
• Error-Disable	Displays the current status of Error-Disable
• Errdisable-Timeout	Displays the current error disabled timeout
• Instance ID	Displays the current Instance ID list
• VLAN Information	Displays the current VLAN Information list

Buttons

: Click to refresh the page; any changes made locally will be undone.

4.6.5 Port Information

This page display Port Information of STP. The Port Information screen in Figure 4-6-6 appears.



Port Information

Port	xe1 ▼		
Basic Port Information			
Port	xe1	Index	5025
Port ID	33697	Priority	128
Role	Disabled	State	Discarding
Cost	2000	Acceptable Frame Type	None
Outgoing Frame Type	STP	Forward Transitions	0
Port References	1	Add Types	Explicit
Port configuration Information			
Port	xe1	Bridge	1
Portfast Features	OFF	Edge Port	OFF
BPDU Guard	OFF	BPDU Filter	OFF
Root Guard	OFF	Link Type	Shared
Protocol Version	MSTP		
Prioriyt Vector			

Port	xe1	Root Bridge ID	0000000000000000
External Path Cost	0	Region Root ID	0000000000000000
Internal Cost	0	Designated Bridge ID	0000000000000000
Designated Port ID	0		
Time Information			
Port	xe1	Bridge	1
Msg Age	0	Max Age Period	0
Hello Time	0	Forward Timer	0
Forward Timer	0	Msg age Timer	0
Hello Timer	0	Topo Change Timer	0

Figure 4-6-6: Port Information Page Screenshot

The page includes the following fields:

Object	Description
Port	Displays the current STP Port
Index	Displays the current STP Index
Port ID	Displays the current STP Port ID
Priority	Displays the current STP Priority
Role	Displays the current STP Role
State	Displays the current STP State
Cost	Displays the current STP Cost
Acceptable Frame Type	Displays the current STP Acceptable Frame Type
Outgoing Frame Type	Displays the current STP Outgoing Frame Type
Forward Transitions	Displays the current STP Forward Transitions
Port References	Displays the current STP Port References
Add Types	Displays the current STP Add Types
Bridge	Displays the current STP Bridge
Portfast Features	Displays the current STP Portfast status
Edge Port	Displays the current STP Edge Port
BPDU Guard	Displays the current BPDU guard configuration.
BPDU Filter	Displays the current BPDU filter configuration.
Root Guard	Displays the current STP Root Guard
Link Type	Displays the current STP Link Type
Protocol Version	Displays the current STP Protocol Version
Root Bridge ID	Displays the current STP Root Bridge ID
External Path Cost	Displays the current STP External Path Cost
Region Root ID	Displays the current STP Region Root ID
Internal Cost	Displays the current STP Internal Cost
Designated Bridge ID	Displays the current STP Designated Bridge ID
Designated Port ID	Displays the current STP Designated Port ID
Msg Age	Displays the current STP Msg Age
Max Age Period	Displays the current STP Max Age Period
Hello Time	Displays the current STP Hello Time
Forward Timer	Displays the current STP Forward Timer
Msg age Timer	Displays the current STP Msg age Timer
Hello Timer	Displays the current STP Hello Timer
Topo Change Timer	Displays the current STP Topo Change Timer

Buttons

Refresh: Click to refresh the page; any changes made locally will be undone.

4.7 Multicast

4.7.1 Multicast Overview

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

About the Internet Group Management Protocol (IGMP) Snooping

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

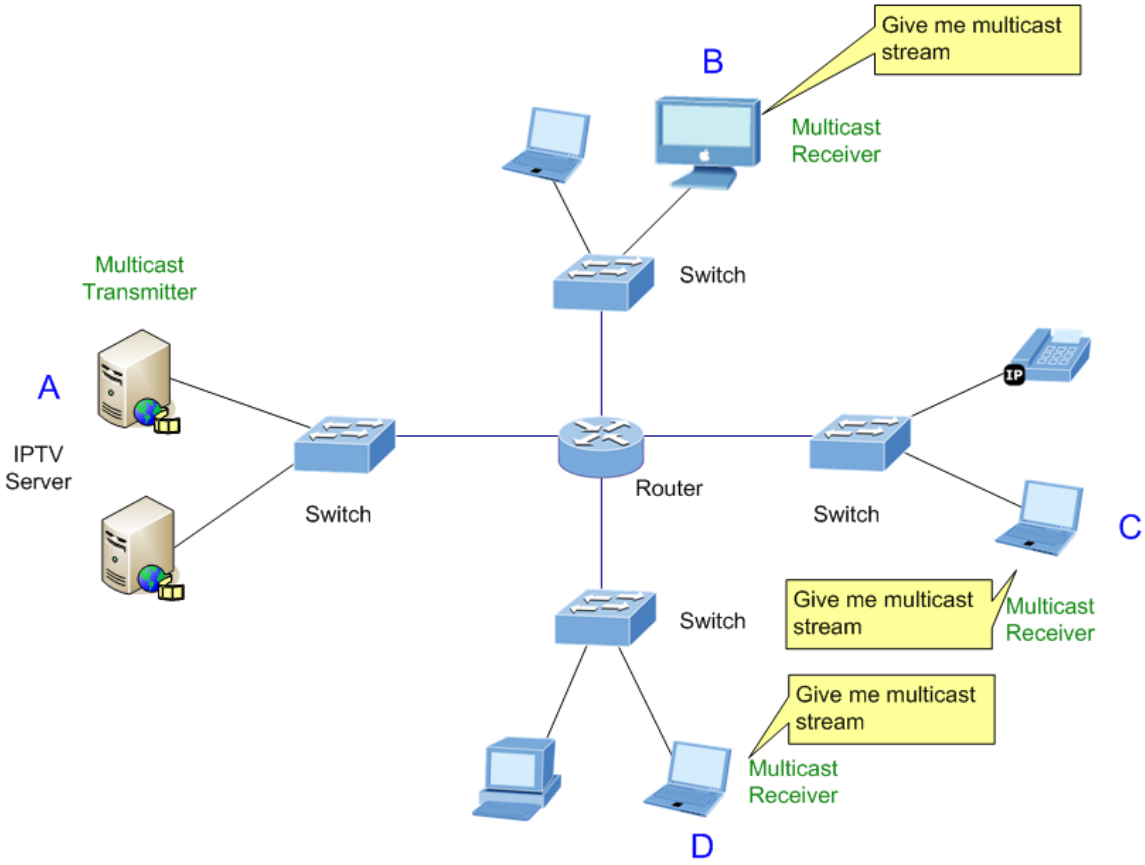


Figure 4-7-1-1 Multicast Service

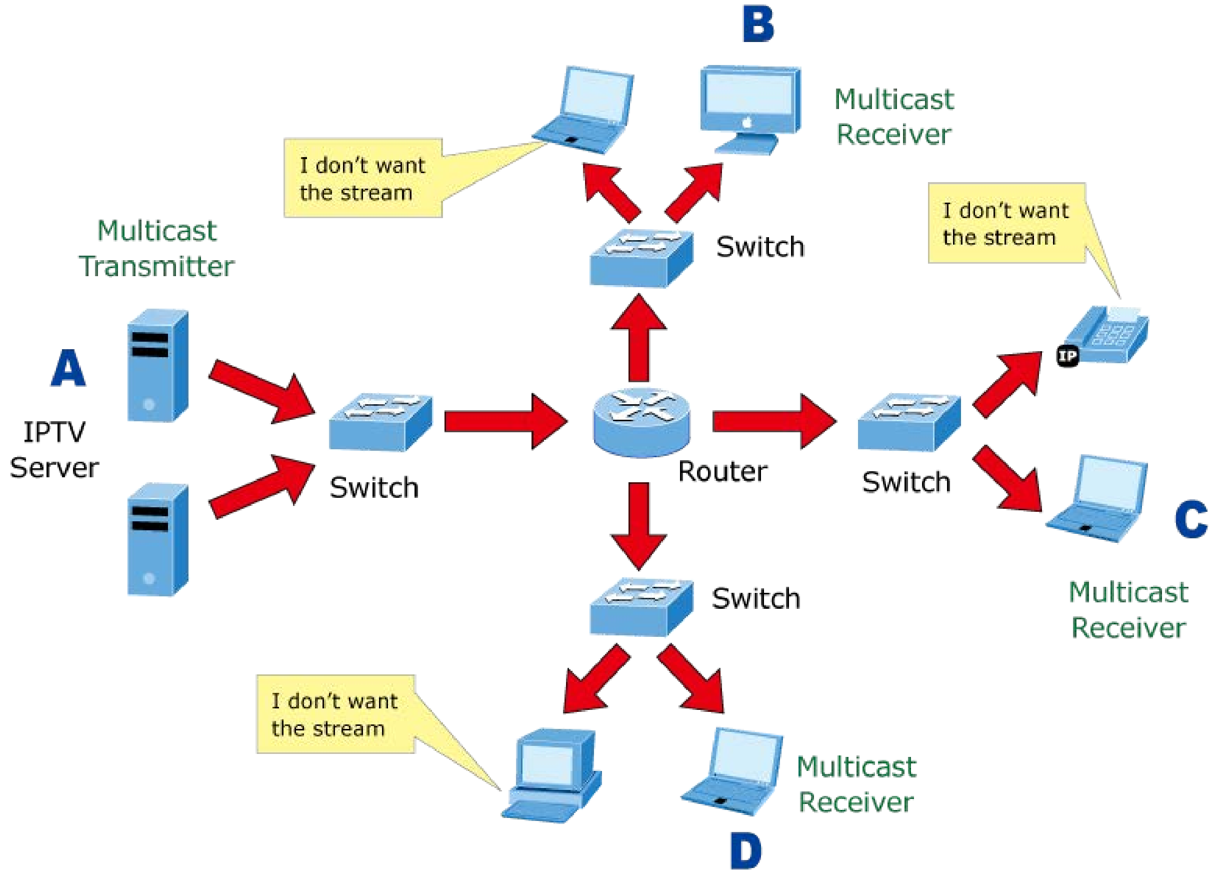


Figure 4-7-1-2 Multicast Flooding

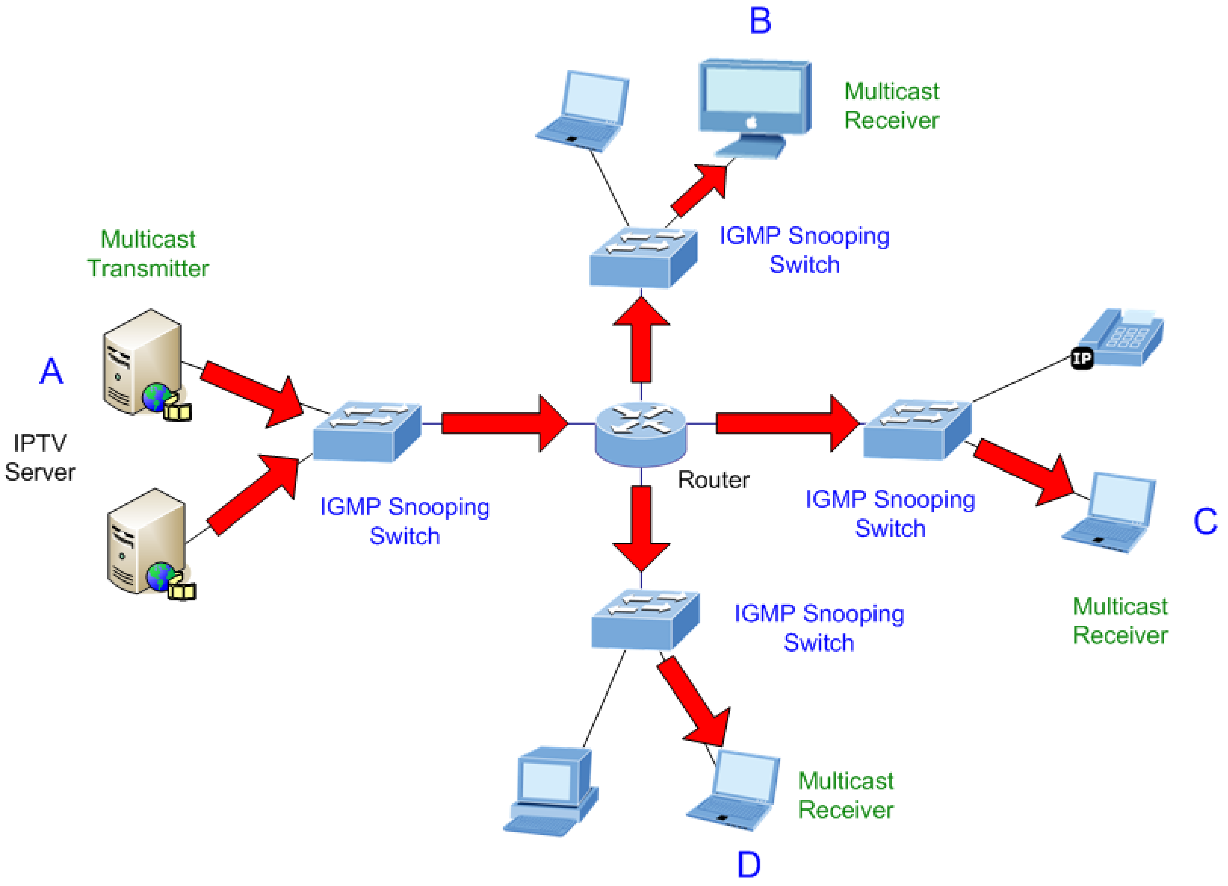


Figure 4-7-1-3 IGMP Snooping Multicast Stream Control

IGMP Versions 1 and 2

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

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

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0 8 16 31

Type	**Response Time**	**Checksum**
Group Address (all zeros if this is a query)		

The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	**Membership Report (version 2)**
0x17	**Leave a Group (version 2)**
0x12	**Membership Report (version 1)**

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

A host sends an IGMP **"report"** to join a group

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

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

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

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

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

The states a computer will go through to join or to leave a multicast group are shown below:

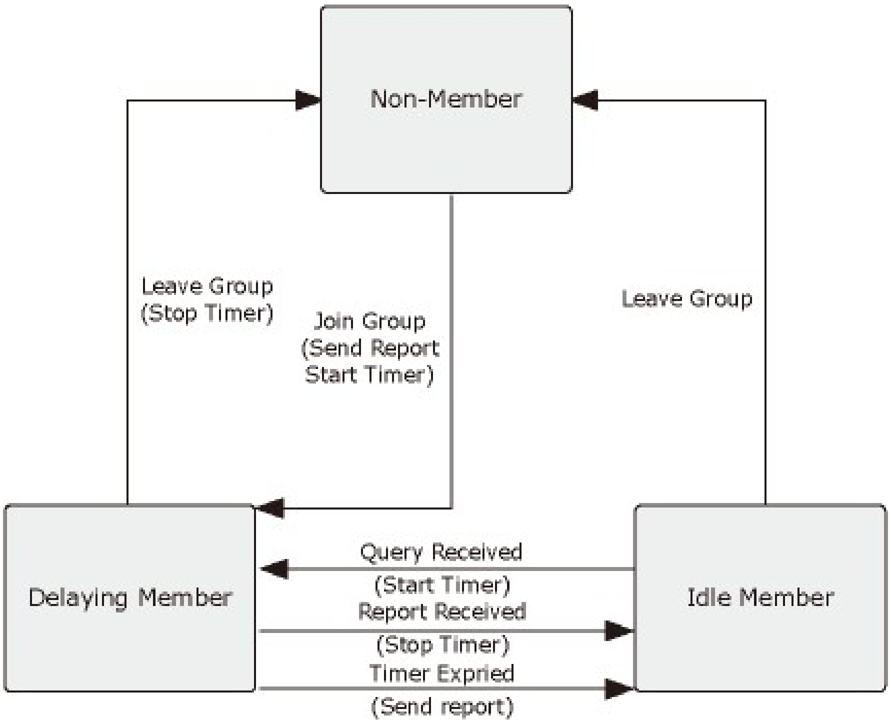


Figure 4-7-1-4 IGMP State Transitions

- **IGMP Querier –**

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

Note

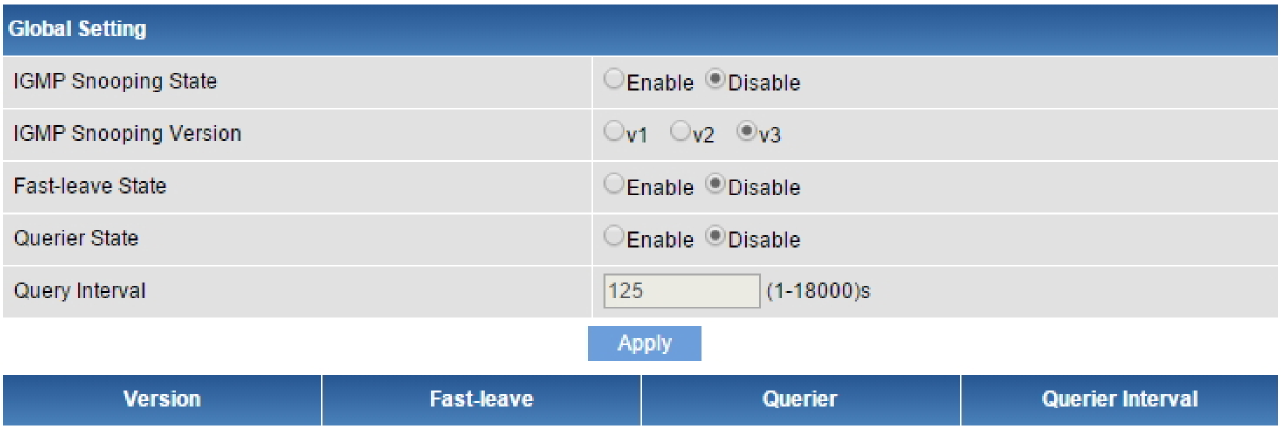
Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

This section has the following items:

■ **Global Setting**	Configures IGMP snooping settings
■ **Router Port Setting**	Configures multicast router port setting
■ **IGMP Information**	Displays the IGMP snooping statistics

4.7.2 Global Setting

This page provides IGMP Snooping global setting configuration. The Global Setting Configuration screen in Figure 4-7-2 appears.



Global Setting	
IGMP Snooping State	○Enable ●Disable
IGMP Snooping Version	○v1 ○v2 ●v3
Fast-leave State	○Enable ●Disable
Querier State	○Enable ●Disable
Query Interval	125 (1-18000)s

Apply

Version	Fast-leave	Querier	Querier Interval

Figure 4-7-2: Global Setting Configuration Page Screenshot

The page includes the following fields:

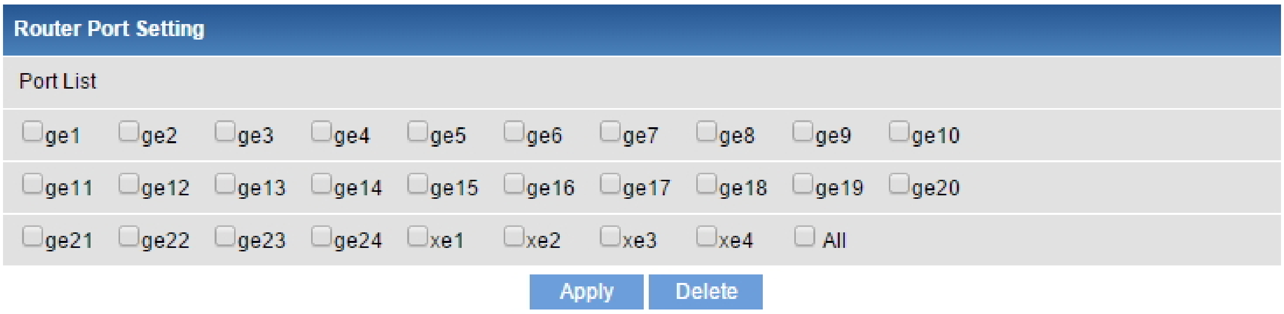
Object	Description
• **IGMP Snooping State**	Enable or disable the IGMP snooping. The default value is "Disabled".
• **IGMP Snooping Version**	Sets the IGMP Snooping operation version. Possible versions are: ■ **v1**: Set IGMP Snooping supported IGMP version 1. ■ **v2**: Set IGMP Snooping supported IGMP version 2. ■ **v3**: Set IGMP Snooping supported IGMP version 3.
• **Fast-leave State**	Enable or disable the Fast-leave State. The default value is "Disabled".
• **Querier State**	Enable or disable the querier state. The default value is "Disabled".
• **Query Interval**	Configures the querier interval time. The default value is 125seconds.

Buttons

Apply: Click to apply changes.

4.7.3 Router Port Setting

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your Managed Switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the Switch. The Router Port Setting screen in Figure 4-7-3 appears.



Router Port Setting

Port List

□ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10
□ge11 □ge12 □ge13 □ge14 □ge15 □ge16 □ge17 □ge18 □ge19 □ge20
□ge21 □ge22 □ge23 □ge24 □xe1 □xe2 □xe3 □xe4 □ All

Figure 4-7-3: Router Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port List**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

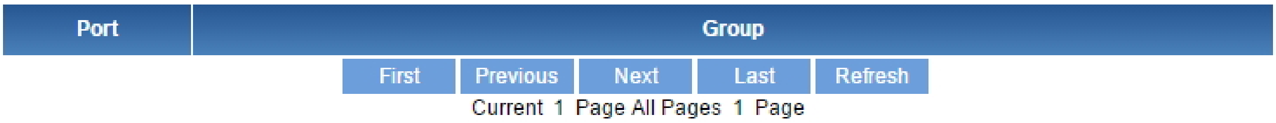
Buttons

Apply: Click to apply changes.

Delete: Click to delete a new data to the feature.

4.7.4 IGMP Information

This page provides IGMP Information. The IGMP Information screen in Figure 4-7-4 appears.



Port	Group

Current 1 Page All Pages 1 Page

Figure 4-7-4: IGMP Information Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Displays the current member port
• **Group**	Displays multicast IP address for a specific multicast service

Buttons

First: Click to move to the first page.

Previous: Click to move to the previous page.

Next: Click to move to the next page.

Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.8 SNMP

4.8.1 SNMP Overview

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

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

- **Network management stations (NMS's):** Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMS's are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents**：Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)**：A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **Network-management protocol**：A management protocol is used to convey management information between agents and NMS's. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations

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

- **Get --** Allows the NMS to retrieve an object instance from the agent.
- **Set --** Allows the NMS to set values for object instances within an agent.
- **Trap --** Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community

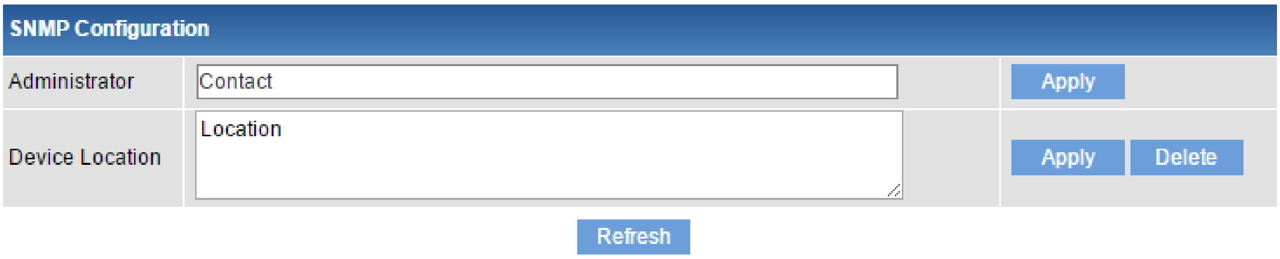
An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. An SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management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

SNMP default communities are:

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

4.8.2 SNMP Management

Configure SNMP Management on this page. The SNMP Management screen in Figure 4-8-2 appears.



SNMP Configuration

Administrator	Contact	Apply
Device Location	Location	Apply Delete

Refresh

Figure 4-8-5: SNMP Management Page

The page includes the following fields:

Object	Description
• **Administrator**	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed characters length is 0 to 64.
• **Device Location**	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed characters length is 0 to 64.

Buttons

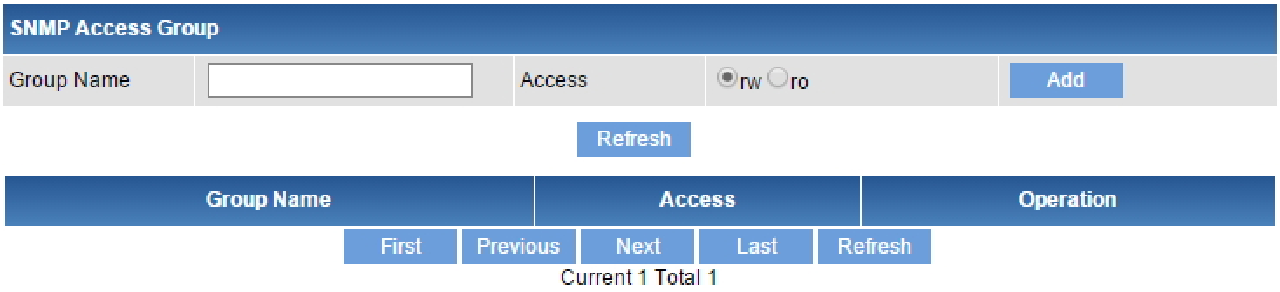
Apply : Click to apply changes.

Refresh : Click to refresh the page; any changes made locally will be undone.

Delete : Click to delete a new data to the feature.

4.8.3 SNMP Access Group

Configure SNMP access group on this page. The entry index keys are Group Name, Access. The SNMP access group screen in Figure 4-8-3 appears.



SNMP Access Group

Group Name		Access	● rw ○ ro	Add

Refresh

Group Name	Access	Operation

First Previous Next Last Refresh

Current 1 Total 1

Figure 4-8-3: SNMP access group Page

The page includes the following fields:

Object	Description
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 16.
• **Access**	Indicates the community read/write access right to permit access to SNMP agent Possible modes are: ■ **rw**: read and write access. ■ **ro**: read only access.
• **Operation**	Click the delete button to remove the profile.

Buttons

Add: Click to add a new data to the feature.

First: Click to move to the first page.

Previous: Click to move to the previous page.

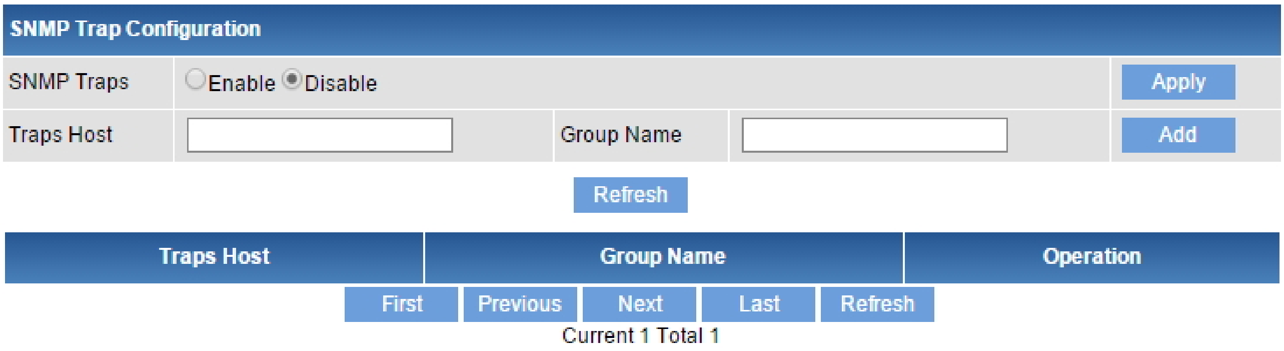
Next: Click to move to the next page.

Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.8.4 SNMP Trap Configuration

Configure SNMPv1 and 2 notification recipients on this page.. The SNMP Trap Configuration screen in Figure 4-8-4 appears.



SNMP Trap Configuration

SNMP Traps	○Enable ●Disable			Apply
Traps Host		Group Name		Add

Refresh

Traps Host	Group Name	Operation

First Previous Next Last Refresh

Current 1 Total 1

Figure 4-8-4: SNMP Trap Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **SNMP Traps**	Enable/disable the SNMP trap.
• **Traps Host**	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It can also represent a legally valid IPv4 address. For example, '192.1.2.34'.
• **Group Name**	Indicates the community access string when send SNMP trap packet.

Buttons

Add: Click to add a new data to the feature.

Apply: Click to apply changes.

First: Click to move to the first page.

Previous: Click to move to the previous page.

Next: Click to move to the next page.

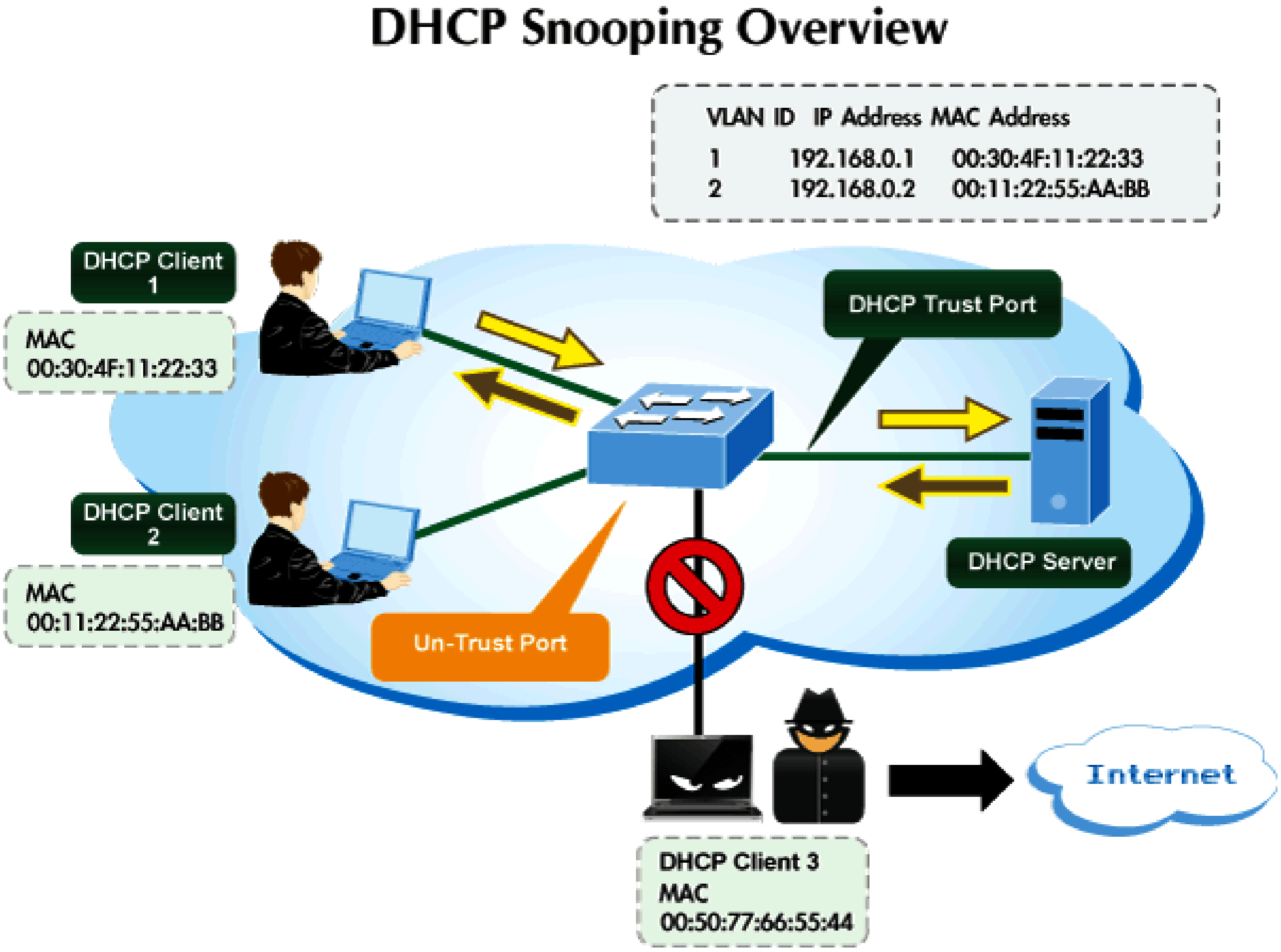
Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.9 DHCP Snooping

4.9.1 DHCP Snooping Overview

The addresses assigned to DHCP clients on unsecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.



Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. **DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall**. When DHCP snooping is enabled globally and enabled on a VLAN interface, **DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped**.

- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

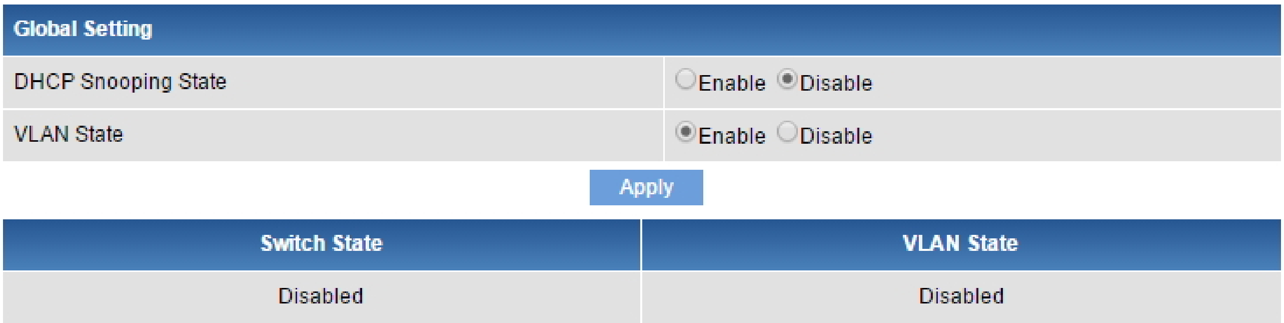
- Filtering rules are implemented as follows:
  - If the global DHCP snooping is disabled, all DHCP packets are forwarded.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:
    - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
    - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
    - If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
    - If the DHCP packet is not a recognizable type, it is dropped.

- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

Additional considerations when the switch itself is a DHCP client – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped

4.9.2 Global Setting

DHCP Snooping is used to block intruder on the untrusted ports of switch when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server. Configure DHCP Snooping on this page. The Global Setting screen in Figure 4-9-2 appears.



Global Setting	
DHCP Snooping State	○Enable ●Disable
VLAN State	●Enable ○Disable

Apply

Switch State	VLAN State
Disabled	Disabled

Figure 4-9-2: Global Setting Page Screenshot

The page includes the following fields:

Object	Description
• **DHCP Snooping State**	Indicates the DHCP snooping mode operation. Possible modes are: ■ **Enabled**: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. ■ **Disabled**: Disable DHCP snooping mode operation.
• **VLAN State**	Indicates the DHCP snooping VLAN mode operation. Possible modes are: ■ **Enabled**: Enable DHCP snooping VLAN mode operation. When enable DHCP snooping VLAN mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. ■ **Disabled**: Disable DHCP snooping VLAN mode operation.

Buttons

Apply: Click to apply changes.

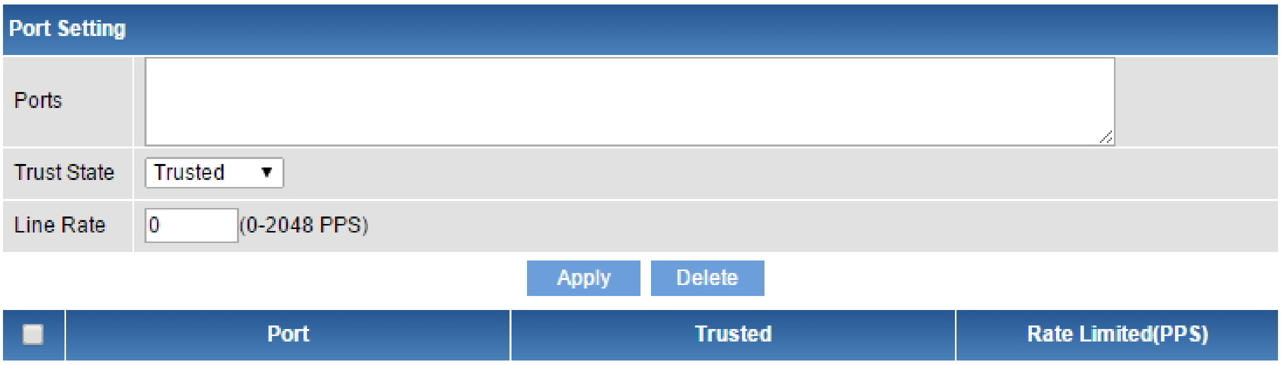
4.9.3 Port Setting

Configures switch ports as trusted or untrusted.

Command Usage

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.
- When DHCP snooping enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- Set all ports connected to DHCP servers within the local network or firewall to trusted state. Set all other ports outside the local network or firewall to untrusted state.

The DHCP Snooping Port Setting screen in Figure 4-9-3 appears.



Port Setting

Ports	
Trust State	Trusted ▼
Line Rate	0 (0-2048 PPS)

□	Port	Trusted	Rate Limited(PPS)

Figure 4-9-3 : DHCP Snooping Port Setting Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this check box table
• **Trust State**	Indicates the DHCP snooping port mode. Possible port modes are: ■ **Trusted**: Configures the port as trusted sources of the DHCP message. ■ **Untrusted**: Configures the port as untrusted sources of the DHCP message.
• **Line Rate**	The allowed values are: **0-2048** in pps.

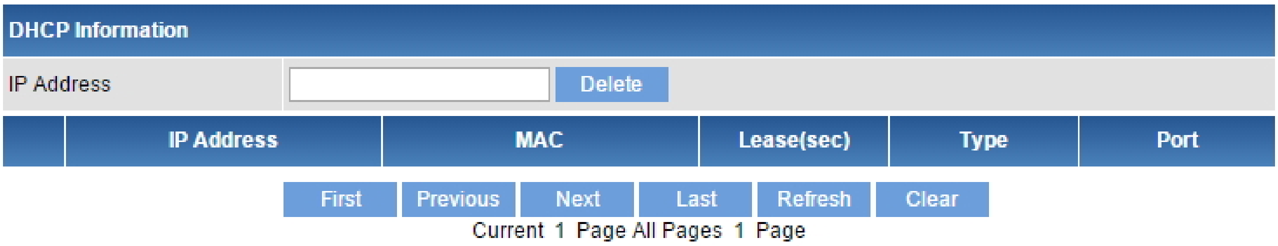
Buttons

Apply : Click to apply changes.

Delete : Click to delete a new data to the feature.

4.9.4 DHCP Information

This page display DHCP Information for the switch. The DHCP Information screen in Figure 4-9-4 appears.



DHCP Information

IP Address

	IP Address	MAC	Lease(sec)	Type	Port

Current 1 Page All Pages 1 Page

Figure 4-9-4: DHCP Information Page Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	Displays the IP Address of DHCP client
• **MAC**	Displays the MAC Address of DHCP client
• **Lease (sec)**	Displays the Lease time of DHCP client
• **Type**	Displays the Type of DHCP client
• **VLAN**	Displays the VLAN ID of DHCP client
• **Interface**	Displays the Interface of DHCP client

Buttons

Delete: Click to delete a new data to the feature.

First: Click to move to the first page.

Previous: Click to move to the previous page.

Next: Click to move to the next page.

Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the table.

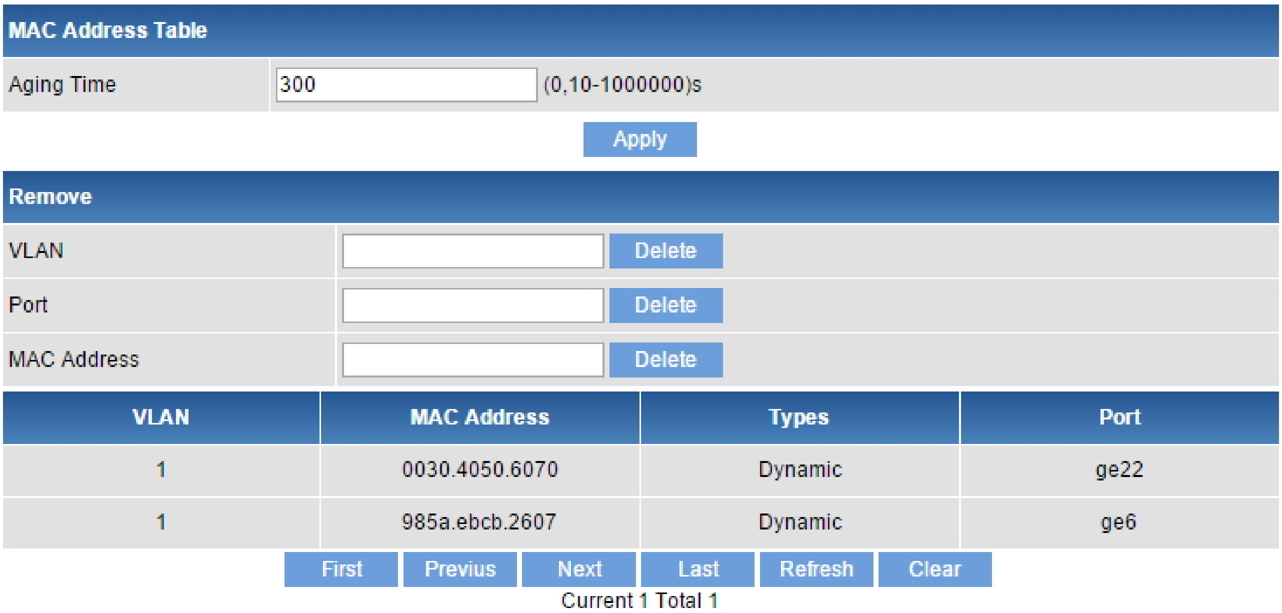
4.10 MAC Address Table

Switching of frames is based upon the DMAC address contained in the frame. The Managed Switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

4.10.1 MAC Address Table

Entries in the MAC Table are shown on this page. The MAC Address Table screen in Figure 4-10-1 appears.



MAC Address Table

Aging Time	300 (0,10-1000000)s

Remove

VLAN	
Port	
MAC Address	

VLAN	MAC Address	Types	Port
1	0030.4050.6070	Dynamic	ge22
1	985a.ebcb.2607	Dynamic	ge6

Current 1 Total 1

Figure 4-10-1: MAC Address Table Screenshot

The page includes the following fields:

Object	Description
• **Aging Time**	Specify the aging time of this switch. The allowed values are 0, 10-1000000seconds and default value is 300seconds
• **VLAN**	Remove the VLAN ID of the MAC address table.
• **Port**	Remove the port of the MAC address table.
• **MAC Address**	Remove the specific MAC address of the MAC address table.

Buttons

: Click to delete a new data to the feature.

: Click to move to the first page.

: Click to move to the previous page.

: Click to move to the next page.

: Click to move to the last page.

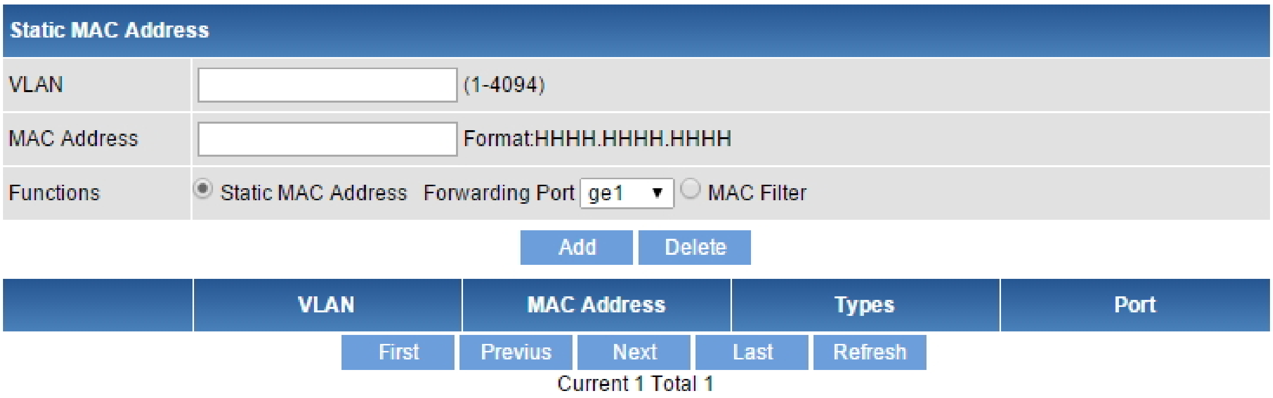
: Click to refresh the page; any changes made locally will be undone.

: Click to clear the table.

: Click to apply changes.

4.10.2 Static MAC Address

By filtering MAC address, the switch can easily filter the per-configured MAC address and reduce the un-safety. The Static MAC Address screen in Figure 4-10-2 appears.



Static MAC Address

VLAN	(1-4094)
MAC Address	Format:HHHH.HHHH.HHHH
Functions	● Static MAC Address Forwarding Port ge1 ▼ ○ MAC Filter

	VLAN	MAC Address	Types	Port

Current 1 Total 1

Figure 4-10-2: Static MAC Address Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN**	The VLAN ID of the entry.
• **MAC Address**	Indicates the MAC address for the specific device in dotted Hexadecimal notation Example: 0030.4FAA.BBEE
• **Functions**	Indicates the Static MAC address/MAC Filter mode. Possible port modes are: ■ **Static MAC**: Physical Static MAC address associated with this interface ■ **Forwarding Port**: Configures the port to trusted sources of the DHCP message. ■ **MAC Filter**: Filter the per-configured MAC address and reduce the un-safety

Buttons

Delete: Click to delete a new data to the feature.

First: Click to move to the first page.

Previous: Click to move to the previous page.

Next: Click to move to the next page.

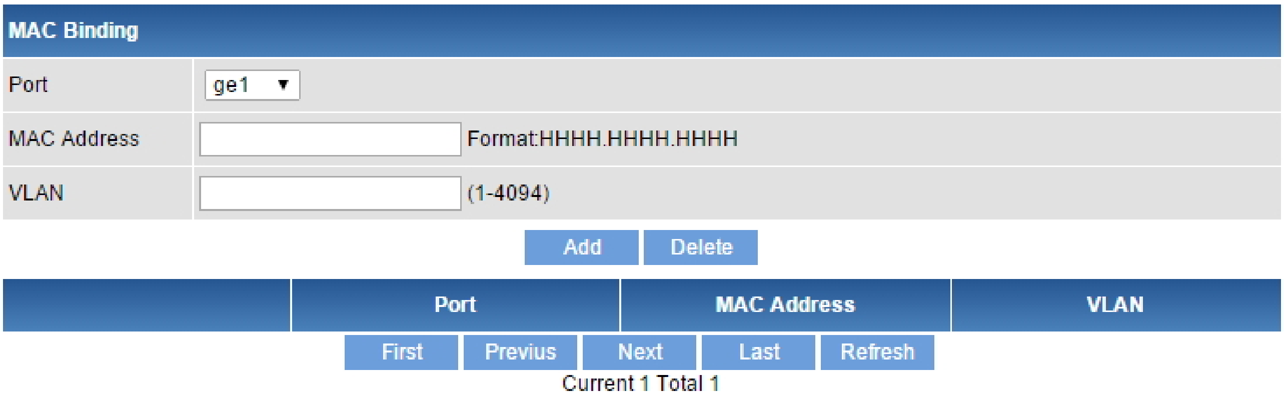
Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the table.

4.10.3 MAC Binding

This page allows you to configure the MAC Binding Limit Control system and port settings. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. The MAC Binding Configuration screen in Figure 4-10-3 appears.



MAC Binding

Port	ge1 ▼
MAC Address	Format:HHHH.HHHH.HHHH
VLAN	(1-4094)

	Port	MAC Address	VLAN

Current 1 Total 1

Figure 4-10-3: MAC Binding Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port from this drop-down list
• **MAC Address**	Indicates the MAC address for the specific device in dotted Hexadecimal notation Example: 0030.4FAA.BBEE
• **VLAN**	The VLAN ID of the entry.

Buttons

Delete: Click to delete a new data to the feature.

First: Click to move to the first page.

Previous: Click to move to the previous page.

Next: Click to move to the next page.

Last: Click to move to the last page.

Refresh: Click to refresh the page; any changes made locally will be undone.

Add: Click to add a new data to the feature.

4.10.4 MAC Auto Binding

This page allows you to configure the MAC auto Binding Limit Control system and port settings with selected port feature. Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. The MAC Auto Binding Configuration screen in Figure 4-10-4 appears.

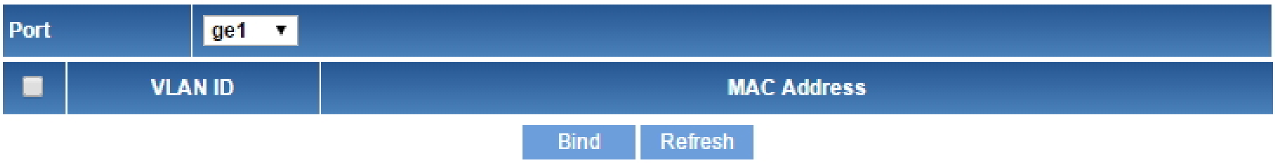


Figure 4-10-4: MAC Auto Binding Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this check box to create MAC auto Binding entry
• **MAC Address**	Displays the MAC address on a given port in dotted Hexadecimal notation Example: 0030.4FAA.BBEE
• **VLAN**	Displays the VLAN ID of the entry.

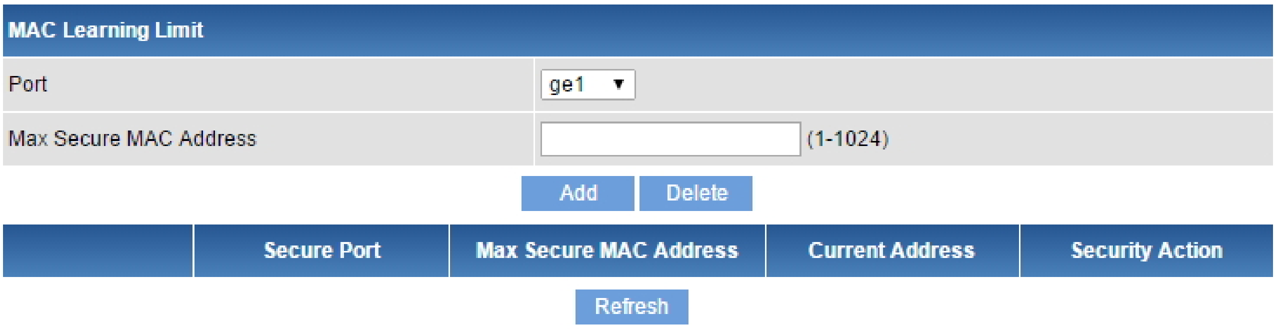
Buttons

Refresh: Click to refresh the page; any changes made locally will be undone.

Bind: Click to bind the MAC address into VLAN ID.

4.10.5 MAC Learning Limit

The maximum number of MAC addresses that can be secured on this port. If the limit is exceeded, the corresponding action is taken. The MAC Learning Limit Configuration screen in Figure 4-10-5 appears.



MAC Learning Limit

Port	ge1 ▼
Max Secure MAC Address	(1-1024)

	Secure Port	Max Secure MAC Address	Current Address	Security Action

Figure 4-10-5: MAC Learning Limit Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list
• **Max Secure Address**	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Buttons

Add: Click to add a new data to the feature.

Delete: Click to delete a new data to the feature.

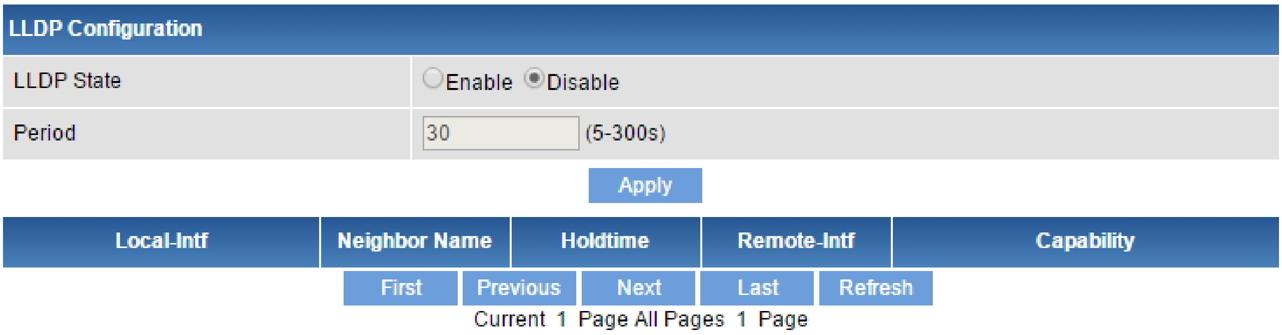
Refresh: Click to refresh the page; any changes made locally will be undone.

4.11 LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device.

4.11.1 LLDP Configuration

This page allows the user to configure the current LLDP settings. The LLDP Configuration screen in Figure 4-11-1 appears.



LLDP Configuration

LLDP State	○Enable ●Disable
Period	30 (5-300s)

Local-Intf	Neighbor Name	Holdtime	Remote-Intf	Capability

Current 1 Page All Pages 1 Page

Figure 4-11-1: LLDP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **LLDP State**	Globally enable or disable LLDP function
• **Period**	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Transmission Interval value. Valid values are restricted to 5 - 300 seconds. Default: **30** seconds

Buttons

First: Click to move to the first page.

Previous: Click to move to the previous page.

Next: Click to move to the next page.

Last: Click to move to the last page.

Apply: Click to apply changes.

Refresh: Click to refresh the page; any changes made locally will be undone.

4.12 Diagnostics

This section provide the Physical layer and IP layer network diagnostics tools for troubleshoot. The diagnostic tools are designed for network manager to help them quickly diagnose problems between point to point and better service customers.

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

This section has the following items:

- **Ping Diagnostics**
- **Traceroute**

4.12.1 Ping Diagnostics

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press "**Start**", ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The Ping Diagnostics screen in Figure 4-12-1 appears.

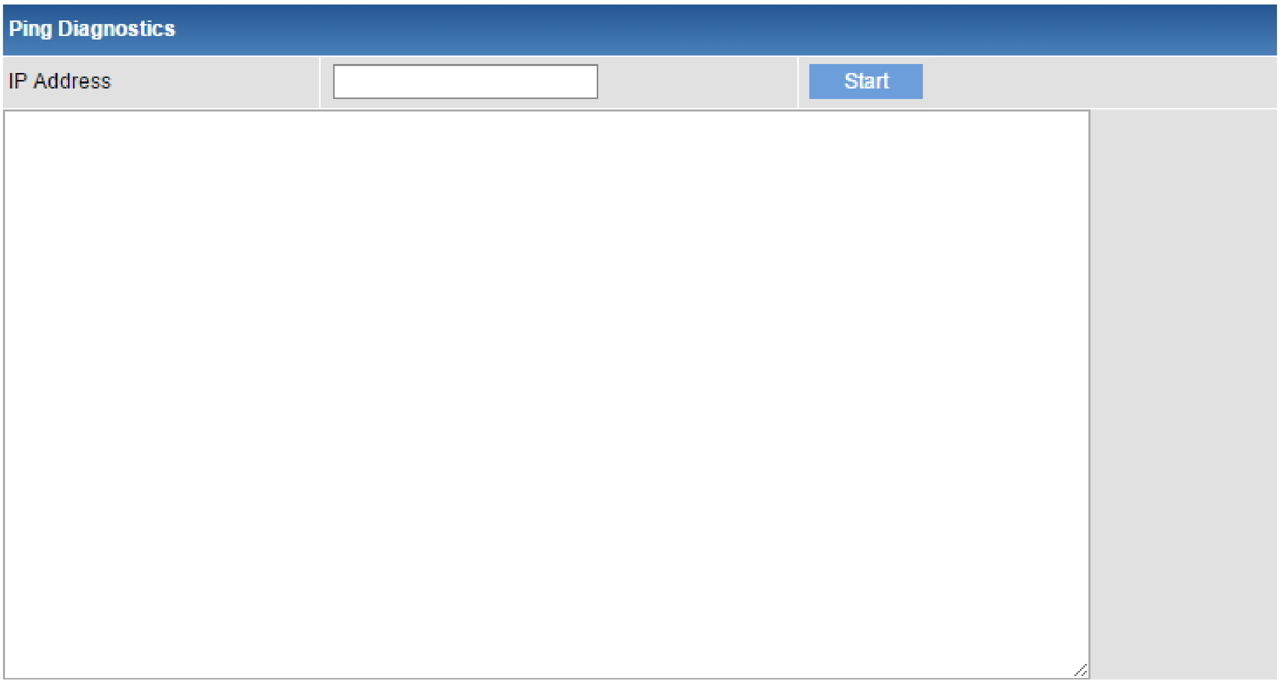


Figure 4-12-1: Ping Diagnostics Page Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address

Buttons

Start : Click to run the applications

4.12.2 Traceroute

Traceroute function is for testing the gateways through which the data packets travel from the source device to the destination device, so to check the network accessibility and locate the network failure.

Execution procedure of the Traceroute function consists of: first a data packet with TTL at 1 is sent to the destination address, if the first hop returns an ICMP error message to inform this packet can not be sent (due to TTL timeout), a data packet with TTL at 2 will be sent. Also the send hop may be a TTL timeout return, but the procedure will carries on till the data packet is sent to its destination. These procedures is for recording every source address which returned ICMP TTL timeout message, so to describe a path the IP data packets traveled to reach the destination. The Traceroute Setting screen in Figure 4-12-2 appears.

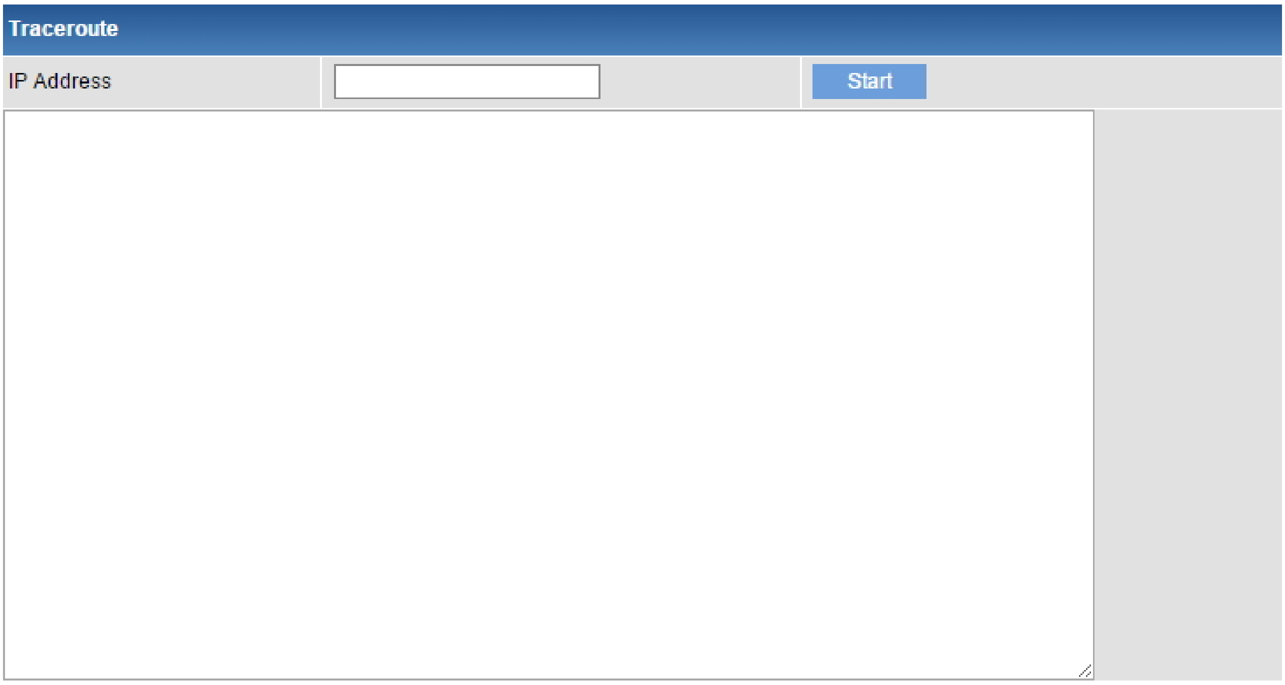


Figure 4-12-2: Traceroute Page Screenshot

The page includes the following fields:

Object	**Description**
• **IP Address**	The destination IP Address

Buttons

Start : Click to run the applications

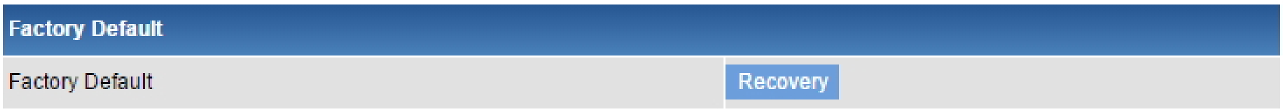
4.13 Maintenance

Use the Maintenance menu items to display and configure basic configurations of the Managed Switch. Under maintenance, the following topics are provided to back up, upgrade, save and restore the configuration. This section has the following items:

■ **Factory Default**	You can reset the configuration of the switch on this page.
■ **Reboot Switch**	You can restart the switch on this page. After restart, the switch will boot normally.
■ **Backup/Upgrade Manager**	You can back up/upgrade the switch settings.

4.13.1 Factory Default

You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in Figure 4-13-1 appears and click to reset the configuration to Factory Defaults.



Factory Default	
Factory Default	Recovery

Figure 4-13-1: Factory Default Configuration Page Screenshot

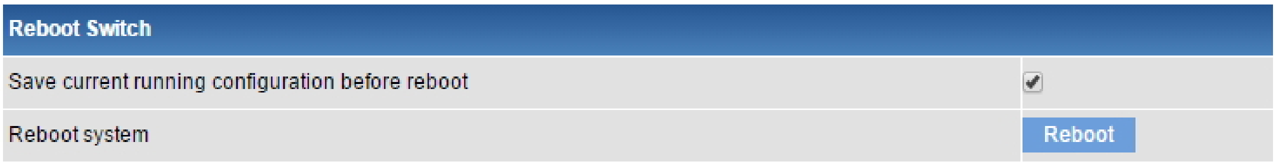
After the "**Recovery**" button is pressed and rebooted, the system will load the default IP settings as follows:

- Default IP address: **192.168.0.100**
- Subnet mask: **255.255.255.0**
- Default Gateway: **192.168.0.254**
- The other setting value is back to disable or none.

> Note
>
> To reset the Managed Switch to the Factory default setting, you can also press the hardware reset button on the front panel for about 10 seconds. After the device is rebooted, you can login the management Web interface within the same subnet of 192.168.0.xx.

4.13.2 Reboot Switch

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user has to re-login the Web interface for about 60 seconds. The Reboot Switch screen in Figure 4-13-2 appears and click to reboot the system.



Reboot Switch	
Save current running configuration before reboot	☑
Reboot system	Reboot

Figure 4-13-2: Reboot Switch Page Screenshot

The page includes the following fields:

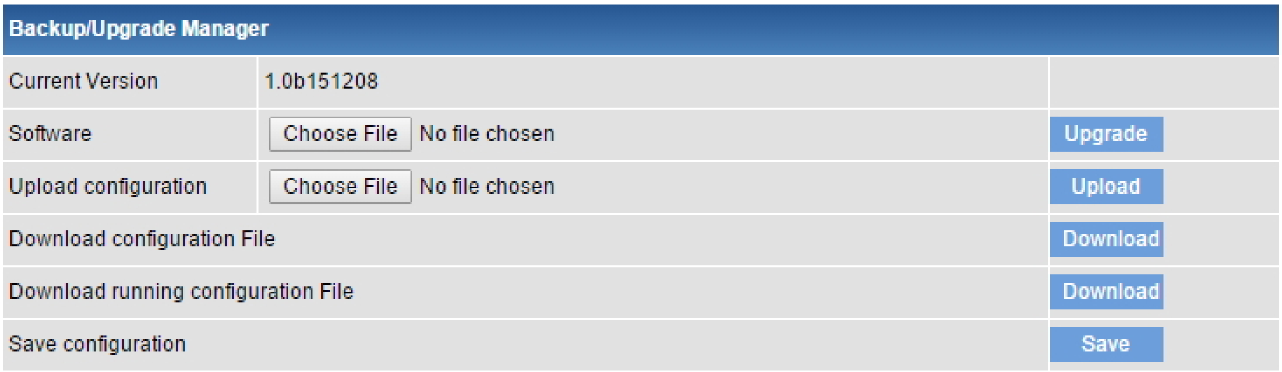
Object	Description
- **Save current running configuration before reboot**	Indicates whether the current running configuration is saved or removed before reboot
- **Reboot system**	Click the Reboot button to restart the switch

Buttons

Reboot : Click to restart the switch.

4.13.3 Backup/Upgrade Manager

This function allows backup/upgrade of the current image or configuration of the Managed Switch to the local management station. The Backup/Upgrade Manager screen in Figure 4-13-3 appears.



Backup/Upgrade Manager		
Current Version	1.0b151208	
Software	Choose File No file chosen	Upgrade
Upload configuration	Choose File No file chosen	Upload
Download configuration File		Download
Download running configuration File		Download
Save configuration		Save

Figure 4-13-3: Reboot Switch Page Screenshot

The page includes the following fields:

Object	Description
Current Version	Displays the current version
Software	Select the firmware to upgrade into the system
Upload configuration	Select the system configuration to upload into the system
Download configuration File	Click to download start-up configuration File
Download running configuration File	Click to download running configuration File
Save configuration	Click to save the configuration

Buttons

Upgrade: Click to upgrade the firmware on the switch.

Upload: Click to upload configuration on the switch.

Download: Click to download configuration on the switch.

Save: Click save the configuration.

5. SWITCH OPERATION

5.1 Address Table

The **Managed Switch** is implemented with an address table. This address table is composed of many entries. Each entry is used to store the address information of some nodes in the network, including MAC address, port no, etc. This information comes from the learning process of **Managed Switch**.

5.2 Learning

When one packet comes in from any port, the **Managed 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 **Managed Switch**, it will also check the destination address besides the source address learning. The **Managed Switch** will look up 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 a different port from this packet comes in, the **Managed Switch** 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 **Managed Switch** stores the incoming frame in an internal buffer and do the complete error checking before transmission. Therefore, no error packets occur; it is the best choice when a network needs efficiency and stability.

The **Managed 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 existence hubs, which nearly always improves the overall performance. An Ethernet switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using the conventional cabling and adapters.

Due to the learning function of the **Managed Switch**, 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 in the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The **Managed Switch** performs **"Store and Fforward"**; 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 detecting the modes and speeds both connected devices are 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.

6. TROUBLESHOOTING

This chapter contains information to help you solve issues. If the Managed Switch is not functioning properly, make sure the Managed 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 Managed Switch.

- **Some stations cannot talk to other stations located on the other port.**

Solution:
Please check the VLAN settings, trunk settings, or port enabled/disabled status.

- **Performance is bad.**

Solution:
Check the full duplex status of the Managed Switch. If the Managed Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

- **Why the Switch doesn't connect to the network.**

Solution:

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

- **1000BASE-T port link LED is lit, but the traffic is irregular.**

Solution:
Check that the attached device is not set to full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

- **Switch does not power up.**

Solution:

1. AC power cord is not inserted or faulty.
2. Check that the AC power cord is inserted correctly.
3. Replace the power cord if the cord is inserted correctly; check that the AC power source is working by connecting a different device in place of the switch.
4. If that device works, refer to the next step.
5. If that device does not work, check the AC power.

APPENDIX A: Networking Connection

A.1 Switch's Data RJ45 Pin Assignments - 1000Mbps, 1000BASE-T

PIN NO	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

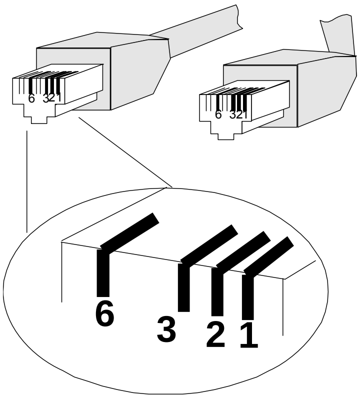
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

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

When connecting your Switch to another Fast Ethernet switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/ connector and their pin assignments:

RJ45 Connector pin assignment		
PIN NO	MDI Media Dependent Interface	MDI-X Media Dependent Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ45 pin assignment



The standard RJ45 receptacle/connector

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

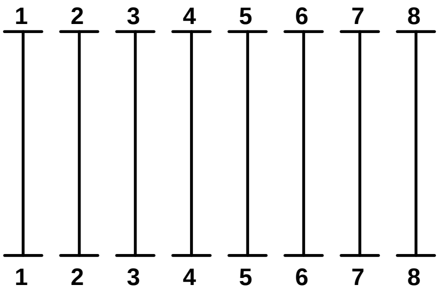
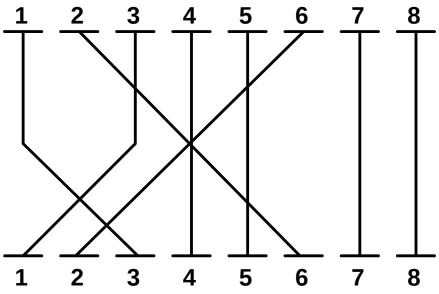
Straight Cable		**SIDE 1**	**SIDE 2**
	**SIDE 1** **SIDE 2**	**1 = White / Orange** **2 = Orange** **3 = White / Green** **4 = Blue** **5 = White / Blue** **6 = Green** **7 = White / Brown** **8 = Brown**	**1 = White / Orange** **2 = Orange** **3 = White / Green** **4 = Blue** **5 = White / Blue** **6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

Figure A-1: Straight-through and Crossover Cable

Please make sure your connected cables are with the same pin assignment and color as the above picture before deploying the cables into your network.

APPENDIX B : GLOSSARY

A

ACE

ACE is an acronym for **A**ccess **C**ontrol **E**ntry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that policy can be associated with a group of ports under the "Ports" web page. There are number of parameters that can be configured with an ACE. Read the web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Port configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List". You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the web page help text for each specific port property.

ACL|Rate Limiters: On this page, you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1 to 1024K packets per second. Under "Ports" and "Access Control List", you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for **A**dvanced **E**ncryption **S**tandard. The encryption key protocol is applied in 802.1x standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for **A**uto **M**edia **S**elect. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if an SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the prefered media.

APS

APS is an acronym for **A**utomatic **P**rotection **S**witching. This protocol is used to secure switching that is done bidirectional in both ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also *Port Aggregation, Link Aggregation*).

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for **C**ontinuity **C**heck. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for **C**ontinuity **C**heck **M**essage. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for **C**isco **D**iscovery **P**rotocol.

D

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID. The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for **D**enial of **S**ervice. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.
An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for **F**ile **T**ransfer **P**rotocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

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

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested web page. The other main standard that controls how the World Wide Web works is HTML, which covers how web pages are formatted and displayed.

Any Web server machine contains, in addition to the web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for **I**nternet **M**essage **A**ccess **P**rotocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across a internet network.

IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP** **M**ulti**C**ast.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol allows bundling several physical ports together to form a single logical port.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The **L**ink **L**ayer **D**iscovery **P**rotocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC

LOC is an acronym for **L**oss **O**f **C**onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for **M**aintenance **E**ntity **E**ndpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for **M**essage-**D**igest algorithm **5**. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs. The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for **Net**work **B**asic **I**nput/**O**utput **S**ystem. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for **N**etwork **F**ile **S**ystem. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM is an acronym for **O**peration **A**dministration and **M**aintenance. It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs.

An LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch includes the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of an MAC address.

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for **P**owered **D**evice. In a PoE> system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The Ping Request is the packet from the origin computer, and the Ping Reply is the packet response from the target.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for **P**ost **O**ffice **P**rotocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet. It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for **Q**oS **C**ontrol **L**ist. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for **Q**uality **of** **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **Re**mote **A**uthentication **D**ial In **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for **R**emote **D**efect **I**ndication. It is an OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SHA

SHA is an acronym for **S**ecure **H**ash **A**lgorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack **P**rotocol using **ROU**ting **T**echnology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service **S**et **Id**entifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for **S**ecure **SH**ell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **Tel**etype **Net**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provides directory service and security features.

Toss

Toss is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 Toss priority control. It is fully decoded to determine the priority from the 6-bit Toss field in the IP header. The most significant 6 bits of the Toss field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for **T**emporal **K**ey **I**ntegrity **P**rotocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame.

V

VLAN

A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP

WEP is an acronym for **W**ired **E**quivalent **P**rivacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

Wi-Fi

Wi-Fi is an acronym for **Wi**reless **Fi**delity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for **W**i-Fi **P**rotected **A**ccess. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for **W**i-Fi **P**rotected **A**ccess - **P**re **S**hared **K**ey. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for **W**i-Fi **P**rotected **A**ccess - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for **W**i-Fi **P**rotected **S**etup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for **W**eighted **R**andom **E**arly **D**etection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for **W**ait **T**o **R**estore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.