User's Manual

WGSW-24040 / WGSW-24040R

24-Port 10/100/1000Mbps
Layer 2 Managed Switch

SGSW-24040 / SGSW-24040R

24-Port 10/100/1000Mbps
Layer 2 Managed Stackable Switch

SGSW-24040P / SGSW-24040P4

24G PoE Managed Stackable Switch

SGSW-24240 / SGSW-24240R

24-Port 100/1000 SFP
Fiber Managed Stackable Switch

Trademarks

Copyright © PLANET Technology Corp. 2009.

Contents subject to which revision without prior notice.

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

Disclaimer

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

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

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

FCC Warning

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

CE Mark Warning

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

WEEE Warning

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

Revision

PLANET 24-Port 10/100/1000Mbps with 4 Shared SFP Combo Managed Switch User's Manual

FOR MODELS: WGSW-24040 / WGSW-24040R / SGSW-24040 / SGSW-24040R / SGSW-24040P / SGSW-24040P4 / SGSW-24240 / SGSW-24240R

REVISION: 1.2 (MARCH.2009)

Part No: EM-WGSW-24040_SGSW-24040 (2080-A93070-001)

TABLE OF CONETNTS

1. INTRODUTION

The PLANET Layer 2 Managed Gigabit Switch series – WGSW standalone, SGSW Stackable, SGSW PoE and SGSW Fiber switch are all multiple ports Gigabit Ethernet Switched with SFP fiber optical connective ability and robust layer 2 features; the description of these models as below:

WGSW-24040	:	24-Port 10/100/1000Base-T with 4 Shared SFP Managed Gigabit Switch
WGSW-24040R	:	24-Port 10/100/1000Base-T with 4 Shared SFP Managed Gigabit Switch / Redundant Power
SGSW-24040	:	24-Port 10/100/1000Base-T with 4 Shared SFP Managed Stackable Switch
SGSW-24040R	:	24-Port 10/100/1000Base-T with 4 Shared SFP Managed Stackable Switch / Redundant Power
SGSW-24040P		24-Port 10/100/1000Base-T PoE Managed Stackable Switch / 220W
SGSW-24040P4		24-Port 10/100/1000Base-T PoE Managed Stackable Switch / 380W
SGSW-24240		24-Port 100/1000Base-X with 8 Shared TP Managed Stackable Switch
SGSW-24240R		24-Port 100/1000Base-X with 8 Shared TP Managed Stackable Switch / Redundant Power

Terms of "**Managed Switch**" means the Switches mentioned titled in the cover page of this User's manual, i.e.WGSW-24040 and SGSW-24040.

1.1 Packet Contents

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

Check the contents of your package for following parts:

☑ **The Managed Switch**   x1

☑ **User's manual CD**   x1

☑ **Quick installation guide**   x1

☑ **19" Rack mount accessory kit**   x1

☑ **Power cord**   x1

☑ **Rubber feet**   X4

☑ **RS-232 DB9 male Console cable**   x1

☑ **CB-STX50 – 50cm stack cable**   x1

    (SGSW Series only)

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

1.2 Product Description

High-Performance / Cost-effective / Telecom class Gigabit solution for Enterprise backbone and Data Center Networking

The PLANET Managed Switch is a L2/L4 Managed Gigabit Switch. Since Gigabit network interface had become the basic equipment and requirement of Enterprise and Network Servers, with 48Gbps switching fabric, the MANAGED SWITCH can handle extremely large amounts of data in a secure topology linking to a backbone or high capacity servers. The powerful QoS and Network Security features make it to meets the needs of effective data traffic control for both Campus and Enterprise, such VoIP, video streaming and multicast application.

High Performance

The Managed Switch provides 24 10/100/1000Mbps Gigabit Ethernet ports with 4 shared Gigabit SFP slots. It boasts a high performance switch architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as 48Gbps, which greatly simplifies the tasks of upgrading the LAN for catering to increase bandwidth demands.

Robust Layer 2 Features

The Managed can be programmed for basic switch management functions such as port speed configuration, Port aggregation, VLAN, Spanning Tree protocol, QoS, bandwidth control and IGMP Snooping. The WGSW-24040 provides 802.1Q Tagged VLAN, Q-in-Q VLAN trunning and private VLAN, the VLAN groups allowed on the WGSW-24040 will be maximally up to 255. Via supporting port aggregation, the Managed Switch allows the operation of a high-speed trunk combining multiple ports, up to eight groups of maximum to 8-ports for trunking, and it supports fail-over as well.

Excellent Traffic Control

PLANET WGSW-24040 is loaded with powerful traffic management and QoS features to enhance services offered by telecoms. The functionality includes QoS features such as wire-speed Layer 4 traffic classifiers and bandwidth limiting that are particular useful for multi-tenant unit, multi business unit, Telco, or Network Service Provide applications. It also empowers the enterprises to take full advantages of the limited network resources and guarantees the best performance at VoIP and Video conferencing transmission.

Efficient Management

For efficient management, the series of Managed Switch is equipped with console, WEB and SNMP management interfaces. With its built-in Web-based management, it offers an easy-to-use, platform-independent management and configuration facility. The Managed Switch supports standard Simple Network Management Protocol (SNMP) and can be managed via any standard-based management software. For text-based management, it can also be accessed via Telnet and the console port.

Powerful Security

The Managed Switch offers comprehensive Access Control List (ACL) for enforcing security to the edge. Its protection mechanisms also comprise of port-based 802.1x and MAC-based user and device authentication. The port-security is effective in limit the numbers of clients pass through, so that network administrators can now construct highly secured corporate networks with time and effort considerably less than before.

Flexibility and Extension solution

The 4 mini-GBIC slots are compatible with 1000Base-SX/LX and WDM SFP(Small Factor Pluggable) fiber-optic modules. The distance can be extended from 550 meters (Multi-Mode fiber) up to above 10/50/70/120 kilometers (Single-Mode fiber or WDM fiber). They are well suited for using within the enterprise data centers and distributions.

Reliability Stacking Management

The SGSW Series Managed Switch provides a switch stacking function to manage up to 16 switches using a single IP address. That helps network managers to easily configure switches via one single IP address instead of connecting and setting each unit one by one. Through its high bandwidth tunnel and stacking technology, it gives enterprise, service provider and telcom flexible control over port density, uplinks and switch stack performance. Up to 384 Gigabit Ethernet ports can be managed by a stacking group and you can add ports and functionality as needed. The stacking technology also enables the advantages of chassis-based switches to be integrated into SGSW Series Managed Switch, but without the expensive up-front cost.

AC / DC Power Redundant to ensure continuous operation

The R series Managed Switch equip with one 100~240V AC power supply unit and one DC -48V power supply unit on its standard package, it provides redundant power supply installation. A redundant power system is also provided to enhance the reliability with either 100~240V AC power supply unit or DC -48V power supply unit. The continuous power systems are specifically designed to handle the demands of high tech facilities requiring the highest power integrity available.

Advanced Features and Centralized Power Management for Enterprise and Campus PoE Networking (PoE Model)

The PLANET SGSW-24040P series PoE Switch provides 24 10/100/1000Mbps Power-over-Ethernet (PoE, IEEE 802.3af compliant) ports which optimize the installation and power management of network devices such as wireless access points (AP), Voice over IP (VoIP) phones, and security video cameras. The PoE capabilities also help to reduce deployment costs for network devices like the wireless AP as a result of freeing from restrictions of power outlet locations. Power and data switching are integrated into one unit and delivered over a single cable. It thus eliminates cost for additional AC wiring and reduces installation time.

The below table lists the major hardware diference between the series model:

Model		WGSW-24040	WGSW-24040R	SGSW-24040	SGSW-24040R	SGSW-24240	SGSW-24240R	SGSW-24040P SGSW-24040P4
Interface	10/100/1000 T	24	24	24	24	8	8	24
	1000SX/LX	4	4	4	4	24, 100FX compatible	24, 100FX compatible	4
Redundant Power		-	-48V DC (-30V~-60V)	-	-48V DC (-30V~-60V)	-	-48V DC (-30V~-60V)	-
Power over Ethernet		-	-	-	-	-	-	IEEE 802.3af
PoE Budget		-	-	-	-	-	-	220W / 380W
Stack Capability		-	-	Hardware stacking, up to 16 units				

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, **INSTALLATION**

The section explains the functions of the 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, **COMMAND LINE INTERFACE**

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

Section 6, **CLI CONFIGURATION**

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

Section 7, **SWITCH OPERATION**

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

Section 8, **POWER OVER ETHERNET OVERVIEW**

The chapter introduce the IEEE 802.3af PoE standard and PoE provision of the Managed Switch.

Section 9, **TROUBSHOOTING**

The chapter explains how to trouble shooting of the Managed Switch.

Appendix A

The section contains cable information of the Managed Switch.

1.4 Product Features

➢ **Physical Port**

WGSW-24040 / WGSW-24040R

■ **24-Port 10/100/1000Base-T** Gigabit Ethernet RJ-45

■ **4 mini-GBIC/SFP slots**, shared with Port-21 to Port-24

■ **RS-232** DB9 console interface for Switch basic management and setup

SGSW-24040 / SGSW-24040R

■ **24-Port 10/100/1000Base-T** Gigabit Ethernet RJ-45

■ **4 mini-GBIC/SFP slots**, shared with Port-21 to Port-24

■ **RS-232** DB9 console interface for Switch basic management and setup

■ **2 High-performance 5GbE** Stacking interface

SGSW-24040P / SGSW-24040P4

■ **24-Port 10/100/1000Base-T** Gigabit Ethernet RJ-45 with **IEEE 802.3af PoE** Injector

■ **4 mini-GBIC/SFP slots**, shared with Port-21 to Port-24

■ **RS-232** DB9 console interface for Switch basic management and setup

■ **2 High-performance 5GbE** Stacking interface

SGSW-24240 / SGSW-24240R

■ **24 100/1000Base-X mini-GBIC/SFP slots**

■ **8-Port 10/100/1000Base-T** Gigabit Ethernet RJ-45, shared with Port-1 to Port-8

■ **RS-232** DB9 console interface for Switch basic management and setup

■ **2 High-performance 5GbE** Stacking interface

➢ **Layer 2 Features**

■ Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standard

■ Supports Auto-negotiation and half duplex/full duplex modes for all 10Base-T/100Base-TX and 1000Base-T ports.

■ Auto-MDI/MDI-X detection for each RJ-45 port

■ Prevents packet loss with back pressure (Half-Duplex) and IEEE 802.3x PAUSE frame flow control (Full-Duplex)

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

■ 8K MAC address table, automatic source address learning and ageing

■ 1392Kbytes embedded memory for packet buffers

■ Support VLAN

  – IEEE 802.1Q Tagged VLAN

  – Up to 255 VLANs groups, out of 4041 VLAN IDs

  – Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)

- Private VLAN Edge (PVE)
■ Support Spanning Tree Protocol

- STP, IEEE 802.1d (Spanning Tree Protocol)

- RSTP, IEEE 802.1w (Rapid Spanning Tree Protocol)

■ Support Link Aggregation

- 802.3ad Link Aggregation Control Protocol (LACP)

- Cisco ether-channel (Static Trunk)

- Maximum 12 trunk groups, up to 16 ports per trunk group

- Up to 16Gbps bandwidth(Duplex Mode)

■ Provide Port Mirror (many-to-1)

■ Port Mirroring to monitor the incoming or outgoing traffic on a particular port

➢ **Quality of Service**

■ 4 priority queues on all switch ports.

■ Supports for strict priority and weighted round robin (WRR) CoS policies

■ Ingress Shaper and Egress Rate Limit per port bandwidth control

■ Traffic-policing policies on the switch port

➢ **Multicast**

■ Supports IGMP Snooping v1, v2 and v3

■ Querier mode support

➢ **Security**

■ IEEE 802.1x Port-Based / MAC-Based network access authentication

■ IP-Based Access Control List (ACL)

■ MAC-Based Access Control List

➢ **Management**

■ WEB-based, Telnet, Console Command Line management

■ Accesses through SNMPv1, v2c and v3 security set and get requests.

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

■ BOOTP and DHCP for IP address assignment

■ Firmware upload/download via HTTP / TFTP

■ SNTP (Simple Network Time Protocol)

■ LLDP Protocol

➢ **Stacking**

■ Hardware stack up to 16 units and 384 ports

■ Stacking architecture supports Chain and Ring mode

■ Mirror across stack

■ Link Aggregation groups spanning multiple switches in a stack

■ Hardware learning with MAC table synchronization across stack

➢ **Redundant Power System** (WGSW-24040R / SGSW-24040R)

■ 100~240V AC / 48V DC Dual power redundant

■ Active-active redundant power failure protection

■ Backup of catastrophic power failure on one supply

■ Fault tolerance and resilience.

➢ **Power over Ethernet   (SGSW-24040P / SGSW-24040P4 Only)**

■ Complies with IEEE 802.3af Power over Ethernet End-Span PSE

■ Up to 24 IEEE 802.3af devices powered

■ Support PoE Power up to 15.4 watts for each PoE ports

■ Auto detect powered device (PD)

■ Circuit protection prevent power interference between ports

■ Remote power feeding up to 100m

■ PoE Management

■ Total PoE power budget control

■ Pert port PoE function enable/disable

■ PoE Port Power feeding priority

■ Per PoE port power limit

■ PD classification detection

1.5 Product Specification

■ **WGSW Standalone models**

Product	WGSW-24040	WGSW-24040R
Hardware Specification		
Copper Ports	24 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports	
SFP/mini-GBIC Slots	4 SFP interfaces, shared with Port-21 to Port-24	
Stacking Ports	---	
Switch Fabric	48Gbps / non-blocking	
Address Table	8K entries	
Share data Buffer	1392 kilobytes	
Switch Processing Scheme	Store-and-Forward	
Flow Control	IEEE 802.3x Pause Frame for Full-Duplex Back pressure for Half-Duplex	

Jumbo Frame	10Kbytes
LED	Power, Link/Act and speed per Gigabit port
Power Consumption	Max. 30 watts / 102 BTU
Power Requirement – AC	AC 100~240V, 50/60Hz	AC : 100~240V, 50/60Hz
Power Requirement – DC	---	-48V DC @ 0.6A Range: -30 ~ -60V
Stacking Numbers	---
Stacking Bandwidth	---
Stack ID Display	---

■ **SGSW Stackable / Fiber models**

Product	SGSW-24040	SGSW-24040R	SGSW-24240	SGSW-24240R
Hardware Specification				
Copper Ports	24 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports		8 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports, shared with Port-1~Port-8	
SFP/mini-GBIC Slots	4 SFP interfaces, shared with Port-21 to Port-24		24 100/1000Base-X Dual Speed SFP interfaces	
Stacking Ports	2 5GbE / Cross-HDMI interface			
Switch Fabric	68Gbps			
Address Table	8K entries			
Share data Buffer	1392 kilobytes			
Switch Processing Scheme	Store-and-Forward			
Flow Control	IEEE 802.3x Pause Frame for Full-Duplex Back pressure for Half-Duplex			
Jumbo Frame	10Kbytes			
LED	Power, Stack Master, Stack Port LNK, Link/Act and speed per Gigabit port			
Power Consumption	Max. 30.2 watts / 102.98 BTU	Max. 30.2 watts / 102.98 BTU	Max. 33.2 watts / 113.21 BTU	Max. 33.2 watts / 113.21 BTU
Power Requirement – AC	AC 100~240V, 50/60Hz	AC : 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC : 100~240V, 50/60Hz
Power Requirement – DC	---	-48V DC @ 0.6A Range: -30 ~ -60V	---	-48V DC @ 0.6A Range: -30 ~ -60V
Stacking Numbers	16			
Stacking Bandwidth	10Gbps Full-Duplex			
Stack ID Display	7-Segment LED Display (1~9, A~F,0)			

■   **SGSW Stackable PoE models**

Product	SGSW-24040P	SGSW-24040P4
Hardware Specification		
Copper Ports	24 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports	
SFP/mini-GBIC Slots	4 SFP interfaces, shared with Port-21 to Port-24	
Stacking Ports	2 5GbE / Cross-HDMI interface	
Switch Fabric	68Gbps	
Address Table	8K entries	
Share data Buffer	1392 kilobytes	
Switch Processing Scheme	Store-and-Forward	
Flow Control	IEEE 802.3x Pause Frame for Full-Duplex Back pressure for Half-Duplex	
Jumbo Frame	10Kbytes	
LED	Power, Stack Master, Stack Port LNK, Link/Act and speed per Gigabit port	
Power Consumption	Max. 290 watts / 989 BTU	Max. 430.2 watts / 1467 BTU
Power Requirement – AC	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz
Power Requirement – DC	----	---
Stacking Numbers	16	
Stacking Bandwidth	10Gbps Full-Duplex	
Stack ID Display	7-Segment LED Display (1~9, A~F,0)	
Power over Ethernet		
PoE Standard	IEEE 802.3af Power over Ethernet / PSE	
PoE Power Supply Type	End-Span	
PoE Power Output	Per Port 48V DC, 350mA . Max. 15.4 watts	
Power Pin Assignment	1/2(+), 3/6(-)	
PoE Power Budget	220 Watts	380 Watts
PoE Ability — Number of PD @ 7Watts	24	24
PoE Ability — Number of PD @ 15.4Watts	14	24

■   **WGSW / SGSW all models**

Product	All Models
Layer 2 function	
System Configuration	Console, Telnet, Web Browser, SNMPv1, v2c and v3
Port configuration	Port disable/enable. Auto-negotiation 10/100/1000Mbps full and half duplex mode selection. Flow Control disable / enable. Bandwidth control on each port.
Port Status	Display each port's speed duplex mode, link status, Flow control status. Auto negotiation status, trunk status.
VLAN	802.1Q Tagged Based VLAN ,up to 255 VLAN groups Q-in-Q Private VLAN
Port trunking	IEEE 802.3ad LACP / Static Trunk Support 12 groups of 16-Port trunk support

QoS	Traffic classification based, Strict priority and WRR
	 4-level priority for switching
	   - Port Number
	   - 802.1p priority
	   - DS/TOS field in IP Packet

IGMP Snooping	IGMP (v1/v2) Snooping, up to 255 multicast Groups IGMP Querier mode support
Access Control List	IP-Based ACL / MAC-Based ACL Up to 256 entries
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-1643 Ethernet MIB RFC-2863 Interface MIB RFC-2665 Ether-Like MIB RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC-2933 IGMP-STD-MIB () RFC3411 SNMP-Frameworks-MIB IEEE802.1X PAE LLDP MAU-MIB
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE

Standards Compliance	IEEE 802.3 10Base-T
	IEEE 802.3u 100Base-TX/100BASE-FX
	IEEE 802.3z Gigabit SX/LX
	IEEE 802.3ab Gigabit 1000T
	IEEE 802.3x Flow Control and Back pressure
	IEEE 802.3ad Port trunk with LACP
	IEEE 802.1d Spanning tree protocol
	IEEE 802.1w Rapid spanning tree protocol
	IEEE 802.1p Class of service
	IEEE 802.1Q VLAN Tagging
	IEEE 802.1x Port Authentication Network Control
	IEEE 802.1ab LLDP

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 unit front panel provides a simple interface monitoring the switch. Figure 2-1 to 2-4 show the front panel of the Managed Switches.

WGSW-24040 / WGSW-24040RFront Panel
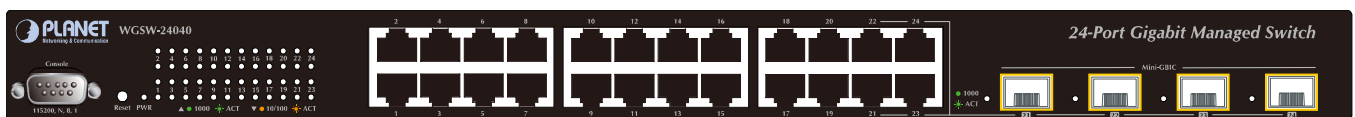
Figure 2-1 WGSW-24040 / WGSW-24040R front panel.

SGSW-24040 / SGSW-24040R Front Panel
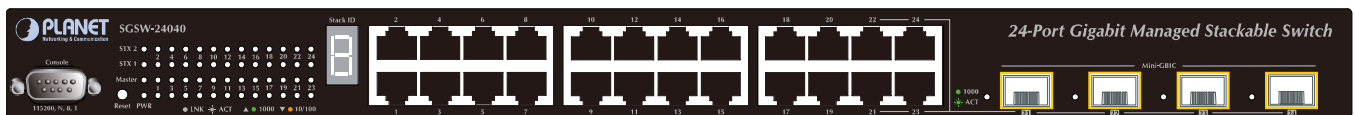
Figure 2-2 SGSW-24040 / SGSW-24040R front panel.

SGSW-24040P / SGSW-24040P4 Front Panel
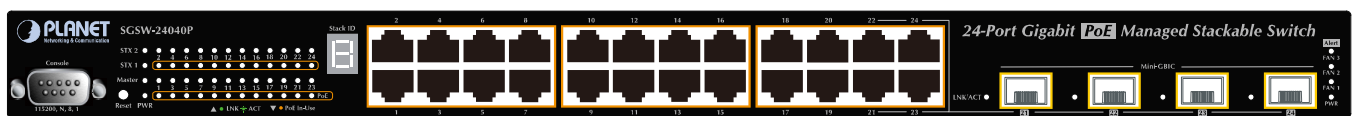
Figure 2-3 SGSW-24040P / SGSW-24040P4 front panel.

SGSW-24240 / SGSW-24240R Front Panel

Figure 2-4 SGSW-24240 / SGSW-24240R front panel.

24

■ **Gigabit TP interface**

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

■ **Gigabit SFP slots**

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

■ **Console Port**

The console port is a DB9, RS-232 male seria port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information includes IP Address setting, factory reset, port management, link status and system setting. Users can use the attached RS-232 cable in the package and connect to the console port on the device. After the connection, users an run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the statup screen of the device.

■ **Reset button**

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

Reset Button Pressed and Released	Function
About **1~3 second**	Reboot the Managed Switch
Until the **PWR** LED lit **off**	Reset the Managed Switch to Factory Default configuration. The Managed Switch will then reboot and load the default settings as below: ◦ Default Password: **admin** ◦ Default IP address: **192.168.0.100** ◦ Subnet mask: **255.255.255.0** ◦ Default Gateway: **192.168.0.254**

■ **Stack ID**

SGSW Series only

Each SGSW Managed Stackable Switch on a stack must have a unique "Stack ID". There are 16 degrees (0~9, A~F) in the rotary switch. The Stack ID is configured via Web or CLI management interface. Use the Stack ID to identify the localtion of the real device.

Note	Stack ID is not equals to the Master Priority that configured in the management interface.

■ **Master LED**

SGSW Series only

If master switch is fail or disconnected to the switch by stack port, the switch with least switch ID will become master.

2.1.2 LED Indications

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

WGSW-24040 / WGSW-24040R LED indication
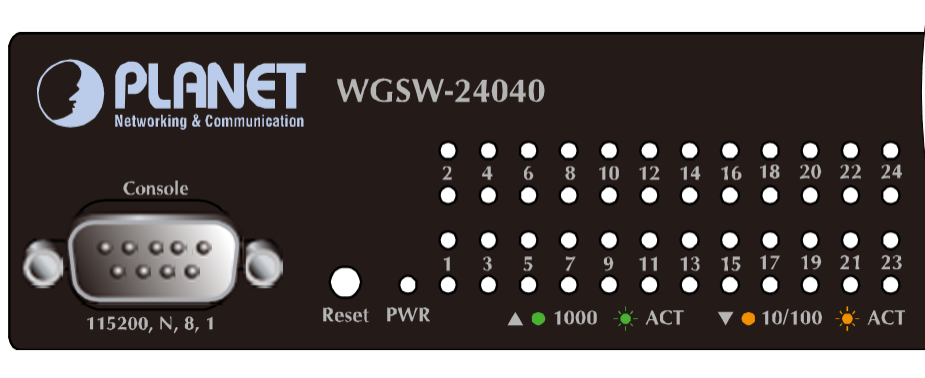
Figure 2-5 WGSW-24040 / WGSW-24040R LED panel

■ **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate that the Switch is powered on. **Blink** to indicate the System is running under booting procedure.

■ **10/100/1000Base-T interfaces**

LED	Color	Function
1000 **LNK/ACT**	**Green**	**Lights:** To indicate the link through that port is successfully established with speed **1000Mbps**
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If L10/100 NK/ACT LED light-> indicate that the port is operating at 10Mbps or 100Mbps If LNK/ACT LED Off -> indicate that the port is link down
10/100 **LNK/ACT**	**Orange**	**Lights:** To indicate the link through that port is successfully established with speed 10Mbps or 100Mbps
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If 1000 LNK/ACT LED light-> indicate that the port is operating at 1000Mbps If 1000 LNK/ACT LED Off -> indicate that the port is link down

■ **1000Base-SX/LX SFP interfaces (Shared Port-21~Port-24)**

LED	Color	Function
1000 LNK	Green	**Lights:** To indicate the link through that SFP port is successfully established with speed **1000Mbps**
		Off: To indicate that the SFP port is link down

SGSW-24040 / SGSW-24040R LED indication
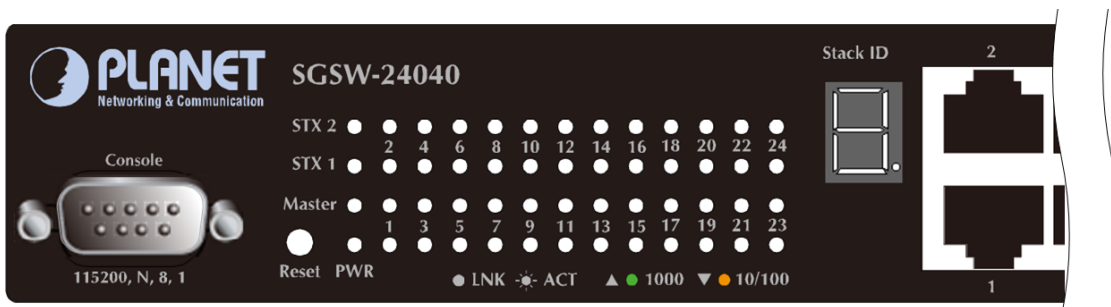
Figure 2-6 SGSW-24040 / SGSW-24040R LED panel

■ **System**

LED	Color	Function
PWR	Green	**Lights** to indicate that the Switch is powered on. **Blink** to indicate the System is running under booting procedure.
Master	Green	**Lights** to indicate that the Switch is the Master of the stack group
STX1	Green	**Lights** to indicate the stacking link through that port is successfully established.
STX2	Green	**Lights** to indicate the stacking link through that port is successfully established.

■ **10/100/1000Base-T interfaces**

LED	Color	Function
1000 LNK/ACT	Green	**Lights:** To indicate the link through that port is successfully established with speed **1000Mbps**
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If L10/100 NK/ACT LED light-> indicate that the port is operating at 10Mbps or 100Mbps. If LNK/ACT LED Off -> indicate that the port is link down

10/100 LNK/ACT	**Orange**	**Lights:** To indicate the link through that port is successfully established with speed 10Mbps or 100Mbps
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If 1000 LNK/ACT LED light-> indicate that the port is operating at 1000Mbps If 1000 LNK/ACT LED Off -> indicate that the port is link down

■ **1000Base-SX/LX SFP interfaces (Shared Port-21~Port-24)**

LED	Color	Function
1000 LNK	**Green**	**Lights:** To indicate the link through that SFP port is successfully established with speed **1000Mbps**
		Off: To indicate that the SFP port is link down

SGSW-24040P / SGSW-24040P4 LED indication
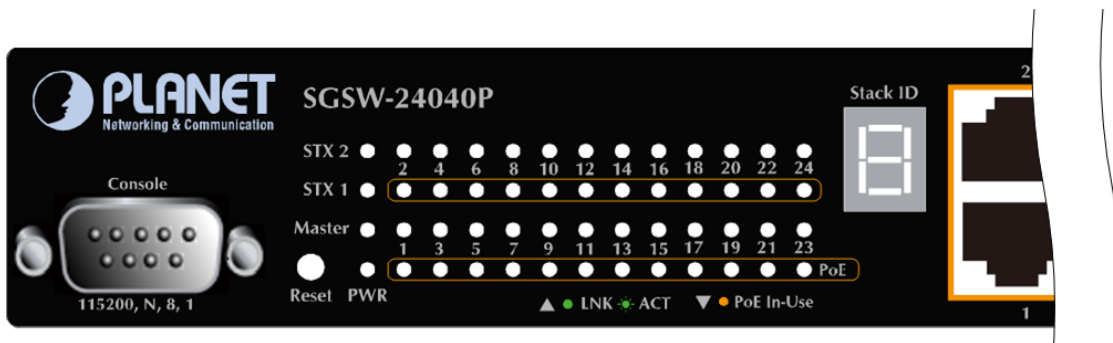
Figure 2-7 SGSW-24040P / SGSW-24040P4 LED panel

■ **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate that the Switch is powered on. **Blink** to indicate the System is running under booting procedure.
Master	**Green**	**Lights** to indicate that the Switch is the Master of the stack group
STX1	**Green**	**Lights** to indicate the stacking link through that port is successfully established.
STX2	**Green**	**Lights** to indicate the stacking link through that port is successfully established.

■ **Alert**

LED	Color	Function
PWR Alert	**Green**	**Lights** to indicate that the power supply failure

28

FAN1 Alert	**Green**	**Lights** to indicate that the FAN1 failure
FAN2 Alert	**Green**	**Lights** to indicate that the FAN2 failure
FAN3 Alert	**Green**	**Lights** to indicate that the FAN3 failure

■ **10/100/1000Base-T interfaces**

LED	Color	Function
10/100/1000 **LNK/ACT**	**Green**	**Lights:** To indicate the link through that port is successfully established with speed 10Mbps or 100Mbps or **1000Mbps**
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If L10/100 NK/ACT LED light-> indicate that the port is operating at 10Mbps or 100Mbps If LNK/ACT LED Off -> indicate that the port is link down
PoE In-Use	**Orange**	**Lights**: To indicate the port is providing 48VDC in-line power
		Off: To indicate the connected device is not a PoE Powered Device (PD)

■ **1000Base-SX/LX SFP interfaces (Shared Port-21~Port-24)**

LED	Color	Function
1000 **LNK**	**Green**	**Lights:** To indicate the link through that SFP port is successfully established with speed **1000Mbps**
		Off: To indicate that the SFP port is link down

SGSW-24240 / SGSW-24240R LED indication
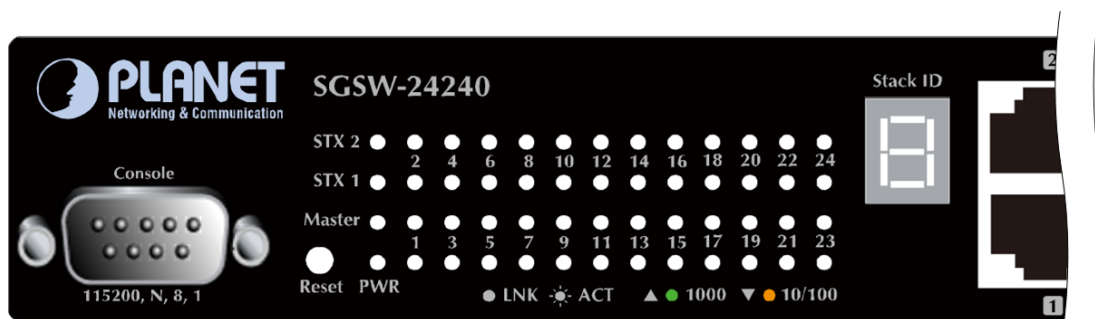
Figure 2-8 SGSW-24240 / SGSW-24240R LED panel

■ **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate that the Switch is powered on. **Blink** to indicate the System is running under booting procedure.
Master	**Green**	**Lights** to indicate that the Switch is the Master of the stack group
STX1	**Green**	**Lights** to indicate the stacking link through that port is successfully established.
STX2	**Green**	**Lights** to indicate the stacking link through that port is successfully established.

■ **10/100/1000Base-T interfaces   (Shared Port-1~Port-8)**

LED	Color	Function
1000 LNK/ACT	**Green**	**Lights:** To indicate the link through that port is successfully established with speed **1000Mbps**
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If L10/100 NK/ACT LED light-> indicate that the port is operating at 10Mbps or 100Mbps If LNK/ACT LED Off -> indicate that the port is link down
10/100 LNK/ACT	**Orange**	**Lights:** To indicate the link through that port is successfully established with speed 10Mbps or 100Mbps
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If 1000 LNK/ACT LED light-> indicate that the port is operating at 1000Mbps If 1000 LNK/ACT LED Off -> indicate that the port is link down

■ **100 / 1000Base-X SFP interfaces**

LED	Color	Function
1000 LNK	**Green**	**Lights:** To indicate the link through that SFP port is successfully established with speed **1000Mbps**
		Off: To indicate that the SFP port is link down
100 LNK/ACT	**Orange**	**Lights:** To indicate the link through that port is successfully established with speed 100Mbps
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If 1000 LNK/ACT LED light-> indicate that the port is operating at 1000Mbps If 1000 LNK/ACT LED Off -> indicate that the port is link down

■ **7-Segment LED Display**

Stack ID (1~9, A~F, 0): To indicate the **Switch ID** of each SGSW Managed Switch. Switch IDs are used to uniquely identify the Managed Switches within a stack. The Switch ID of each Managed Switch is shown on the display on the front of the Managed Switch and is used widely in the web pages as well as in the CLI commands of the Stack group.

Stack ID	1	2	3	4	5	6	7	8	9	A.	B.	C.	D.	E.	F.	0
Switch ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

2.1.3 Switch Rear Panel

The rear panel of the Managed Switch indicates an AC inlet power socket, which accept input power from 100 to 240V AC, 50-60Hz. Figure 2-5 to Figure 2-8 shows the rear panel of these Managed Switches

WGSW-24040 Rear Panel

Figure 2-9 Rear panel of **WGSW-24040**

WGSW-24040R Rear Panel

Figure 2-10 Rear panel of **WGSW-24040R**

SGSW-24040 Rear Panel

Figure 2-11 Rear panel of **SGSW-24040**

SGSW-24040R Rear Panel

Figure 2-12 Rear panel of **SGSW-24040R**

SGSW-24040P / SGSW-24040P4 Rear Panel

Figure 2-13 Rear panel of **SGSW-24040P** / **SGSW-24040P4**

SGSW-24240 Rear Panel

Figure 2-14 Rear panel of **SGSW-24240**

SGSW-24240R Rear Panel

Figure 2-15 Rear panel of **SGSW-24240R**

■ **AC Power Receptacle**

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

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

Power Notice:

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

In some area, 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.

■ **Stack ports**

SGSW-24040 / SGSW-24040R

There are two High-Performance stack ports on the rear panel. One is **STX1 / Cascade Down** and the other is **STX2 / Cascade UP**.

- When stacked, the **STX1 / Cascade Down** port should connect to the other switch's **STX2 / Cascade UP** port and the **STX2 / Cascade UP** port should connect to other switch's **STX1 / Cascade Down** out.

- You can just use attached PLANET CB-STX50 or longer stack cable CB-STX200 connector to stack.

32

- The CB-STX50 and CB-STX200 are Cross-Overed HDMI cables, only attached PLANET stack cable can be used.

- Plug-and-play connection.
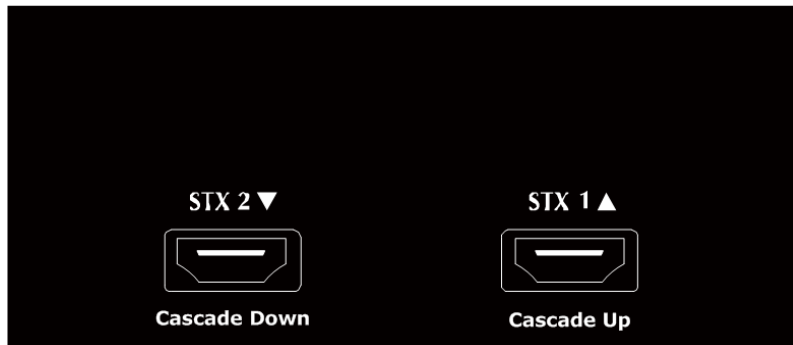
Figure 2-16 SGSW-24040 / SGSW-24040R Stack Ports

■ **DC Power Connector**

The rear panel of the WGSW-24040R and SGSW-24040R contains a power switch and a DC power connector, which accepts DC power input voltage from -30V to -60V DC. Connect the power cable to the Managed Switch at the input terminal block. The size of the two screws in the terminal block is M3.5.
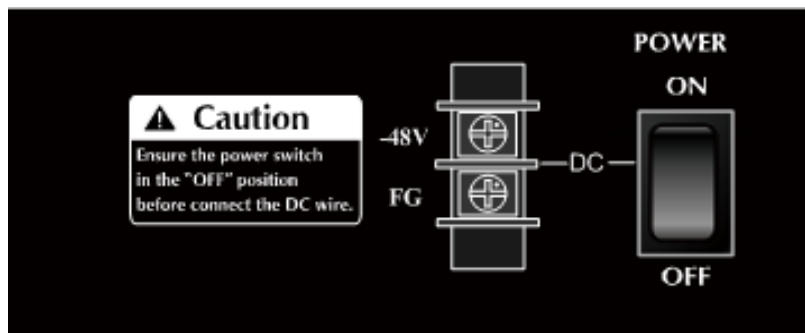
Figure 2-17 Rear Panel of WGSW-24040R / SGSW-24040R

Warning:	Before connect the DC power cable to the input terminal block of WGSW-24040R or SGSW-24040R, ensure that the power switch in the "**OFF"** position and the DC power is **OFF**

2.2 Install 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 follows these steps:

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

Step2: Place the Managed Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-18.
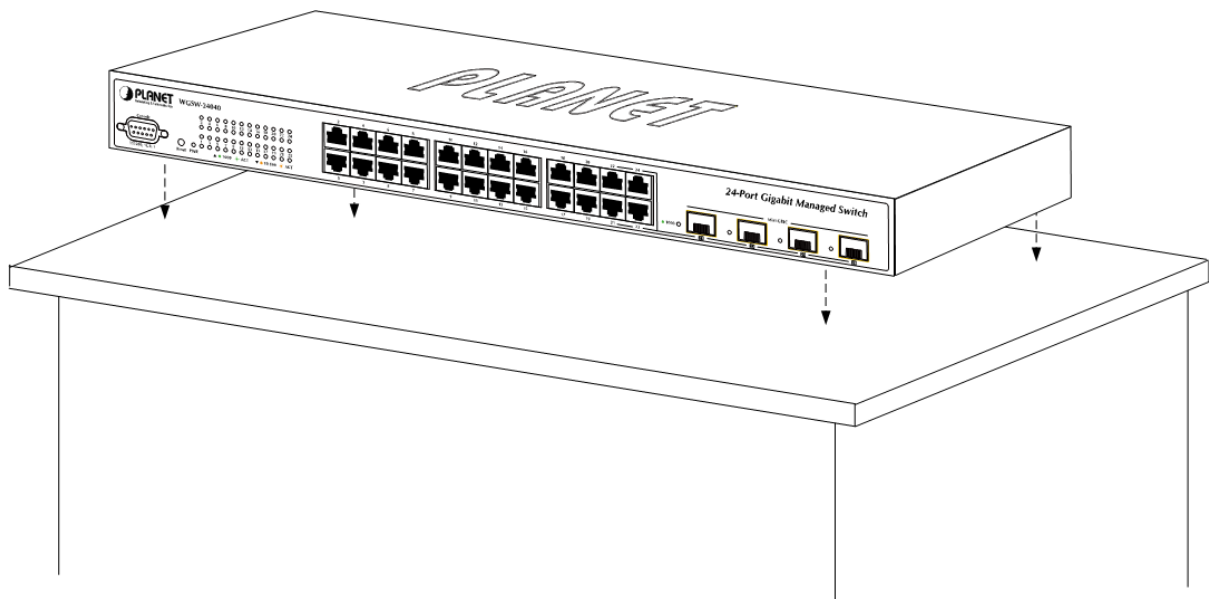
Figure 2-18 Place the Managed Switch on the desktop

Step3: 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 Specification.

Step4: Connect the Managed Switch to network devices.

Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the Managed Switch

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

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

Step5: Supply power to the 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 follows the instructions described below.

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

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

Figure 2-19 shows how to attach brackets to one side of the Managed Switch.
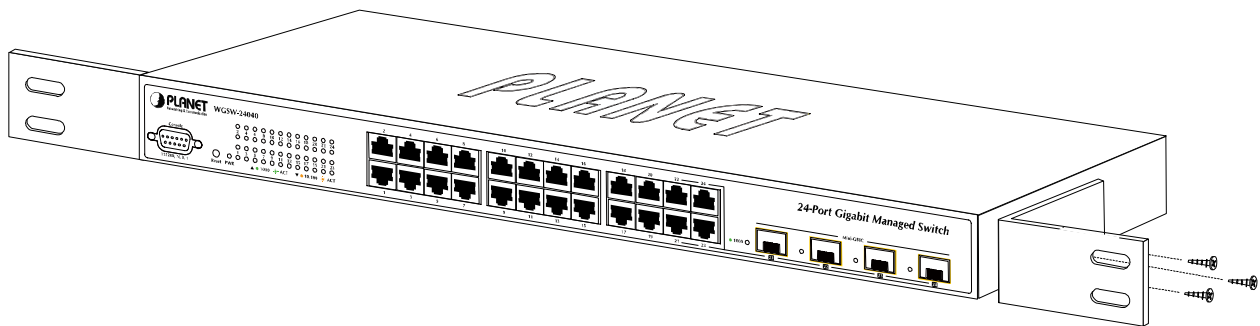
Figure 2-19 Attach brackets to the Managed Switch.

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

Step3: Secure the brackets tightly.

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

Step5: After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-20.
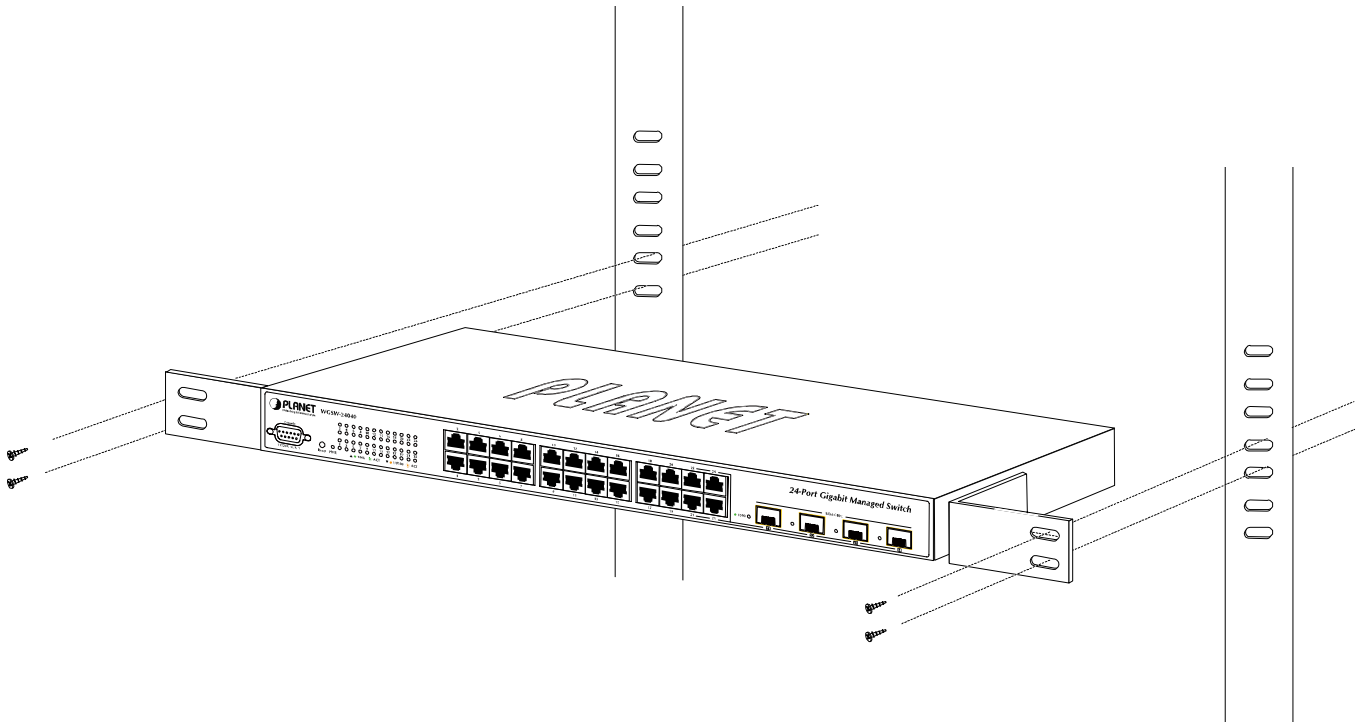
Figure 2-20 Mounting SGSW-24040 in a Rack

Step6: Proceeds with the steps 4 and steps 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 transceiver

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

The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Managed Switch. As the Figure 2-21 appears.

MGB-SX/LX

1000Base-SX/LX
LC Fiber
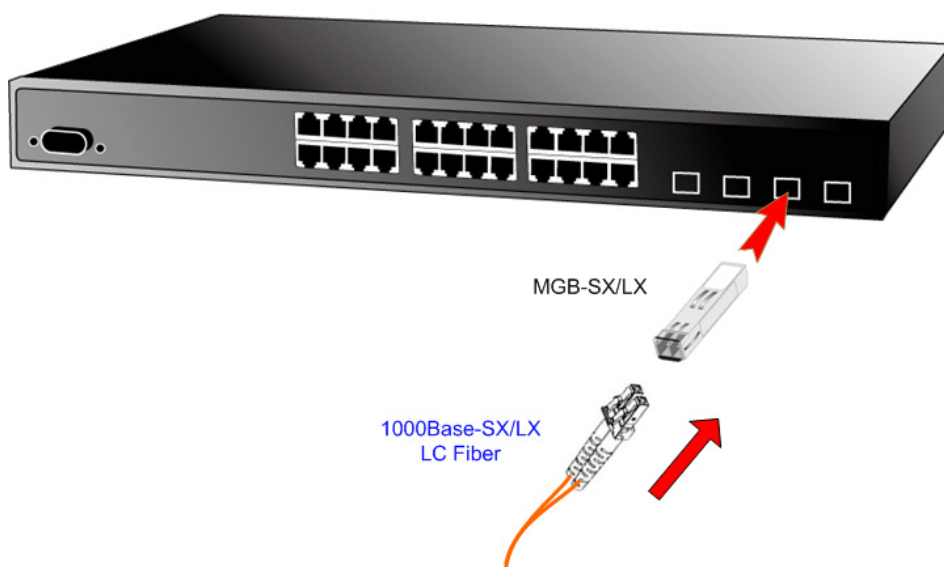
Figure 2-21 Plug-in the SFP transceiver

■ **Approved PLANET SFP Transceivers**

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

- ■ **MGB-SX** SFP (1000BASE-SX SFP transceiver / Multi-mode / 850nm / 220m~550m)
- ■ **MGB-LX** SFP (1000BASE-LX SFP transceiver / Single mode / 1310nm / 10km)
- ■ **MGB-L30** SFP (1000BASE-LX SFP transceiver / Single mode / 1310nm / 30km)
- ■ **MGB-L50** SFP (1000BASE-LX SFP transceiver / Single mode / 1310nm / 50km)
- ■ **MGB-LA10** SFP (1000BASE-LX SFP transceiver / WDM Single mode / TX: 1310nm, RX: 1550nm/ 10km)
- ■ **MGB-LB10** SFP (1000BASE-LX SFP transceiver / WDM Single mode / TX: 1550nm, RX: 1310nm / 10km)

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

Before connect the other Managed Switches, workstation or Media Converter.

1. Make sure both side of the SFP transceiver are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.
2. Check the fiber-optic cable type match the SFP transceiver model.

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

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

■ **Connect the fiber cable**

1. Attach the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a Media Converter..
3. Check the LNK/ACT LED of the SFP slot on the front of the Managed Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link failed. Co works with some fiber-NICs or Media Converters, set the Link mode to "1000 Force" is needed.

■ **Remove the transceiver module**

1. Make sure there is no network activity by consult or check with the network administrator. Or through the management interface of the switch/converter (if available) to disable the port in advance.
2. Remove the Fiber Optic Cable gently.
3. Turn the handle of the MGB module to horizontal.
4. Pull out the module gently through the handle.
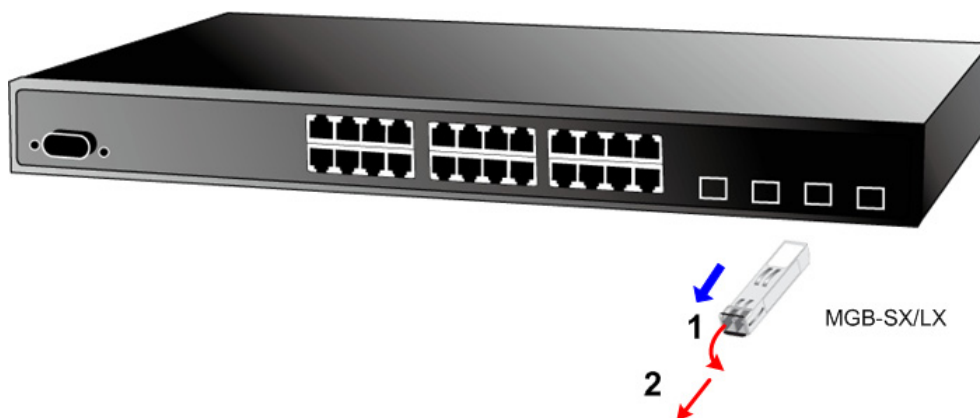
Figure 2-22 Pull out the SFP transceiver

Note	Never pull out the module without pull the handle or the push bolts on the module. Direct pull out the module with violent could damage the module and SFP module slot of the Managed Switch.

2.2.4 Connecting DC Power Supply – WGSW-24040R / SGSW-24040R

The WGSW-24040R and SGSW-24040R support -48VDC power input, connect the power cable to the switch at the input
terminal block.

1. The size of the two screws in the terminal block is M3.5.

2. The terminals are marked "-48V", "FG".

3. Loosen the two screws so you can slide the DC cable beneath it. Insert the DC cable into the connector first, and screw it
   down tight.

4. Connect the power cable to the DC power supply. After power up or reset, the Managed Switch performs a cold start
   procedure.
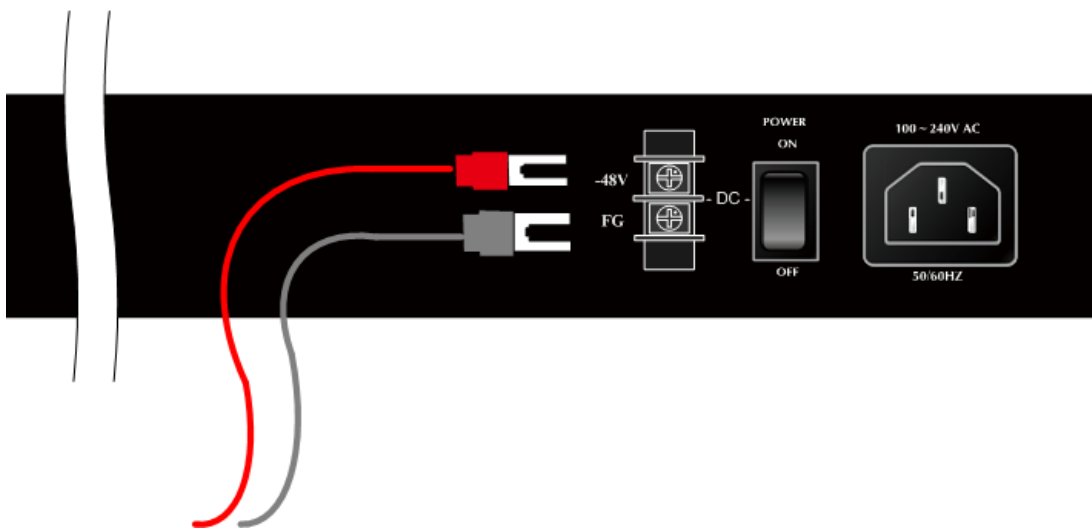
Figure 2-23 -48VDC connector

Warning:	Before connect the DC power cable to the input terminal block of Managed Switch, ensure that the power switch in the "**OFF"** position and the DC power is **OFF**

2.3 Stack Installation

SGSW-24040 / SGSW-24040R

The SGSW-24040 series Managed Switch provides a switch stacking function to manage up to 16 switches using a single IP address. And up to 384 Gigabit Ethernet ports can be managed by a stacking group and you can add ports and functionality as needed. You can add SGSW-24040 series switches as needed to support more network clients, knowing that your switching fabric will scale to meet increasing traffic demands.

Two types of stack topologies are supported by the SGSW-24040 series:

■ **Chain topology (same as a disconnected ring)**

■ **Ring topology**

Please find the following picture for sample connection.

Figure 2-24 Chain Stack topology
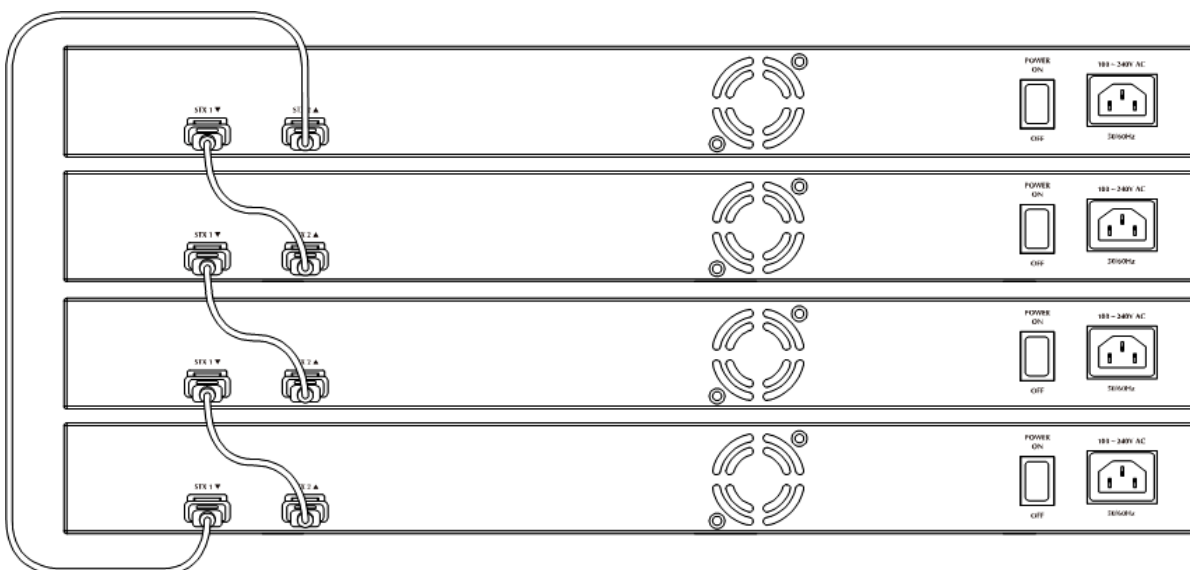
Figure 2-25 Ring Stack topology

40

2.3.1 Connecting Stacking cable

Before attempting to connect stacking ports, verify that you have the required stack cables. The following cables are used to connect stacked switches:

- **CB-STX50**:   50cm, Short stack cable –used to connect adjacent SGSW switches.
- **CB-STX200**: 200cm, Long / Redundant stack cable – used to connect the top and bottom SGSW switches of a stack.

There are two high-performance HDMI-like Stack ports on the rear panel for proprietary management stack. Only attached PLANET CB-STX50 and CB-STX200 cross-overed HDMI cable can be used.

STEP-1: Plug one end of the cable in the "**STX1 / Cascade Down**" port and the other end to the "**STX2 / Cascade UP**" port of next device.

STEP-2: Repeat the step for every device in the stack cluster, then ending at last switch.
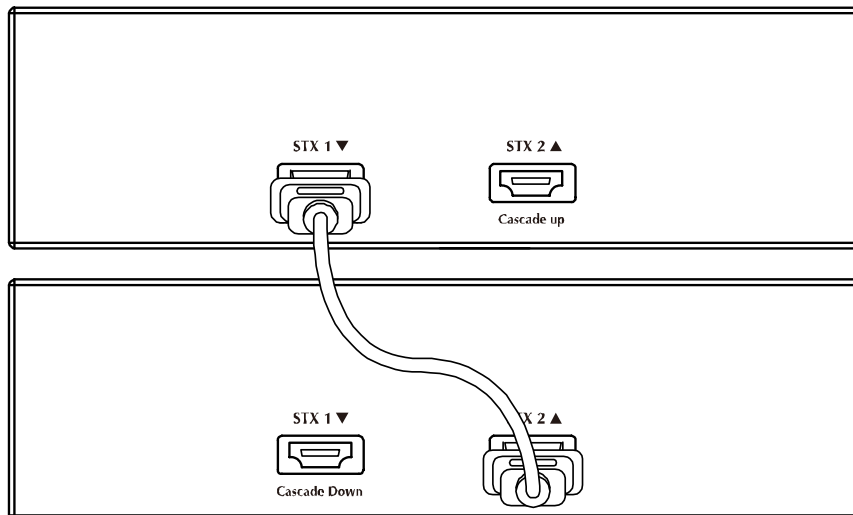
Figure 2-26 Stacking connection

STEP-3: If you wish to implement stack redundancy, use the long stack cable –CB-STX200 to connect the stack port marked "**STX1 / Cascade Down**" on the bottom switch to the port marked "**STX2 / Cascade Up**" on the top switch of the stack.

Note	The stack port is for management and data packets to be transmitted between other SGSW stackable switches, the stack ports can't be configured with Layer 2 features via management interface.

STEP-4: Power up the stack switches.

2.3.2 Management Stacking

The stack operation of the SGSW Managed Switch supports Plug and Play Stacking connection and auto stack configuration.

STEP-5: Once the stack start operation, the Stack master be automatically elected without any configure. The Stack master is indicated by a lit green "**Master**" LED on the front panel. As the Figure 2-19 appears.
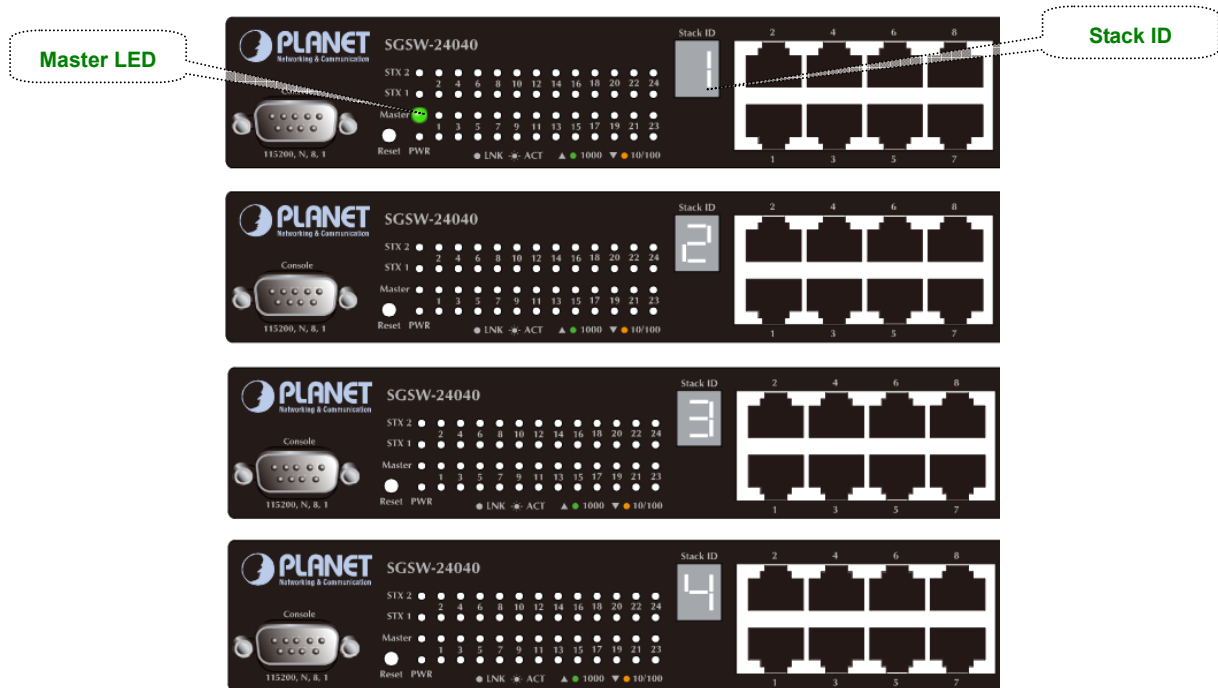
Figure 2-27 Stack Master with "Master" LED lit

STEP-6: When a SGSW Switch is added to the stack, a Switch ID is automatically assigned to the SGSW Switch. The automatic SID assignment can be modified by choosing a different Switch ID on the Stack Configuration page. This method allows Switch IDs to be assigned so that it is easier for the user to remember the ID of each switch.

STEP-7: Connect the **RS-232 serial cable** to the console port on the front of the stack master, then loin the SGSW Switch to start the switch management. Or you can use the **PLANET Smart Discovery Utility** to displayt the IP address of the stack and Web login the stack with this IP address. The default IP address of the SGSW Switch is *192.168.0.100*.
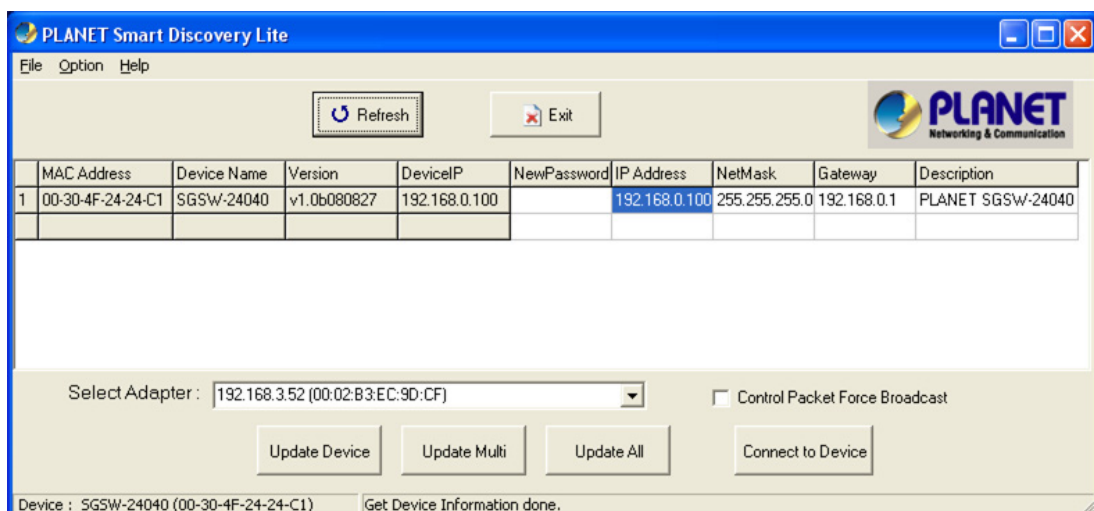
Figure 2-28 Use PLANET Smart Discovery Utility to display the IP address of stack master

Note	1. The stack switch with least priority ID or MAC Address number will become Master. Only Master switch's management interface (console, telnet, web and SNMP) is accessible.
	2.

It's allow to build a stack of up to 16 PLANET SGSW Switches. If there is the space limitation or power issue and you wish to stack all the switches in different racks, use long stack cables "CB-STX200" to connect two stacks.
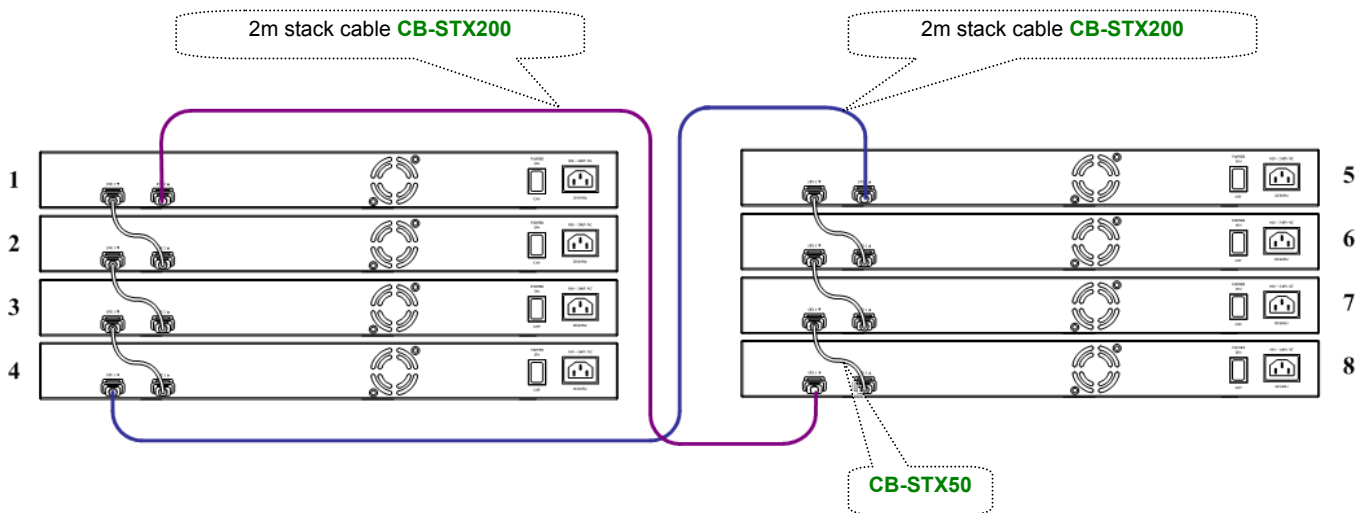
Figure 2-29 Separated Stack connection

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** of subscribers running Windows 98/ME, NT4.0, 2000/XP, MAC OS9 or later, Linux, UNIX or other platform compatible with **TCP/IP** protocols.
- **Workstation** installed with **Ethernet NIC** (Network Interface Card)
- **Serial Port** connect (Terminal)
  - Above PC with COM Port (DB-9 / RS-232) or USB-to-RS-232 converter
- Ethernet Port connect
  - Network cables - Use standard network (UTP) cables with RJ45 connectors.
- Above Workstation installed with **WEB Browser** and J**AVA runtime environment** Plug-in

> It is recommended to use Internet Explore 6.0 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 HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems • Secure	• Must be near switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1 Management Methods Comparison

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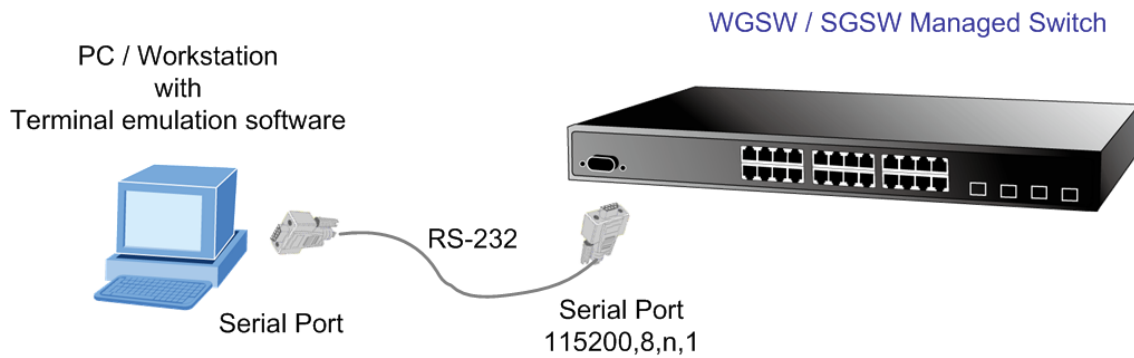
Figure 3-1 Console management

Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as **HyperTerminal**) to the Managed Switch console (serial) port.

When using this management method, a **straight DB9 RS-232 cable** is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:

The default parameters are:

- **115200 bps**
- **8 data bits**
- **No parity**
- **1 stop bit**
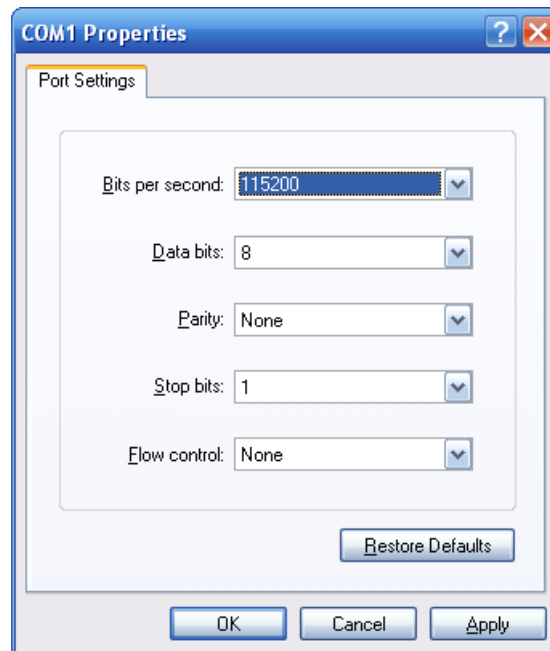
Figure 3-2 Terminal parameter settings

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

3.4 Web Management

The 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.
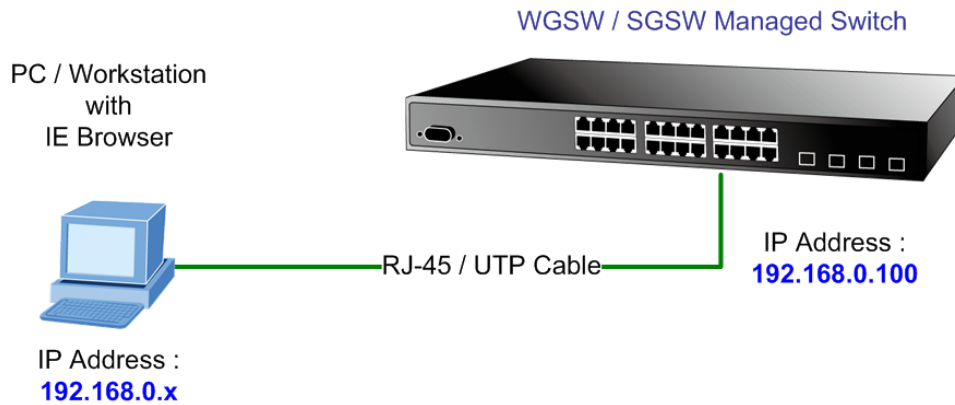
Figure 3-3 Web management

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 6.0** or later, **Safari** or **Mozilla Firefox 1.5** or later.

Figure 3-4 Web main screen of Managed Switch

47

3.5 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the Managed Switch, such as SNMPc Network Manager, HP Openview Network Node Management (NNM) or What's Up Gold. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string. If the SNMP 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 gets and sets community strings for the Managed Switch are public.
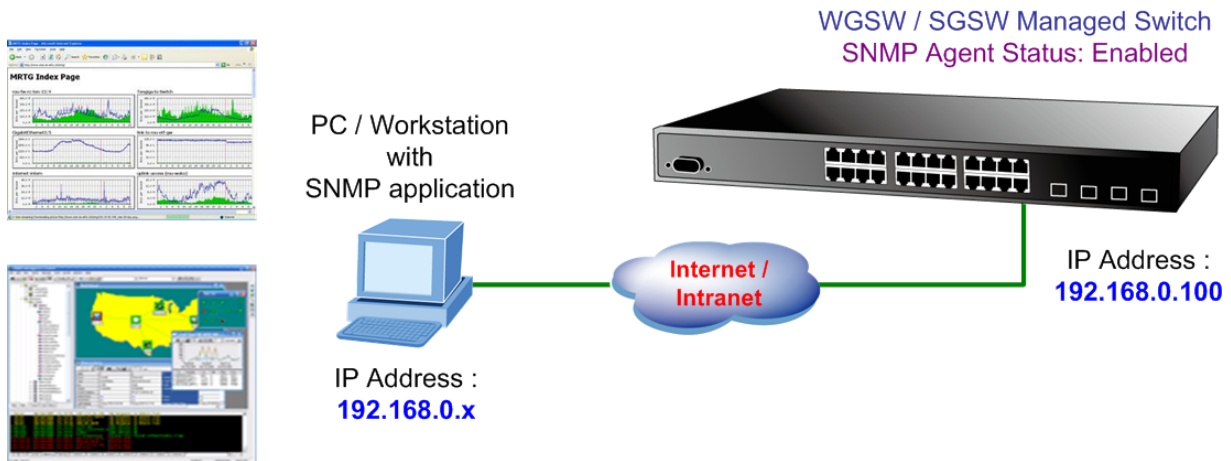
Figure 3-4 SNMP management

3.6 Protocols

The Managed Switch supports the following protocols:

- Virtual terminal protocols, such as Telnet
- Simple Network Management Protocol (SNMP)

3.6.1 Virtual Terminal Protocols

A virtual terminal protocol is a software program, such as **Telnet**, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the Managed Switch before you can establish access to it with a virtual terminal protocol.

	Terminal emulation differs from a virtual terminal protocol in that you must connect a terminal directly to the console (serial) port.
Note	

To access the Managed Switch through a Telnet session:

1. Be Sure of the Managed Switch is configured with an IP address and the Managed Switch is reachable from a PC.

2.   Start the Telnet program on a PC and connect to the Managed Switch.

The management interface is exactly the same with RS-232 console management.

3.6.2 SNMP Protocol

Simple Network Management Protocol (SNMP) is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

3.6.3 Management Architecture

All of the management application modules use the same Messaging Application Programming Interface (MAPI). By unifying management methods with a single MAPI, configuration parameters set using one method (console port, for example) are immediately displayable by the other management methods (for example, SNMP agent of Web browser).
The management architecture of the switch adheres to the IEEE open standard. This compliance assures customers that the Managed Switch is compatible with, and will interoperate with other solutions that adhere to the same open standard.

4. WEB CONFIGURATION

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

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 6.0. 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, IE6.0 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, make sure the manager PC must be set on same the IP subnet address with the Managed Switch.

For example, the default IP address of the WGSW / SGSW 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.
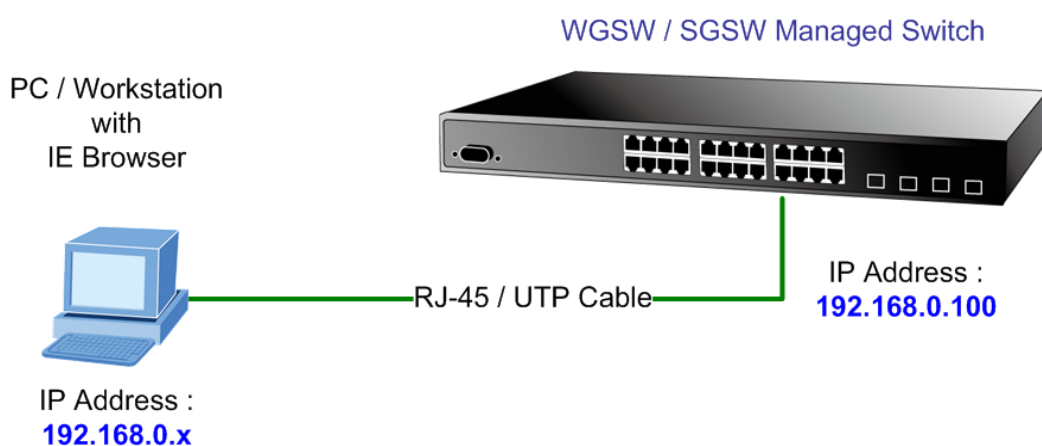
Figure 4-1-1 Web Management

■ **Logging on the switch**

1. Use Internet Explorer 6.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address as following:

http://192.168.0.100

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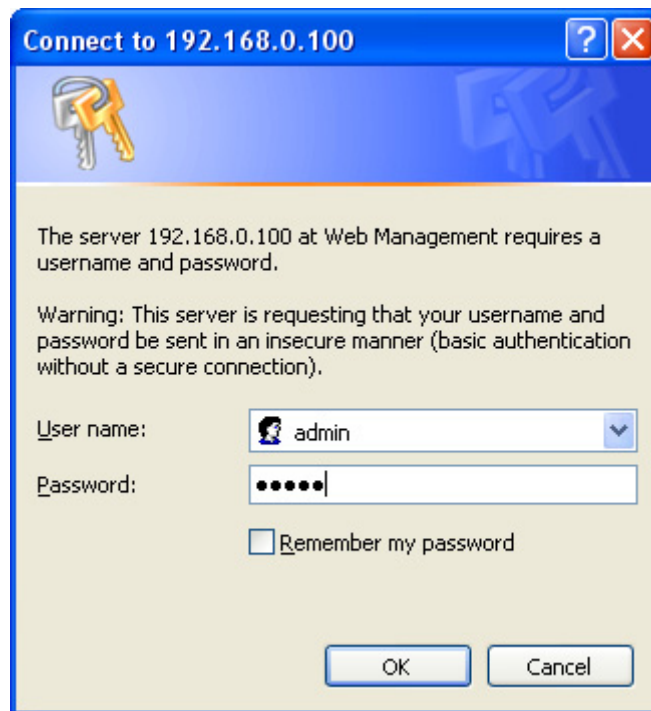
Figure 4-1-2 Login screen

Default User name: **admin**
Default Password: **admin**

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

Figure 4-1-3 Default 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 let you access all the commands and statistics the Managed Switch provides.

1. It is recommended to use Internet Explore 6.0 or above to access Managed Switch.

2. The changed IP address take effect immediately after click on the **Save** button, 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 WGSW / SGSW 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.
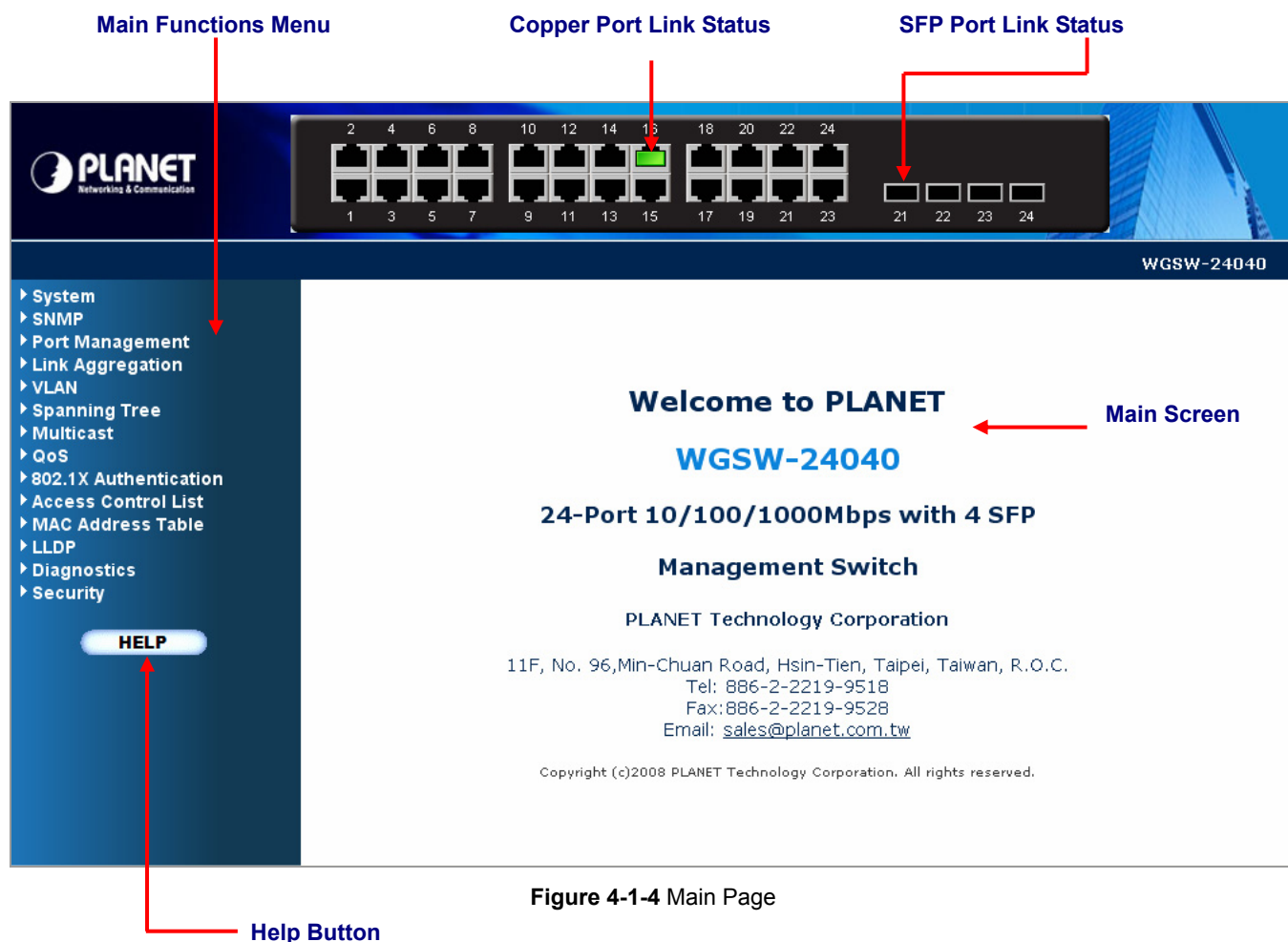
Figure 4-1-4 Main Page

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 states are illustrated as follows:

State	Disabled	Down	Link
RJ-45 Ports			
SFP Ports			
Stack 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 setup the Managed Switch by select the functions those listed in the Main Function. The screen in Figure 4-1-5 appears.
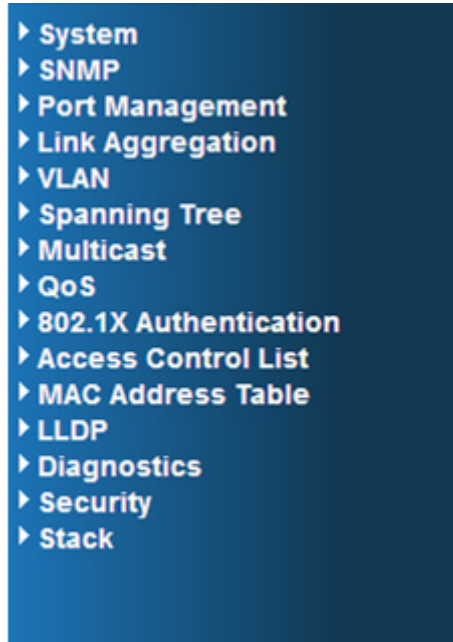
Figure 4-1-5 WGSW/SGSW Managed Switch Main Funcrions Menu

4.2 System

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

- **System Information**   Provides basic system description, including contact information
- **IP Configuration**   Sets the IP address for management access
- **User Authentication**   Allows to configure the system password required to access the web pages or log in from CLI.
- **SNTP Configuration**   Simple Network Time Protocol. Configures SNTP client settings, including broadcast mode or aspecified list of servers
- **Web Firmware Upgrade**   Upgrade the firmware via Web browser
- **TFTP Firmware Upgrade**   Upgrade the firmware via TFTP server
- **Configuration Save**   Save/view the switch configuration to remote host
- **Configuration Upload**   Upload the switch configuration from remote host
- **Factory Default**   Reset the configuration of the Managed Switch
- **System Reboot**   Restarts the switch

4.2.1 System Information

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

Figure 4-2-1 System Information page screenshot

The page includes the following fields:

Object	Description
• **Contact**	The system contact configured in SNMP \ System Information \ System Contact.
• **Name**	The system name configured in SNMP \ System Information \ System Name.
• **Location**	The system location configured in SNMP \ System Information \ System Location
• **MAC Address**	The MAC Address of this switch.
• **System Date**	The current (GMT) system time and date. The system time is obtained through the configured SNTP Server, if any.
• **System Uptime**	The period of time the device has been operational.
• **Switch ID**	The switch ID. (SGSW-Series Only)
• **Software Version**	The software version of the switch.
• **Software Date**	The date when the switch software was produced.

Buttons

Auto-refresh   : Check this box to enable an automatic refresh of the page at regular intervals.

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

For the SGSW series stackable switch, the System Information page add additional column to identify the current switch ID of stack member switches in a stack group. The screen as below appears:

System Information

System	
Contact Name Location	SGSW-24040
Hardware	
MAC Address	00-30-4f-24-24-c1
Time	
System Date	2008-09-04 14:25:17 +0800
System Uptime	0d 02:22:25

Switch ID	Software Version
1	v1.0b080827
2	v1.0b080827
3	v1.0b080827

Auto-refresh ☐ **Refresh**

4.2.2 IP Configuration

The IP Configuration includes the IP Address, Subnet Mask and Gateway. The Configured column is used to view or change the IP configuration.Fill up the IP Address, Subnet Mask and Gateway for the device. The screen in Figure 4-2-2 appears.
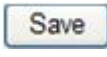
Figure 4-2-2 IP Configuration page screenshot

The Current column is used to show the active IP configuration.

Object	Description
• **DHCP Client**	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
• **IP Address**	Provide the IP address of this switch in dotted decimal notation.
• **IP Mask**	Provide the IP mask of this switch dotted decimal notation.
• **IP Router**	Provide the IP address of the router in dotted decimal notation.
• **SNTP Server**	Provide the IP address of the SNTP Server in dotted decimal notation.
• **VLAN ID**	Provide the managed VLAN ID. The allowed range is `1` through `4095`.
• **Timezone Offset**	Provide the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from `-720` to `720` minutes.

Buttons

Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

4.2.3 User Authentication

This page allows you to configure the system password required to access the web pages or log in from CLI. After setup completed, please press **"Save"** button to take effect. Please login web interface with new password, the screen in Figure 4-2-3 appears.
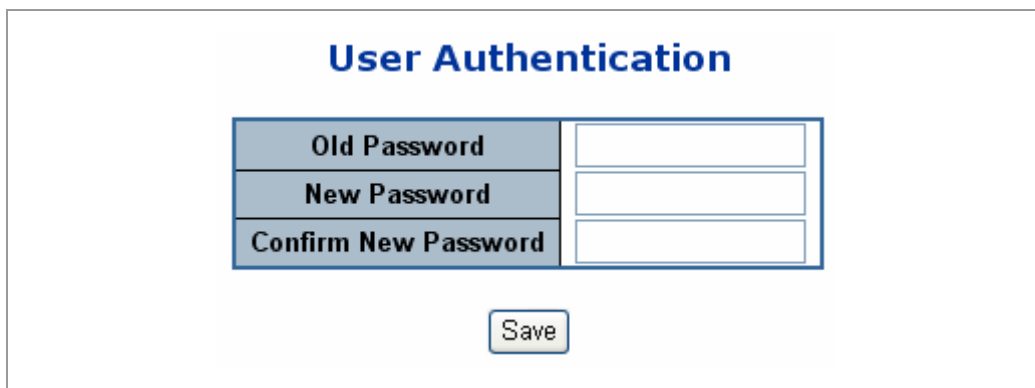
Figure 4-2-3 User Authentication page screenshot

The page includes the following fields:

Object	Description
• **Old Password**	Enter the current system password. If this is incorrect, the new password will not be set.
• **New Password**	The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126. It will not display as it is typed, only asterisks (*) will show. Passwords are alpha numeric characters in length, and are case sensitive.
• **Confirm New Password**	The new password must be entered twice to catch typing errors. To confirm that you entered it correctly, this field will not display, but will show asterisks (*)

> **Note**
> After change the default password, if you forget the password. Please press the **"Reset"** button in the front panel of the Managed Switch over 10 seconds and then release, the current setting includes VLAN, will be lost and the Managed Switch will restore to the default mode.

4.2.4 SNTP Configuration

In the System sub-function menu, you can see the SNTP Configuration (see Figure 4-4), by which you can configure the time settings for the Managed Switch. You can specify SNTP Servers and set GMT Timezone. The SNTP Configuration screen in Figure 4-2-4 appears.

SNTP Configuration

SNTP Server	0.0.0.0
Timezone Offset (minutes)	0
System Date	1970-01-01 00:12:25 +0000
System Uptime	0d 00:12:25

Save   Reset

Figure 4-2-4 SNTP Configuration page screenshot

The Time page includes the following fields:

Object	Description
• **SNTP Server**	Provide the IP address of the SNTP Server in dotted decimal notation. Enter a user-defined SNTP server IP addresses or hostname. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a SNTP server. Unicast SNTP requests will be sent to this address. If this address is a DNS hostname, then that hostname should be resolved into an IP address each time a SNTP request is sent to it.
• **Timezone Offset**	Provide the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from `-720` to `720` minutes.
• **System Date**	Display the current local date and time (UTC) of the last SNTP request or receipt of an unsolicited message. The field format is Year-Month-Day HH : MM : SS. For example, 2008-08-20 21:15:03
• **System Uptime**	Display the time passed since the device boot up.

Note	The device supports the **Simple Network Time Protocol (SNTP)**. SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. SNTP operates only as a client, and cannot provide time services to other systems.

It is recommended that you research any time server selection to ensure that it can meet your specific time server requirements. Any NTP time server selection should be evaluated to determine if the server in question meets your specific time server requirements.

For more detail about the Time Server and Time Server List, please refer to the following URL:

http://ntp.isc.org/bin/view/Servers/WebHome

http://ntp.isc.org/bin/view/Servers/NTPPoolServers

http://support.microsoft.com/kb/262680/en-us

4.2.5 WEB Firmware Upgrade

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

The Web Firmware Upgrade screen in Figure 4-2-5 appears.
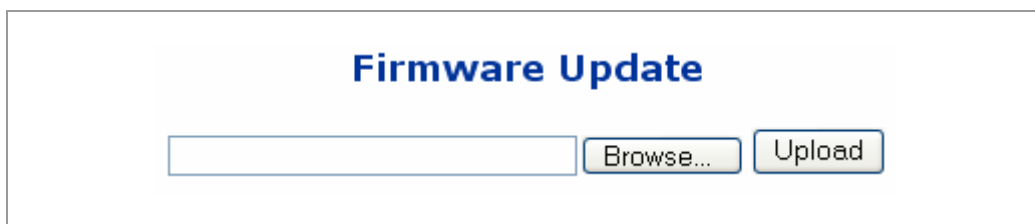
Figure 4-2-5 Web Firmware Upgrade page screenshot

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

1. Click **System** -> Web **Firmware Upgrade**.

2. The Firmware Upgrade screen is displayed as in Figure 4-2-5.

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

4. Select on the firmware then click "**Upload**", the **Software Upload Progress** would show the file upload status.

5. Once the software be loaded to the system successfully. The following screen appears. Click the "**Yes**" button to activate the new software immediately. The system will load the new software after reboot.

Figure 4-2-6 Software successfully loaded notice screen

4.2.6 TFTP Firmware Upgrade

The **Firmware Upgrade** page provides the functions to allow a user to update the Managed Switch firmware from the TFTP server in the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. The screen in Figure 4-2-7 appears.
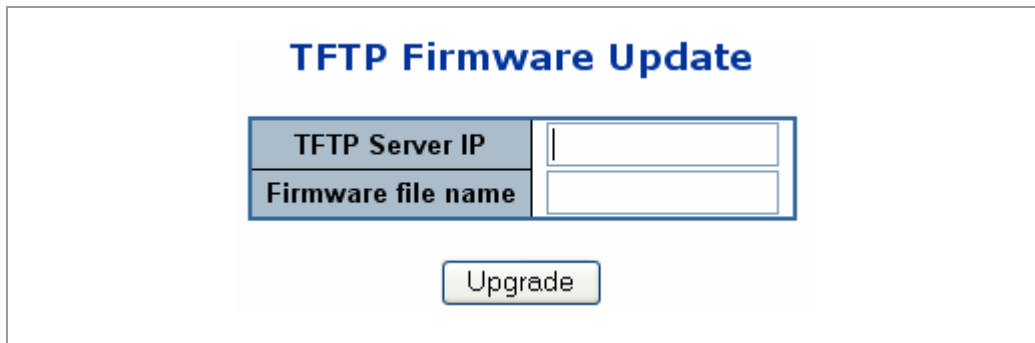
Figure 4-2-7 TFTP Firmware Update page screenshot

The page includes the following fields:

Object	Description
• **TFTP Server IP**	Fill in your TFTP server IP address.
• **Filename**	The name of firmware image. (Maximum length : 24 characters)
• **Upgrade button**	Press the button for upgrade the switch firmware.

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

1. Click **System** -> **TFTP Firmware Upgrade**.

2. The Firmware Upgrade screen is displayed as in Figure 4-2-7.

3. Fill in the **TFTP server IP Address** and the **firmware file name**, click the "**Upgrade**" button of the main page, the system would pop up the confirm message

.
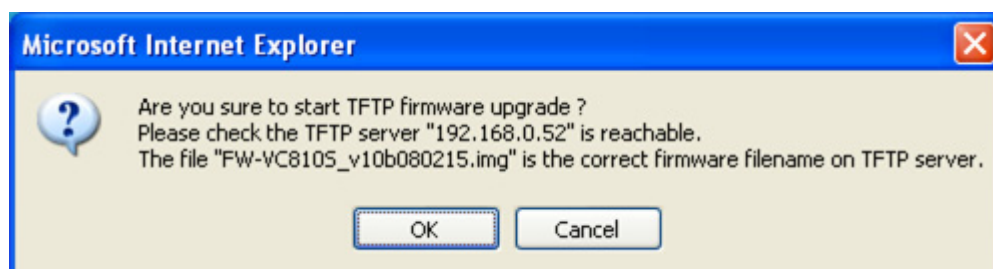
Figure 4-2-8 TFTP Firmware upgrade pop-up message
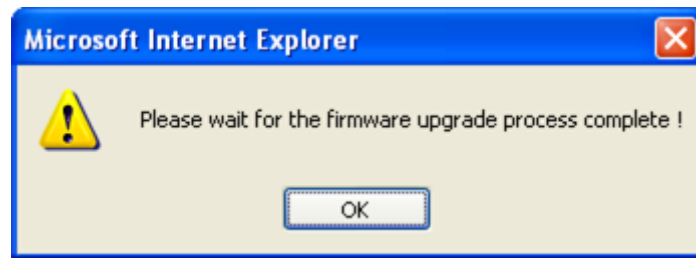
Figure 4-2-9 Firmware Upgrade pop-up message

4. Click "**OK**", the Switch will start the TFTP upgrade procedure.

5. Please check your TFTP server application to confirm the TFTP file is well transmit to the Switch.

6. The Switch will reboot then, and It will cost 2 to 3 minutes for the TFTP firmware upgrade and reboot procedure. Please wait for the process complete.

7. Once the new software is loaded to the system successfully, the Login screen appears. Enter the user name and password to login the Switch.

Note	**DO NOT Power OFF** the switch until the update progress is complete.

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

4.2.7 Configuration Save

This function allows backup and reload the current configuration of the Managed Switch to the local management station. The screen in Figure 4-2-10 appears.
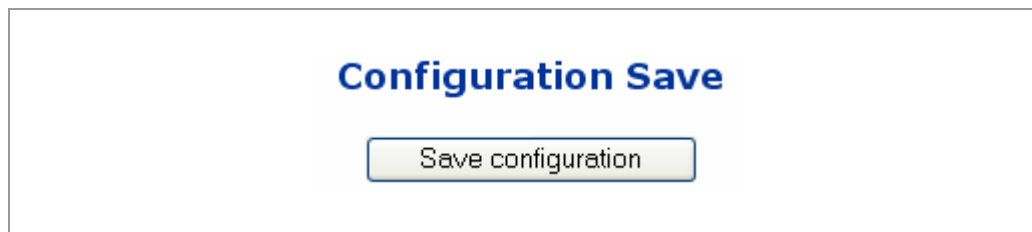
Figure 4-2-10 Configuration Save page screenshot

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:

Header tags: <?xml version="1.0"?> and <configuration>. These tags are mandatory and must be present at the beginning of the file.

Section tags: <platform>, <global> and <switch>. The platform section must be the first section tag and this section must include the correct platform ID and version. The global section is optional and includes configuration which is not related to specific switch ports. The switch section is optional and includes configuration which is related to specific switch ports.

Module tags: <ip>, <mac>, <port> etc. These tags identify a module controlling specific parts of the configuration.

Group tags: <port_table>, <vlan_table> etc. These tags identify a group of parameters, typically a table.

Parameter tags: <mode>, <entry> etc. These tags identify parameters for the specific section, module and group. The <entry> tag is used for table entries.

Configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire configuration including syntax descriptions is included in the file. The file may then be modified using an editor and loaded to a switch.

The example below shows a small configuration file only including configuration of the MAC address age time and the learning mode per port. When loading this file, only the included parameters will be changed. This means that the age time will be set to 200 and the learn mode will be set to automatic.

■ **Save Configuration**

1. Press the *"Save Configuration"* button to save the current configuration in manager workstation. The following screens in Figure 4-2-11 and 4-2-12 appear
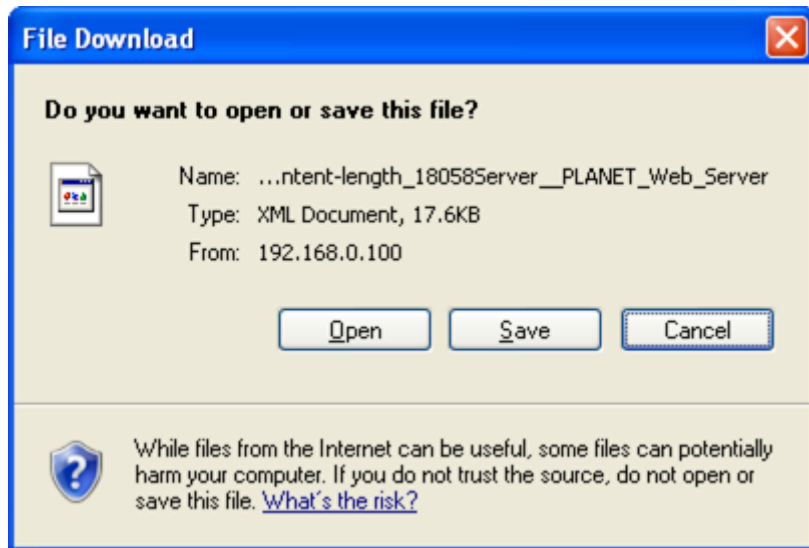
Figure 4-2-11 File Download screen

2. Chose the file save path in management workstation.
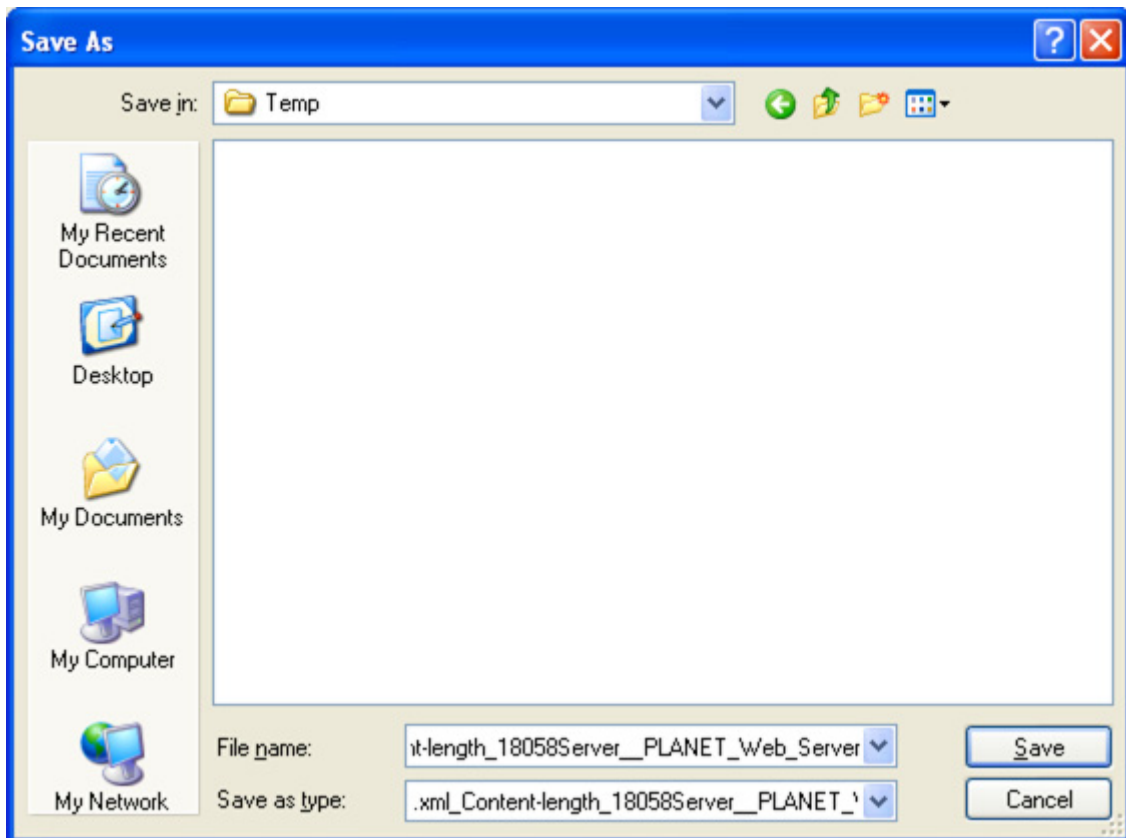
Figure 4-2-12 File save screen

4.2.8 Configuration Upload

This function allows backup and reload the current configuration of the Managed Switch to the local management station. The screen in Figure 4-2-13 appears.
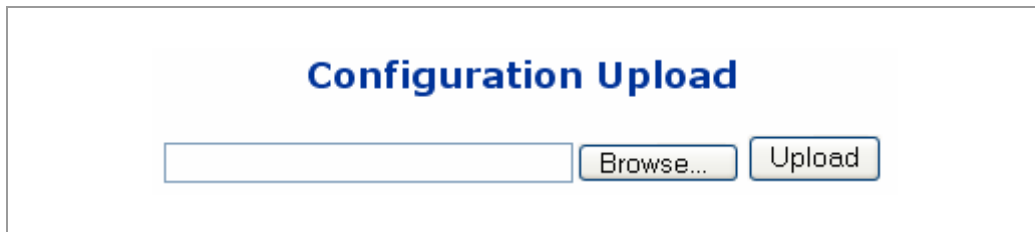
Figure 4-2-13 Configuration Upload page screenshot

■ **Configuration Upload**

1. Click the "**Browse**" button of the main page, the system would pop up the file selection menu to choose saved configuration.
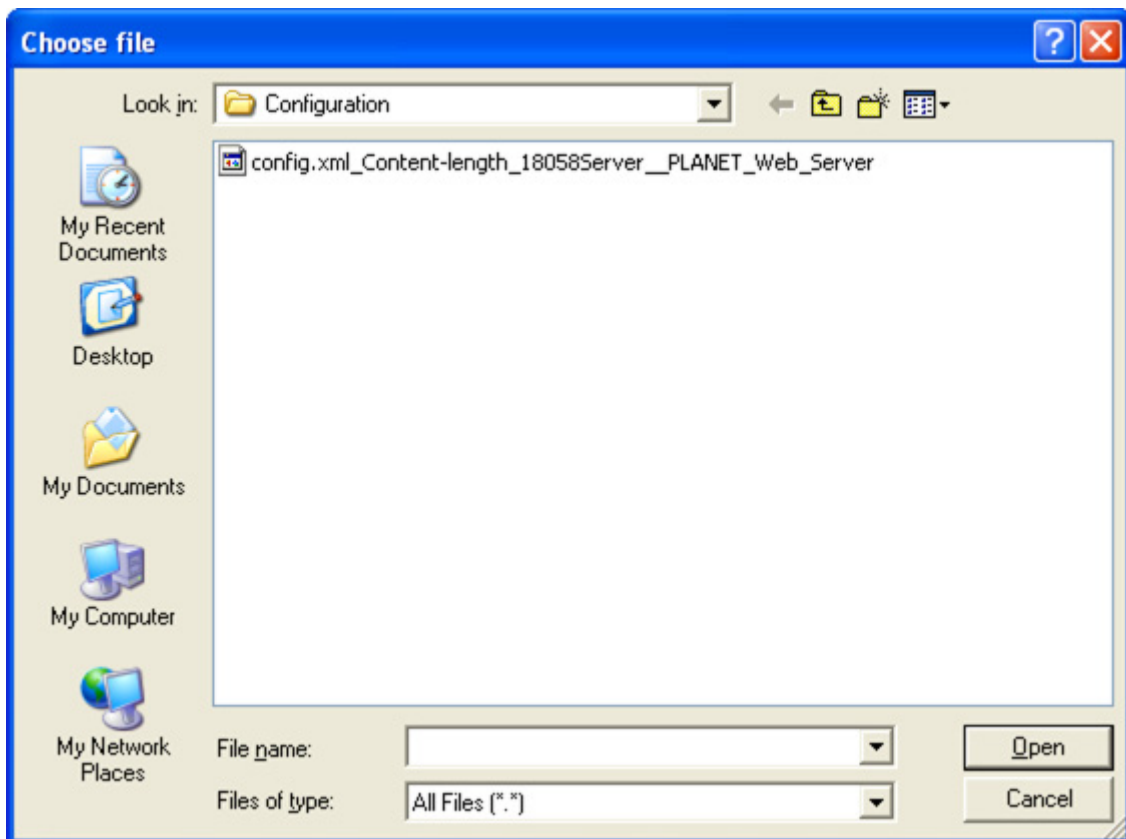
Figure 4-2-14 Windows file selection menu popup

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

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

4.2.9 Factory Default

The Factory Reset button can reset the Managed Switch back to the factory default mode. Be aware that the entire configuration will be reset; include the IP address of the Managed Switch. Once the Factory Reset item is pressed, the screen in Figure 4-2-15 appears.

Figure 4-2-15 Factory Default Reset screen

After the "**Factory**" button be pressed and rebooted, the system will load the default IP settings as following:

◦　Default IP address: **192.168.0.100**

◦　Subnet mask: **255.255.255.0**

◦　Default Gateway: **192.168.0.254**

◦　The other setting value is back to disable or none.

> To reset the Managed Switch to the Factory default setting, you can also press the hardware reset button at the front panel about 10 seconds. After the device be rebooted. You can login the management WEB interface within the same subnet of 192.168.0.xx.
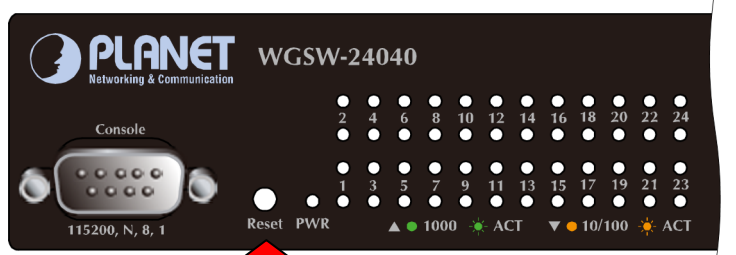
Hardware Reset button

4.2.10 System Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user have to re-login the WEB interface about 60 seconds later, the screen in Figure 4-2-16 appears.
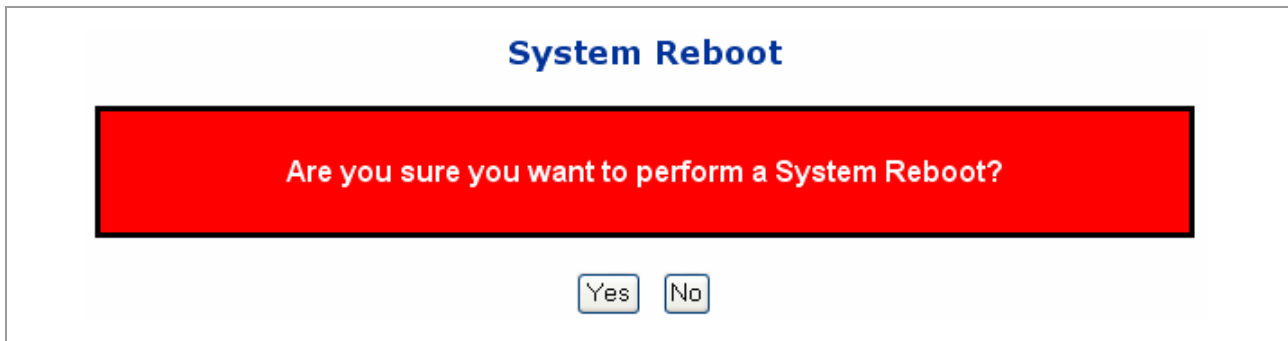
Figure 4-2-16 System Reboot page screenshot

You can also check the **SYS LED** at the front panel to identify the System is load completely or not. If the SYS LED is blinking, then it is in the firmware load stage; if the SYS LED light on, you can use the WEB browser to login the Switch.

4.3 Simple Network Management Protocol

4.3.1 SNMP Overview

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

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

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

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

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

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

SNMP Operations

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

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

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

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

SNMP community

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

- **Write** = private

- **Read** = public

4.3.2 SNMP System Configuration

Configure SNMP on this page.

The SNMP System Configuration screen in Figure 4-3-1 appears.

Figure 4-3-1 SNMP System Configuration page screenshot

Object	Description
• **Mode**	Indicates the SNMP mode operation. Possible modes are: • **Enabled**: Enable SNMP mode operation. • **Disabled**: Disable SNMP mode operation.
• **Version**	Indicates the SNMP supported version. Possible versions are: • **SNMP v1**: Set SNMP supported version 1. • **SNMP v2c**: Set SNMP supported version 2c. • **SNMP v3**: Set SNMP supported version 3.
• **Read Community**	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table.
• **Write Community**	Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table.
• **Engine ID**	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

4.3.3 SNMP System Information Configuration

The switch system information is provided here.

The System Information Configuration screen in Figure 4-3-2 appears.

Figure 4-3-2 System Information Configuration page screenshot

The page includes the following fields:

Object	Description
• **System Contact**	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
• **System Name**	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
• **System Location**	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

4.3.4 SNMP Trap Configuration

Configure SNMP trap on this page.

The SNMP Trap Configuration screen in Figure 4-3-3 appears.

Figure 4-3-3 SNMP Trap Configuration page screenshot

The page includes the following fields:

Object	Description
• **Trap Mode**	Indicates the SNMP trap mode operation. Possible modes are: • **Enabled**: Enable SNMP trap mode operation. • **Disabled**: Disable SNMP trap mode operation.
• **Trap Version**	Indicates the SNMP trap supported version. Possible versions are: • **SNMP v1**: Set SNMP trap supported version 1. • **SNMP v2c**: Set SNMP trap supported version 2c. • **SNMP v3**: Set SNMP trap supported version 3.
• **Trap Community**	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
• **Trap Destination Address**	Indicates the SNMP trap destination address.
• **Trap Authentication Failure**	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are: • **Enabled**: Enable SNMP trap authentication failure. • **Disabled**: Disable SNMP trap authentication failure.
• **Trap Inform Mode**	Indicates the SNMP trap inform mode operation. Possible modes are: • **Enabled**: Enable SNMP trap inform mode operation. • **Disabled**: Disable SNMP trap inform mode operation.
• **Trap Inform Timeout (seconds)**	Indicates the SNMP trap inform timeout. The allowed range is **0** to **2147**.
• **Trap Inform Retry Times**	Indicates the SNMP trap inform retry times. The allowed range is **0** to **255**.

• **Trap Probe Security Engine ID**	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:
	• **Enabled**: Enable SNMP trap probe security engine ID mode of operation.
	• **Disabled**: Disable SNMP trap probe security engine ID mode of operation.
• **Trap Security Engine ID**	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
• **Trap Security Name**	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

4.3.5 SNMPv3 Configuration

4.3.5.1   SNMPv3 Accesses Configuration

Configure SNMPv3 accesses table on this page. The entry index key are Group Name, Security Model and Security Level. The SNMPv3 Accesses Configuration screen in appears.

Figure 4-3-4 SNMPv3 Accesses Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

• **Security Model**	Indicates the security model that this entry should belong to. Possible security models are:
	• **any**: Accepted any security model (v1|v2c|usm).
	• **v1**: Reserved for SNMPv1.
	• **v2c**: Reserved for SNMPv2c.
	• **usm**: User-based Security Model (USM)
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are:
	• **NoAuth, NoPriv**: None authentication and none privacy.
	• **Auth, NoPriv**: Authentication and none privacy.
	• **Auth, Priv**: Authentication and privacy.
• **Read View Name**	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Write View Name**	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

4.3.5.2 SNMPv3 Communities Configuration

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

The SNMPv3 Communities Configuration screen in Figure 4-3-5 appears.

Figure 4-3-5 SNMPv3 Communities Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Community**	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters

	from 33 to 126.
• **Source IP**	Indicates the SNMP access source address.
• **Source Mask**	Indicates the SNMP access source address mask.

4.3.5.3 SNMPv3 Groups Configuration

Configure SNMPv3 groups table on this page. The entry index key are Security Model and Security Name.

The SNMPv3 Groups Configuration screen in Figure 4-3-6 appears.

Figure 4-3-6 SNMPv3 Groups Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Security Model**	Indicates the security model that this entry should belong to. Possible security models are: • **v1**: Reserved for SNMPv1. • **v2c**: Reserved for SNMPv2c. • **usm**: User-based Security Model (USM).
• **Security Name**	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

4.3.5.4 SNMPv3 Users Configuration

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

The SNMPv3 Users Configuration screen in Figure 4-3-7 appears.

Figure 4-3-7 SNMPv3 Users Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Engine ID**	A octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
• **User Name**	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are: • **NoAuth, NoPriv**: None authentication and none privacy. • **Auth, NoPriv**: Authentication and none privacy. • **Auth, Priv**: Authentication and privacy. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.
• **Authentication Protocol**	Indicates the authentication protocol that this entry should belong to. Possible authentication protocol are: • **None**: None authentication protocol. • **MD5**: An optional flag to indicate that this user using MD5 authentication protocol. • **SHA**: An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.

• **Authentication Password**	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.	
• **Privacy Protocol**	Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are: • **None**: None privacy protocol. • **DES**: An optional flag to indicate that this user using DES authentication protocol.	
• **Privacy Password**	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.	

4.3.5.5 SNMPv3 Views Configuration

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

The SNMPv3 Views Configuration screen in Figure 4-3-8 appears.
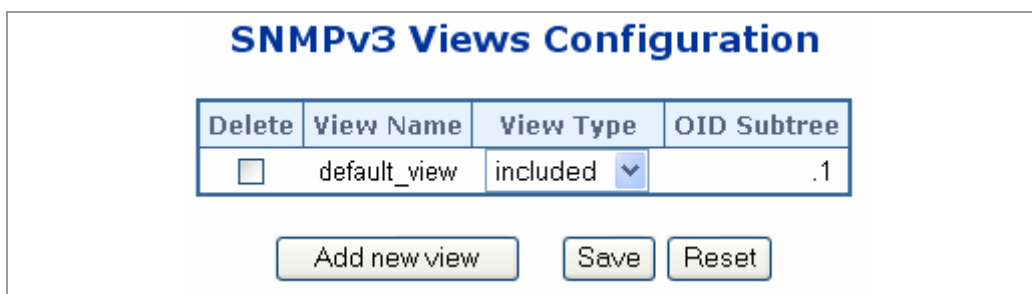
Figure 4-3-8 SNMPv3 Views Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	• **Check to delete the entry. It will be deleted during the next save.**
• **View Name**	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **View Type**	Indicates the view type that this entry should belong to. Possible view type are: • **included**: An optional flag to indicate that this view subtree should be included. • **excluded**: An optional flag to indicate that this view subtree should be excluded.

General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.

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

4.4 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 connection settings
- ■ **Port Statistics**   Lists Ethernet and RMON port statistics
- ■ **Mirror Port Configuration**   Sets the source and target ports for mirroring

4.4.1 Port Configuration

This page displays current port configurations. Ports can also be configured here.

The port settings relate to the currently selected stack unit, as reflected by the page header.

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

The Port Configuration screen in Figure 4-4-1 appears.

Figure 4-4-1 Port Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	This is the logical port number for this row.
• **Link**	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
• **Current Link Speed**	Provides the current link speed of the port.
• **Configured Link Speed**	Select any available link speed for the given switch port. Draw the menu bar to select the mode. • **Auto Speed** - Setup Auto negotiation. • **10 half** - Force sets 10Mbps/Half-Duplex mode. • **10 Full** - Force sets 10Mbps/Full-Duplex mode. • **100 half** - Force sets 100Mbps/Half-Duplex mode. • **100 full** - Force sets 100Mbps/Full-Duplex mode. • **1000 full** - Force sets 10000Mbps/Full-Duplex mode. • **Disable** - Shutdown the port manually.
• **Flow Control**	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.
• **Maximum Frame**	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is **1518** bytes to **9600** bytes.
• **Excessive Collision Mode**	Configure port transmit collision behavior. • **Discard**: Discard frame after 16 collisions (default). • **estart**: Restart backoff algorithm after 16 collisions.
• **Power Control**	The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port. • **Disabled**: All power savings mechanisms disabled. • **ActiPHY**: Link down power savings enabled. • **Dynamic**: Link up power savings enabled.

- **Enabled**: Link up and link down power savings enabled.

- **Total Power Usage**   Total power usage in board, measured in percent.

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

4.4.2 Port Statistics Overview

This page provides an overview of general traffic statistics for all switch ports. The ports belong to the currently selected stack unit, as reflected by the page header.

The Port Statistics Overview screen in Figure 4-4-2 appears.

Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	1371	1076	228393	558988	0	0	0	0	9
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0

Auto-refresh ☐ [Refresh] [Clear]

Figure 4-4-2 Port Statistics Overview page screenshot

The displayed counters are:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Packets**	The number of received and transmitted packets per port.
• **Bytes**	The number of received and transmitted bytes per port.
• **Errors**	The number of frames received in error and the number of incomplete transmissions per port.
• **Drops**	The number of frames discarded due to ingress or egress congestion.
• **Filtered**	The number of received frames filtered by the forwarding process.

4.4.3 Detailed Port Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The selected port belong to the currently selected stack unit, as reflected by the page header.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. The Detailed Port Statistics screen in Figure 4-4-3 appears.

Figure 4-4-3 Detailed Port Statistics Port 1 page screenshot

The page includes the following fields:

Receive Total and Transmit Total

Object	Description
• **Rx and Tx Packets**	The number of received and transmitted (good and bad) packets
• **Rx and Tx Octets**	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
• **Rx and Tx Unicast**	The number of received and transmitted (good and bad) unicast packets.
• **Rx and Tx Multicast**	The number of received and transmitted (good and bad) multicast packets.
• **Rx and Tx Broadcast**	The number of received and transmitted (good and bad) broadcast packets.
• **Rx and Tx Pause**	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Object	Description
• **Rx Drops**	The number of frames dropped due to lack of receive buffers or egress congestion.
• **Rx CRC/Alignment**	The number of frames received with CRC or alignment errors.
• **Rx Undersize**	The number of short [1] frames received with valid CRC.
• **Rx Oversize**	The number of long [2] frames received with valid CRC.
• **Rx Fragments**	The number of short [1] frames received with invalid CRC.
• **Rx Jabber**	The number of long [2] frames received with invalid CRC.
• **Rx Filtered**	The number of received frames filtered by the forwarding process. Short frames are frames that are smaller than 64 bytes. Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Object	Description
• **Tx Drops**	The number of frames dropped due to output buffer congestion.
• **Tx Late/Exc. Coll.**	The number of frames dropped due to excessive or late collisions.

4.4.4 Port Mirroring Configuration

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

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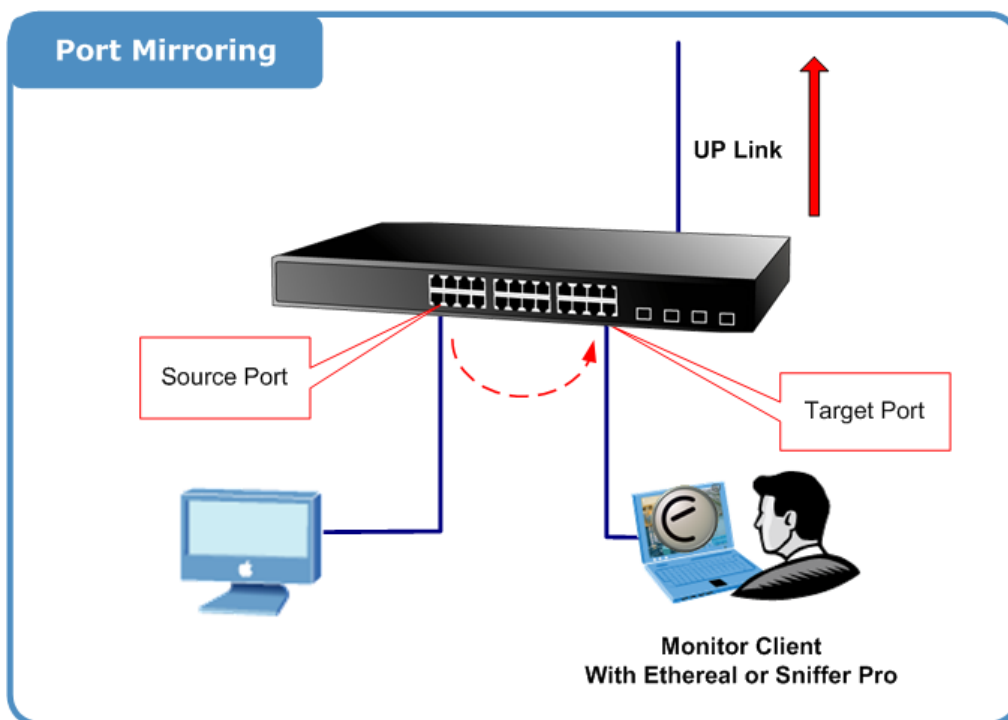
Figure 4-4-4 Port Mirror application

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

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

Mirror Port Configuration

The Port Mirror Configuration screen in Figure 4-4-5 and Figure 4-4-6 appears.

■ **WGSW Standalone Switch**
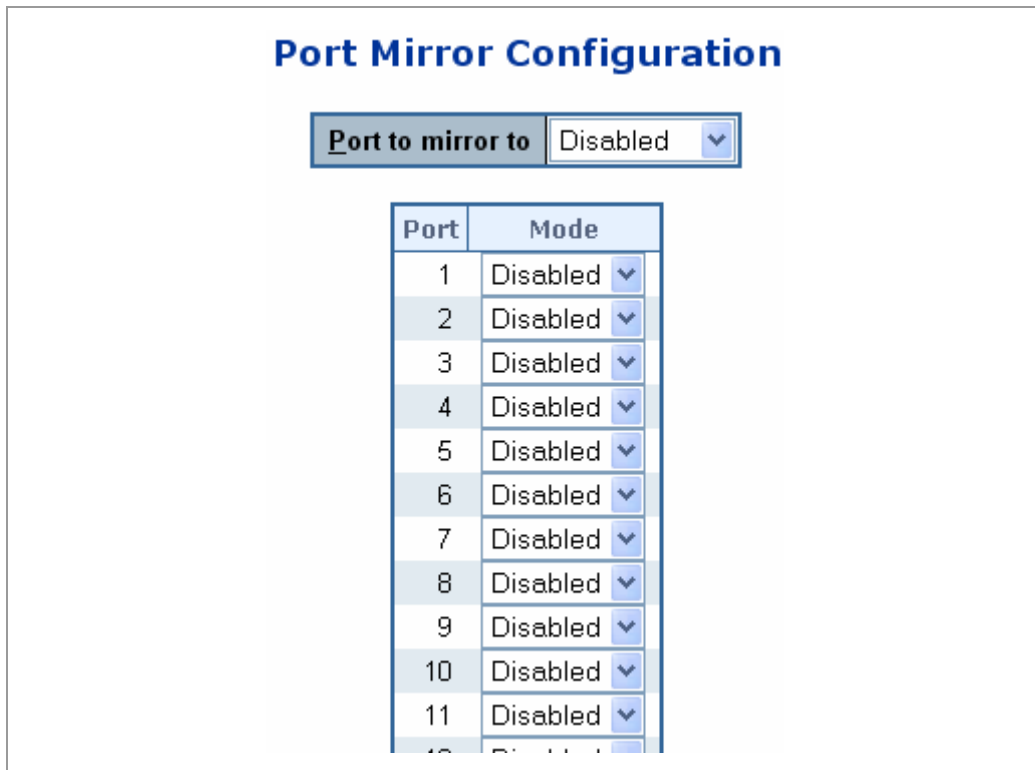
Figure 4-4-5 Port Mirror Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port to mirror to**	Frames from ports that have either source or destination mirroring enabled are mirrored to this port. Disabled disables mirroring.
• **Port**	The logical port for the settings contained in the same row.
• **Mode**	Select mirror mode.
	• **Rx only** Frames received at this port are mirrored to the mirroring port. Frames transmitted are not mirrored.
	• **Tx only** Frames transmitted from this port are mirrored to the mirroring port. Frames received are not mirrored.
	• **Disabled** Neither frames transmitted or frames received are mirrored.
	• **Enabled** Frames received and frames transmitted are mirrored to the mirror port.

■   **SGSW Stackable Switch**

The SGSW Stackable switch supports port mirror function over stack switch.
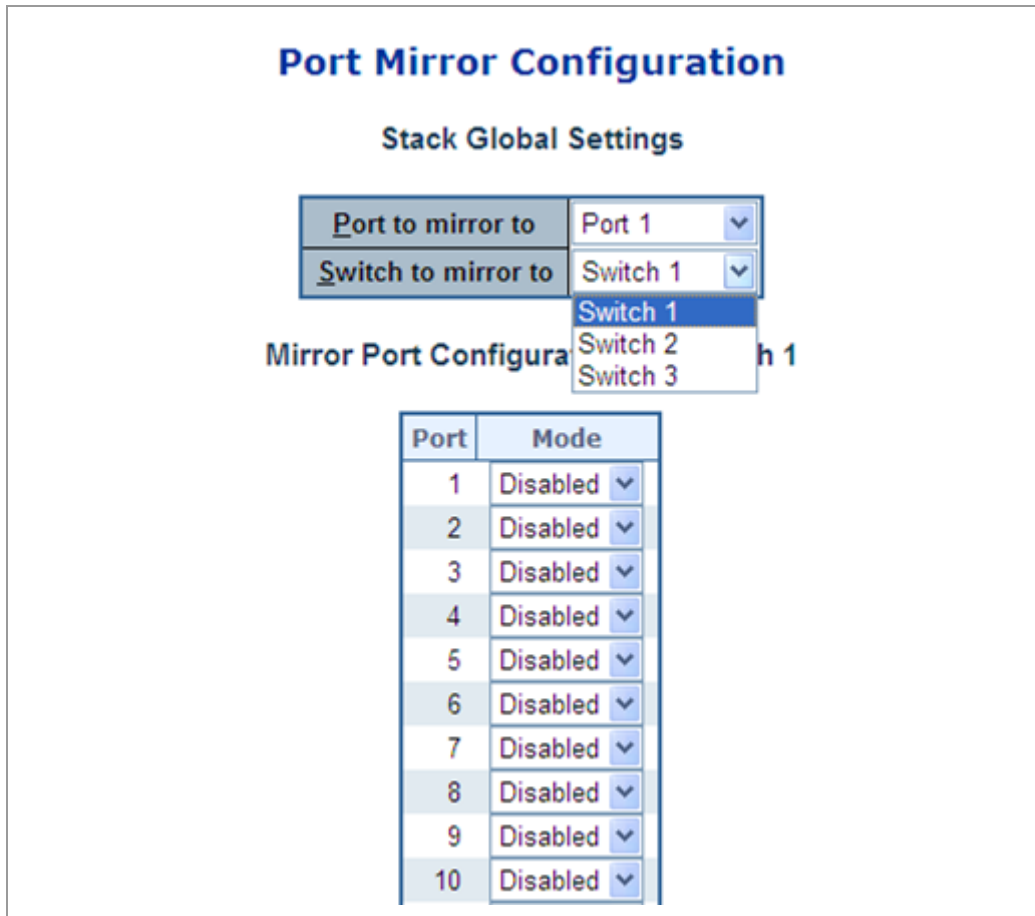
Figure 4-4-6 Port Mirror Configuration page screenshot

The page includes the following fields:

Object	Description
● **Switch to mirror to**	Frames from ports that have either source or destination mirroring enabled are mirrored to this switch.

4.4.5 SFP Module Information

You can check the physical or operational status of an SFP module via the SFP Module Information page. This page shows the operational status, such as the transceiver type, speed, wavelength and supports distance of SFP module on a specific interface. You can also use the hyperlink of port no. to check the statistics on an speficic interface.

SFP Module Information for Switch 1

Port	Type	Speed	Wave Length(nm)	Distance(m)
1	--	--	--	--
2	--	--	--	--
3	--	--	--	--
4	--	--	--	--
5	--	--	--	--
6	--	--	--	--
7	1000Base-LX	1000-Base	1310	10000
8	100Base-FX	155M	1310	40000
9	--	--	--	--
10	--	--	--	--
11	--	--	--	--
12	--	--	--	--
13	--	--	--	--
14	--	--	--	--
15	--	--	--	--
16	--	--	--	--
17	--	--	--	--
18	--	--	--	--
19	--	--	--	--
20	--	--	--	--
21	--	--	--	--
22	--	--	--	--
23	--	--	--	--
24	--	--	--	--

Auto-refresh ☐ Refresh

Figure 4-4-7 SFP Module Information page screenshot

The page includes the following fields:

Object	Description
• **Type**	Display the type of current SFP module, the possible types are: • 1000Base-SX • 1000Base-LX • 100Base-FX
• **Speed**	Display the spedd of current SFP module, the speed value or description is get from the SFP module. Different vendors SFP modules might shows different speed information.
• **Wave Length(nm)**	Display the wavelength of current SFP module, the wavelength value is get from the SFP module. Use this column to check if the wavelength values of two nodes are the matched while the fiber connection is failed.
• **Distance(m)**	Display the supports distance of current SFP module, the distance value is get from the SFP module.

4.5 Link Aggregation

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

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

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

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

The device supports the following Aggregation links :

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

- ■ **Link Aggregation Control Protocol** (**LACP**) LAGs - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.
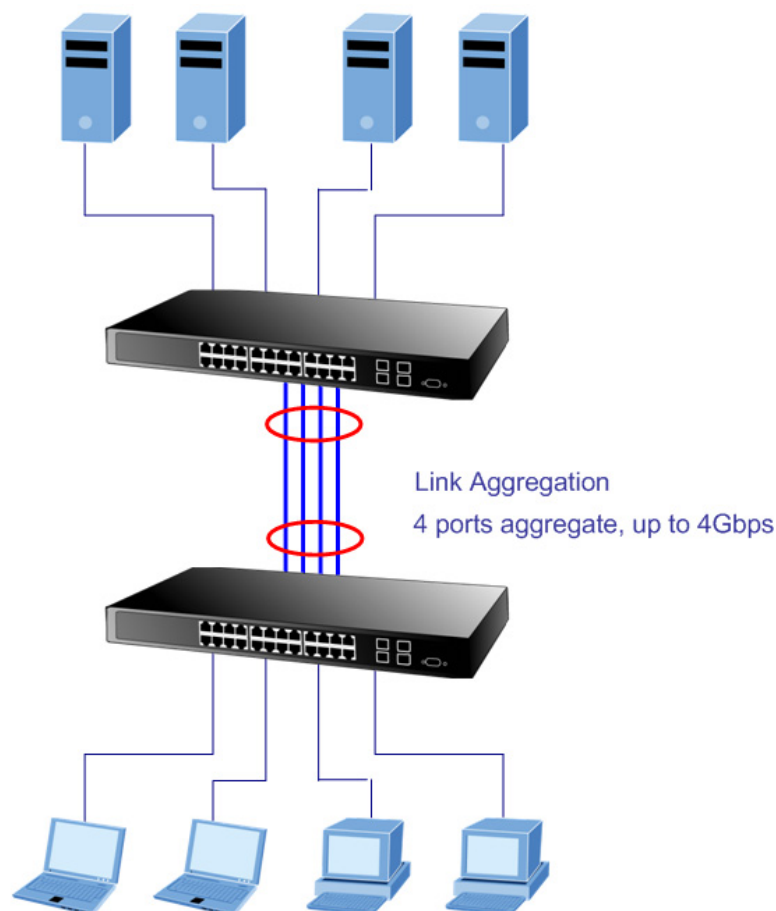
Figure 4-5-1 Link Aggregation

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

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 4 consecutive ports into a single dedicated connection between any two the Switch or other Layer 2 switches. However, before making any physical connections between devices, use the Link aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

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

It allows a maximum of 16 ports to be aggregated at the same time. The Managed Switch support Gigabit Ethernet ports (up to 12 groups). If the group is defined as a LACP static link aggregationing group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregationing group, then the number of ports must be the same as the group member ports.

The aggregation code ensures that frames belonging to the same frame flow (for example, a TCP connection) are always forwarded on the same link aggregation member port. Reording of frames within a flow is therefore not possible. The aggregation code is based on the following information:

- **Source MAC**
- **Destination MAC**
- **Source and destination IPv4 address.**
- **Source and destination TCP/UDP ports for IPv4 packets**

Normally, all 5 contributions to the aggregation code should be enabled to obtain the best traffic distribution among the link aggregation member ports. Each link aggregation may consist of up to 16 member ports. Any quantity of link aggregation s may be configured for the device (only limited by the quantity of ports on the device.) To configure a proper traffic distribution, the ports within a link aggregation must use the same link speed.

4.5.1 Static Aggregation Configuration

This page is used to configure the Aggregation hash mode and the aggregation group. The aggregation hash mode settings are global, whereas the aggregation group relate to the currently selected stack unit, as reflected by the page header.

Hash Code Contributors
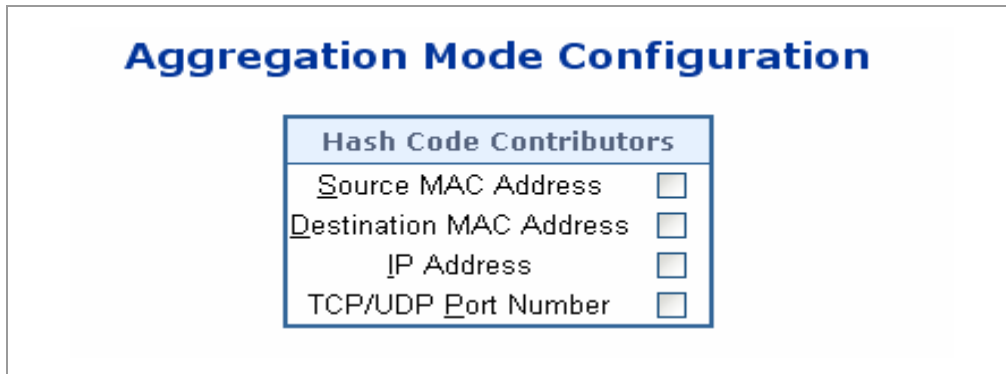
Figure 4-5-2 Aggregation Mode Configuration page screenshot

Object	Description
• **Source MAC Address**	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
• **Destination MAC Address**	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
• **IP Address**	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
• **TCP/UDP Port Number**	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Static Aggregation Group Configuration

The Aggregation Group Configuration screen in Figure 4-5-3 appears.

Figure 4-5-3 Aggregation Group Configuration page screenshot

The page includes the following fields:

.
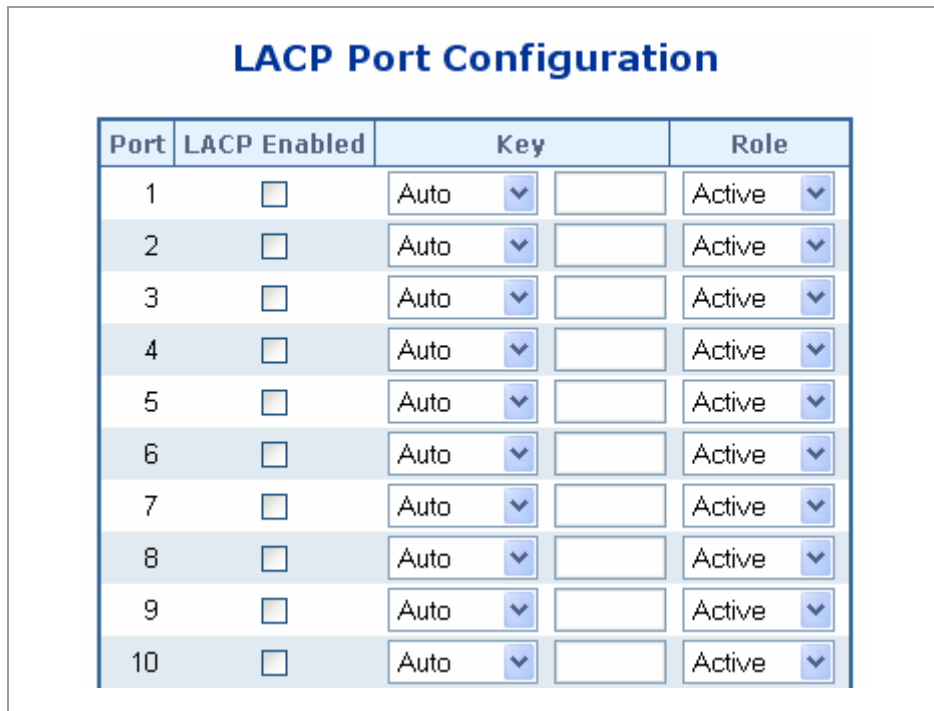
Object	Description
• **Locality**	Indicates the aggregation group type. This field is only valid for stackable switches. • **Global**: The group members may reside on different units in the stack. The device supports two 8-port global aggregations. • **Local**: The group members reside on the same unit. Each local aggregation may consist of up to 16 members.
• **Group ID**	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
• **Port Members**	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group.

4.5.2 LACP Configuration

Link Aggregation Control Protocol (LACP) - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. LACP allows switches connected to each other to discover automatically whether any ports are member of the same LAG.

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. The LACP port settings relate to the currently selected stack unit, as reflected by the page header. The LACP Port Configuration screen in Figure 4-5-4 appears.

Figure 4-5-4 LACP Port Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.
• **LACP Enabled**	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs per stack.
• **Key**	The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot. The default setting is "**Auto**"
• **Role**	The Role shows the LACP activity status. The Active will transmit LACP packets

each second, while Passive will wait for a LACP packet from a partner (speak if

spoken to).

4.5.3 LACP System Status

This page provides a status overview for all LACP instances. The LACP Status page display the current LACP aggregation

Groups and LACP Port status . The LACP System Status screen in Figure 4-5-5 appears.
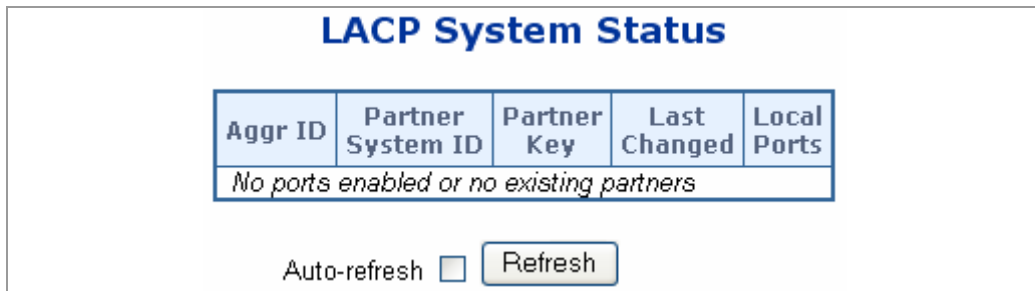
Figure 4-5-5 LACP System Status page screenshot

The page includes the following fields:

Object	Description
• **Aggr ID**	The Aggregation ID associated with this aggregation instance.
	For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
• **Partner System ID**	The system ID (MAC address) of the aggregation partner.
• **Partner Key**	The Key that the partner has assigned to this aggregation ID.
• **Last changed**	The time since this aggregation changed.
• **Local Ports**	Shows which ports are a part of this aggregation for this switch/stack.
	The format is: "Switch ID:Port".

4.5.4 LACP Port Status

This page provides a status overview for LACP status for all ports.

The LACP Port Status screen in Figure 4-5-6 appears.

LACP Port Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	No	-	-	-	-

Auto-refresh ☐ Refresh

Figure 4-5-6 LACP Port Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.
• **LACP**	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down.
• **Key**	The key assigned to this port. Only ports with the same key can aggregate together.
• **Aggr ID**	The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
• **Partner System ID**	The partners System ID (MAC address).
• **Partner Port**	The partners port number connected to this port.

4.5.5 LACP statistics

This page provides an overview for LACP statistics for all ports.

The LACP statistics screen in Figure 4-5-7 appears.

Figure 4-5-7 LACP Port statistics page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.
• **LACP Transmitted**	Shows how many LACP frames have been sent from each port.
• **LACP Received**	Shows how many LACP frames have been received at each port.
• **Discarded**	Shows how many unknown or illegal LACP frames have been discarded at each port.

4.6 VLAN

4.6.1 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.
	3. The 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:

- **IEEE 802.1Q VLAN**   Enable IEEE 802.1Q Tag based VLAN group
- **IEEE 802.1Q Tunneling**   Enables 802.1Q (QinQ) Tunneling
- **Private VLAN**   Creates/removes primary or community VLANs

4.6.2 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).

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

This Managed Switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- 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
- Priority tagging

■ 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.

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

normally.

Some relevant terms:

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

■ 802.1Q VLAN Tags

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

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

802.1Q Tag

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

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

Preamble	Destination Address	Source Address	VLAN TAG	Ethernet Type	Data	FCS
	6 bytes	6 bytes	4 bytes	2 bytes	46-1517 bytes	4 bytes
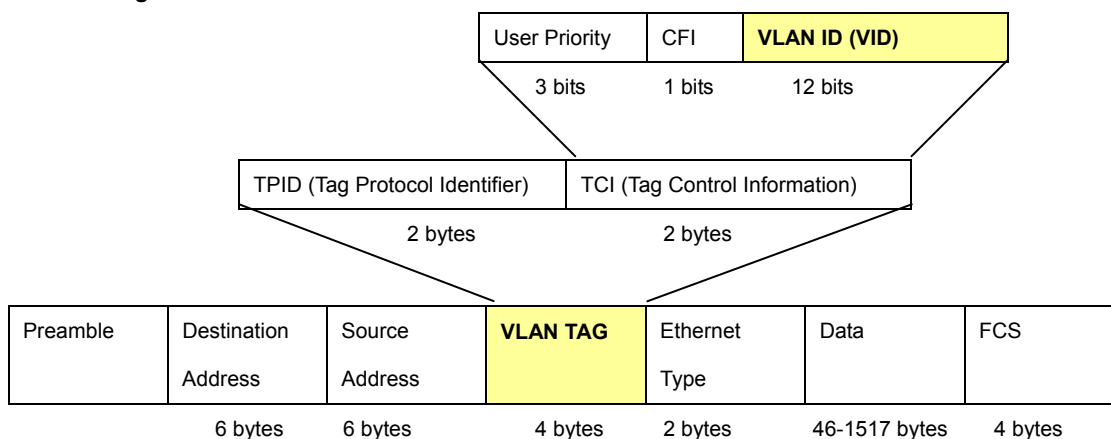
The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag

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

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

New Tagged Packet

Priority	CFI	VLAN ID
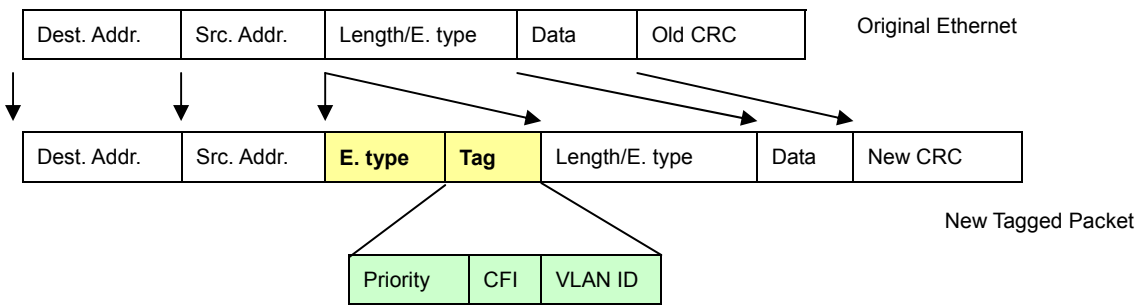
■ **Port VLAN ID**

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

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

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

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

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

■ **Default VLANs**

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

■ **Assigning Ports to VLANs**

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more

VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

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

■ **VLAN Classification**

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

■ **Port Overlapping**

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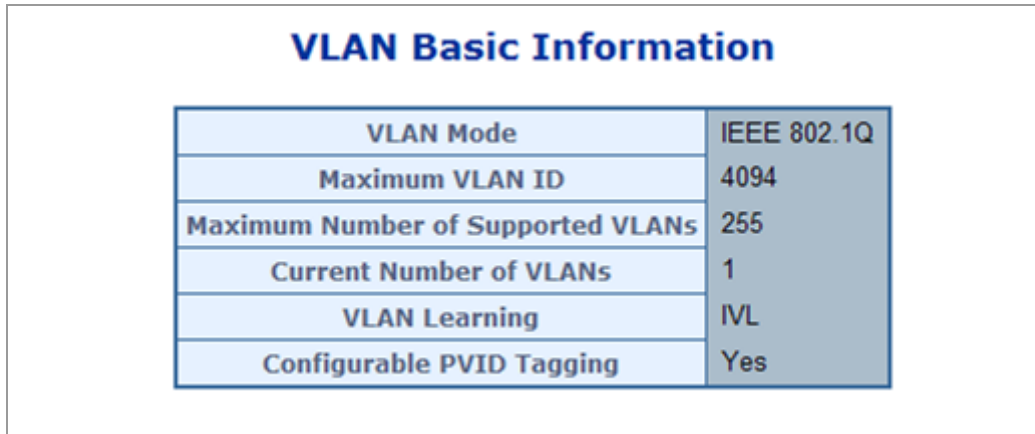
■ **Untagged VLANs**

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

4.6.3 VLAN Basic Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the Managed Switch.

The VLAN Basic Information screen in Figure 4-6-1 appears.

Figure 4-6-1 VLAN Basic Information page screenshot

The page includes the following fields:

Object	Description
• **VLAN Mode**	Display the current VLAN mode used by this Managed Switch ■ Port-Based ■ IEEE 802.1Q VLAN
• **Maximum VLAN ID**	Maximum VLAN ID recognized by this Managed Switch.
• **Maximum Number of Supported VLANs**	Maximum number of VLANs that can be configured on this Managed Switch.
• **Current number of VLANs**	Display the current number of VLANs
• **VLAN Learning**	Display the VLAN learning mode. The Managed Switch supports IVL (IVL Independent vlan learning).

4.6.4 VLAN Port Configuration

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

Understand nomenclature of the Switch

■ **IEEE 802.1Q Tagged and Untagged**

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

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

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

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

■ **IEEE 802.1Q Tunneling (Q-in-Q)**

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

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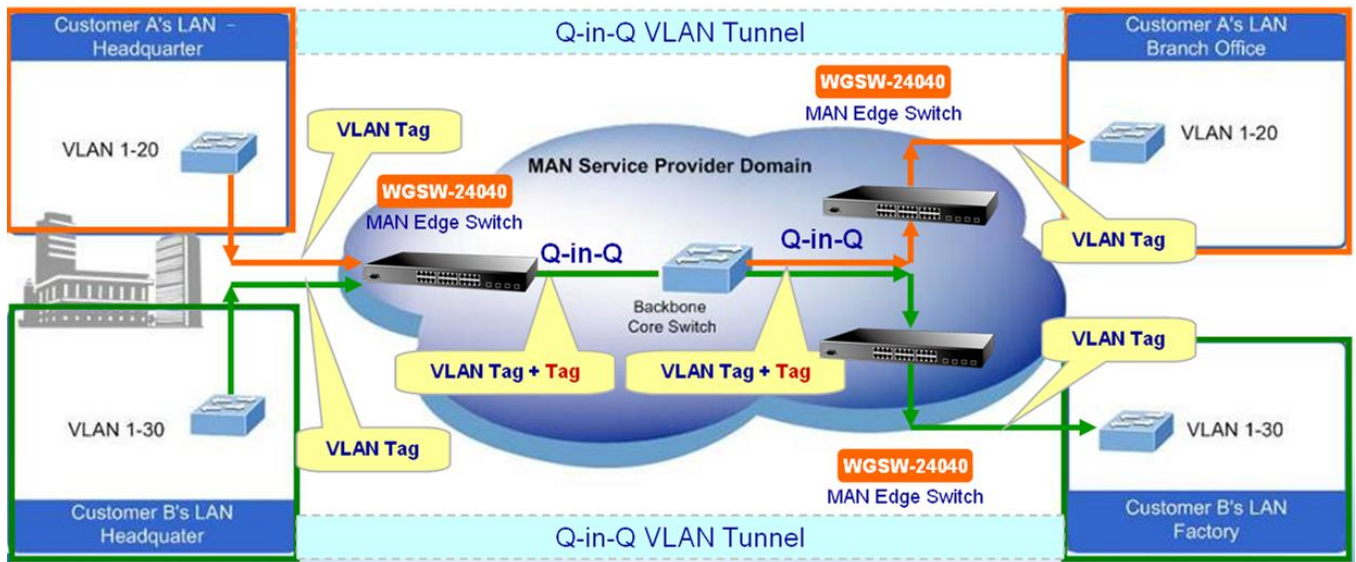
The Managed Switch supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so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

This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

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

VLAN Port Configuration

The VLAN Port Configuration screen in Figure 4-6-2 appears.

Figure 4-6-2 VLAN Port Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	This is the logical port number for this row.
• **PVID**	Allow assign PVID for selected port. The range for the PVID is **1-4094.** The PVID will be inserted into all **untagged** frames entering the ingress port. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.
• **Ingress Filtering**	Enable ingress filtering for a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).
• **Accept 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. By default, the field is set to All.
• **Link Type**	Allow 802.1Q Untagged or Tagged VLAN for selected port. When adding a VLAN to selected port, it tells the switch whether to keep or remove the tag from a frame on egress. • **Untag:** outgoing frames without VLAN-Tagged. • **Tagged:** outgoing frames with VLAN-Tagged.

- **Q-in-Q Mode**

  Sets the Managed Switch to **QinQ** mode, and allows the QinQ tunnel port to be configured. The default is for the Managed Switch to function in **Disable** mode.

  - **Disable**

    The port operates in its normal VLAN mode.
    (This is the default.)

  - **MAN Port:**

    Configures IEEE 802.1Q tunneling (QinQ) for an uplink port to another device within the service provider network.

  - **Customer Port:**

    Configures IEEE 802.1Q tunneling (QinQ) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.

- **Set Out layer VLAN tag ether type**

  The **Tag Protocol Identifier (TPID)** specifies the ethertype of incoming packets on a tunnel access port.

  - **802.1Q Tag : 8100**

  - **vMAN Tag : 88A8**

  Default : 802.1Q Tag

	The port must be a member of the same VLAN as the Port VLAN ID.
Note	

4.6.5 VLAN Membership Configuration

■   **Adding Static Members to VLANs (VLAN Index)**

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices.

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN. The VLAN Membership Configuration screen in Figure 4-6-3 appears.

Figure 4-6-3 VLAN Membership Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a VLAN entry, check this box. The entry will be deleted on all stack switch units during the next Save.
• **VLAN ID**	Indicates the ID of this particular VLAN.
• **Port Members**	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
• **Adding a New VLAN**	Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is thereafter present on the other stack switch units, but with no port members. A VLAN without any port members on any stack unit will be deleted when you click "Save". The button can be used to undo the addition of new VLANs.

4.6.6 Private VLAN Configuration

Overview

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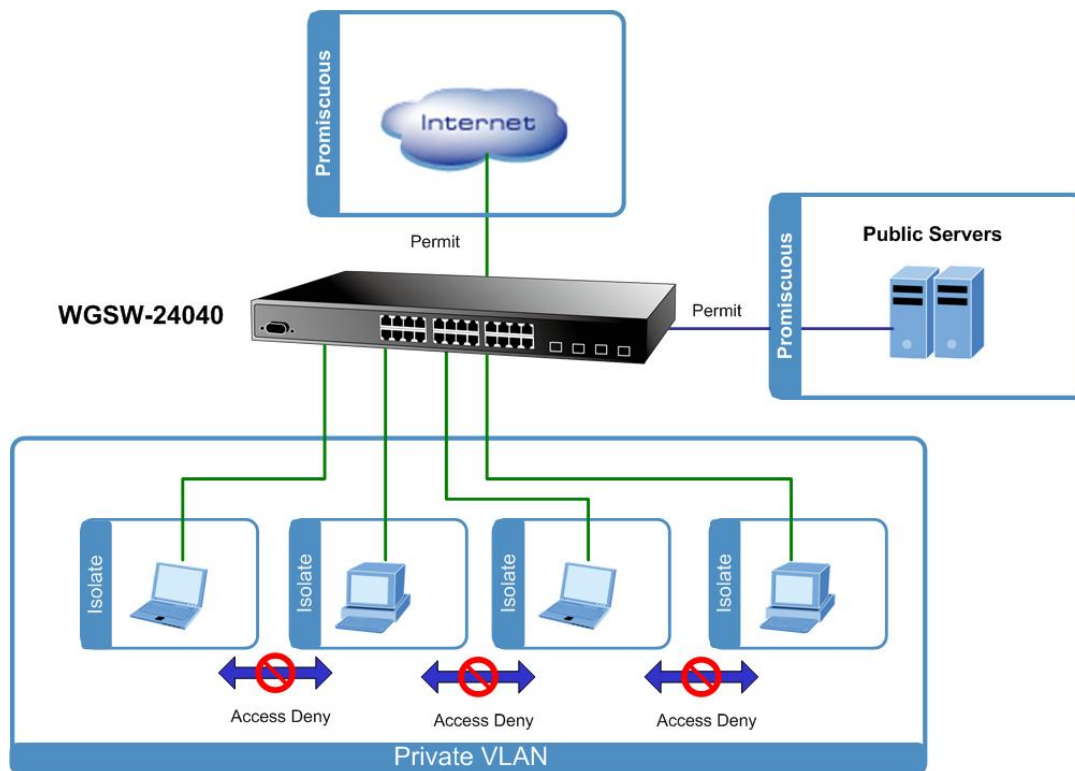
For private VLANs to be applied, the switch must first be configured for standard VLAN operation When this is in place, one or more of the configured VLANs can be configured as private VLANs. Ports in a private VLAN fall into one of these two groups:

- ■ **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 promiscous ports 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.

The port settings relate to the currently selected stack unit, as reflected by the page header. This feature works across the stack.
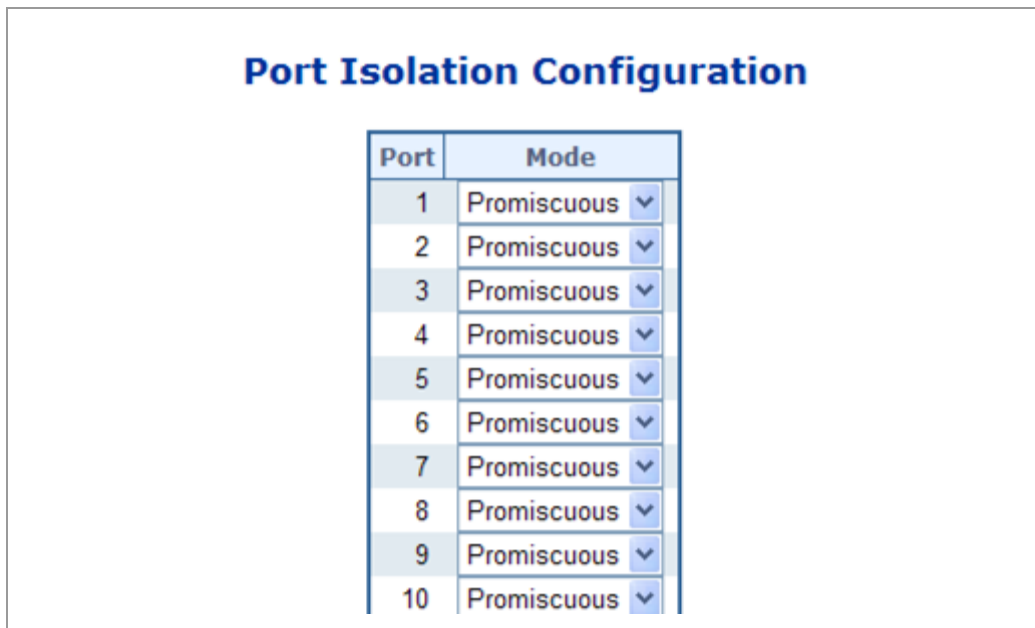
Figure 4-6-4 Private VLAN Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch interface.
• **PVLAN Port Type**	Displays private VLAN port types.
	Isolated A single stand-alone VLAN that contains one promiscuous port and one or more isolated (or host) ports. This VLAN conveys traffic between the isolated ports and a lone promiscuous port.
	- Promiscuous A promiscuous port can communicate with all the interfaces within a private VLAN. This is the default setting.

4.7 Rapid Spanning Tree Protocol

4.7.1 Theory

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

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

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

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

The Switch STP performs the following functions:

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

Bridge Protocol Data Units

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

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

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

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

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

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch

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

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

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

- Ports included in the STP are selected.

Creating a Stable STP Topology

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

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

STP Port States

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

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

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

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

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

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

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

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking

- From blocking to listening or to disabled

- From listening to learning or to disabled

- From learning to forwarding or to disabled

- From forwarding to disabled

- From disabled to blocking
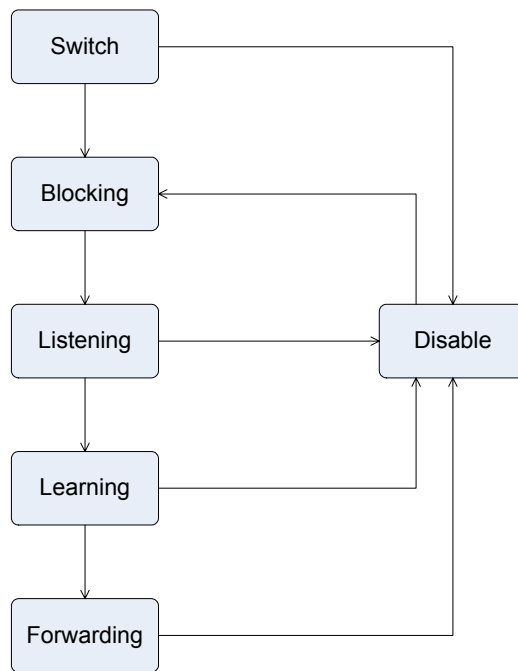
Figure 4-7-1 STP Port State Transitions

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: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	32768 + MAC

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

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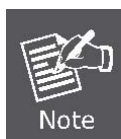
Note	Observe the following formulas when setting the above parameters: **Max. Age _ 2 x (Forward Delay - 1 second)** **Max. Age _ 2 x (Hello Time + 1 second)**

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.
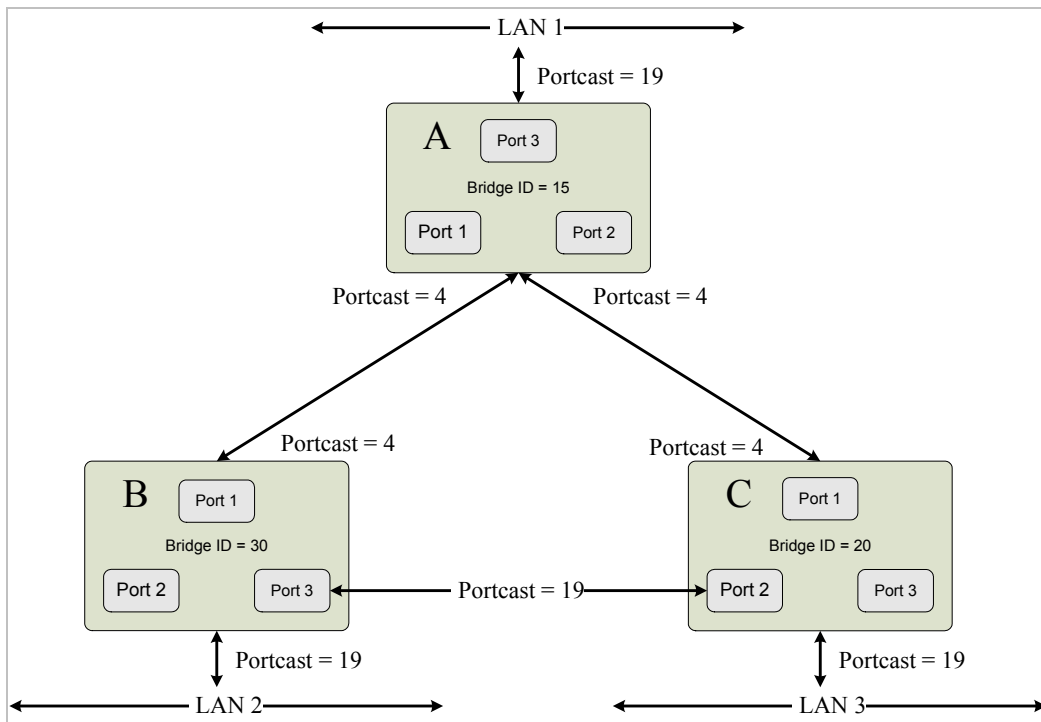
Figure 4-7-5 Before Applying the STA Rules

In this example, only the default STP values are used.
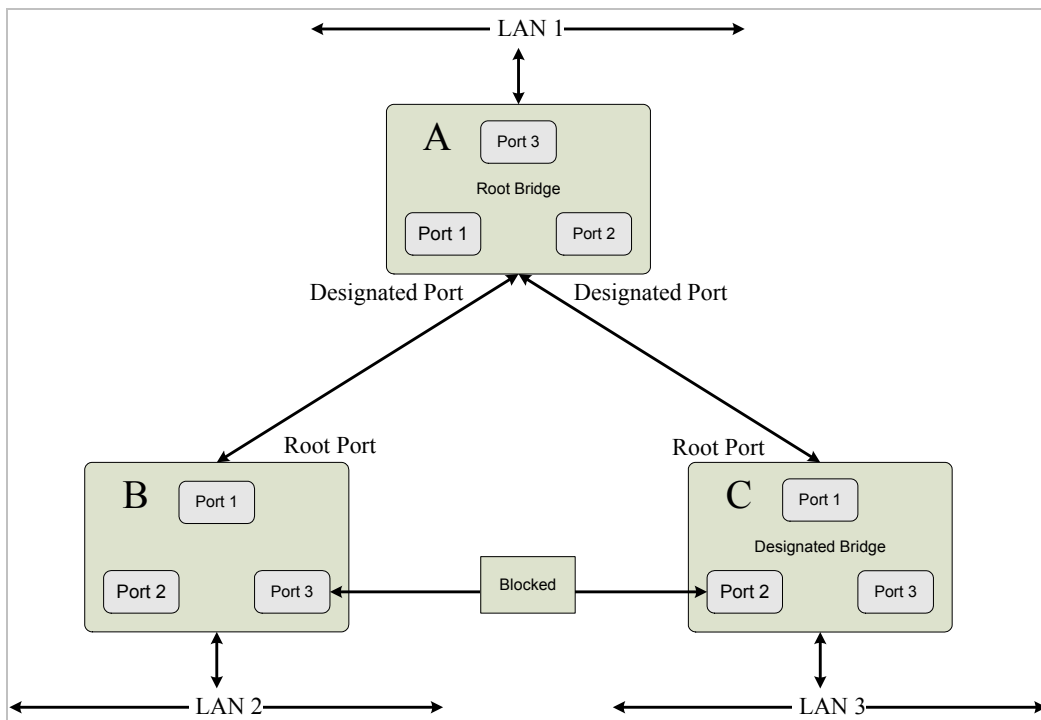
Figure 4-7-6 After Applying the STA Rules

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 = 4) 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 = 19). 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.

4.7.2 RSTP System Configuration

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

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

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

The RSTP System Configuration screen in Figure 4-7-7 appears.

Figure 4-7-7 RSTP System Configuration page screenshot

The page includes the following fields:

Object	Description
• **System Priority**	A value used to represent the priority component of a Bridge Identifier.
• **Max Age**	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 200 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)]
• **Forward Delay**	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds -Default: 15 -Minimum: The higher of 4 or [(Max. Message Age / 2) + 1] -Maximum: 30
• **Protocol Version**	The STP compatibility mode setting. **Normal – Rapid STP (802.1w)**: Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.

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

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

4.7.3 RSTP Bridge Status

This page provides a status overview for all RSTP bridge instances.

The displayed table contains a row for each RSTP bridge instance, where the column displays the following information:

The RSTP Bridge Status screen in appears.

Figure 4-7-8 RSTP Bridge Status page screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID associated with this Bridge instance. This is also a link to the RSTP Detailed Bridge Status.
• **Active Ports**	The number switch ports active in the RSTP bridge instance (aggregated ports count only as *one*).
• **Bridge ID**	The Bridge ID of this Bridge instance.
• **Root ID**	The Bridge ID of the currently elected root bridge.
• **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.
• **Topology Flag**	The current state of the Topology Change Flag for this Bridge instance.

4.7.4 RSTP Port Configuration

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

This page contain settings for aggregations and physical ports. The aggregation settings are stack global.

The RSTP port settings relate to the currently selected stack unit, as reflected by the page header.

The RSTP Port Configuration screen in Figure 4-7-9 appears.

Figure 4-7-9 RSTP Port Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical RSTP port.
• **RSTP Enabled**	Controls whether RSTP is enabled on this switch port.
• **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
• **Edge**	Controls whether the port is known to connect directly to edge devices. (*no* Bridges attached). The Edge flag is cleared by receipt of any BPDUs on the port. Transitioning to the forwarding state is faster for edge ports than for other ports. (This applies to physical ports only. Aggregations are always *Non-Edge*).
• **Point2Point**	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transitions to the forwarding state is faster for point-to-point LANs than for shared media. (This applies to physical ports only. Aggregations are always *forced Point2Point*).

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

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

Table 4-7-1 Recommended STP Path Cost Range

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

Table 4-7-2 Recommended STP Path Costs

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

Table 4-7-3   Default STP Path Costs

4.7.5 RSTP Port Status

This page displays the RSTP port status for port physical ports in the currently selected switch.

The RSTP Port Status screen in Figure 4-7-10 appears.

Figure 4-7-10 RSTP Port Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical RSTP port.
• **Role**	The current RSTP port role. The port role can be one of the following values: • **Disabled** • **Alternate** • **Backup** • **Root** • **Designated** • **Non-STP.**

• **State**	The current RSTP port state. The port state can be one of the following values:
	
	   • **Disabled**
	
	   • **Blocking**
	
	   • **Learning**
	
	   • **Forwarding**
	
	   • **Non-STP**.

• **Bridge**	The RSTP Bridge instance (VLAN ID). This is also a link to the RSTP Detailed Bridge Status, if the port is RSTP enabled.

4.7.6 RSTP Port Statistics

This page displays the RSTP port statistics counters for port physical ports in the currently selected switch.

The RSTP Port Statistics screen in appears.
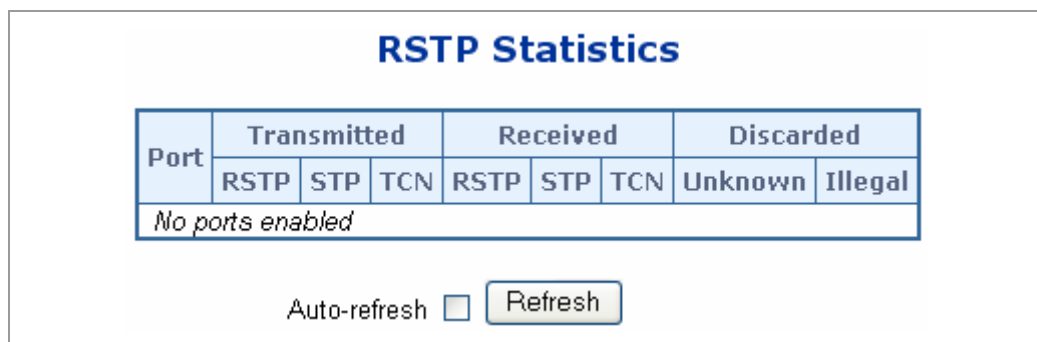
Figure 4-7-11 RSTP Statistics page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical RSTP port.
• **RSTP**	The number of RSTP Configuration BPDU's received/transmitted on the port.
• **STP**	The number of legacy STP Configuration BPDU's received/transmitted on the port.
• **TCN**	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
• **Discarded Unknown**	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
• **Discarded Illegal**	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

4.8 Quality of Service

4.8.1 Understand QOS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

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

You can use QoS on your system to:

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

QoS Terminology

- **Classifier**－classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The Switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** － is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- **Service Level**－defines the priority that will be given to a set of classified traffic. You can create and modify service levels.
- **Policy**－comprises a set of "rules" that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- **QoS Profile**－consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- **Rules**－comprises a service level and a classifier to define how theSwitch will treat certain types of traffic. Rules are associated with a QoS Profile (see above).

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

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

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

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

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

4.8.2 QoS Control List Configuration

This page lists the QCEs for a given QCL.

- Frames can be classified by 4 different QoS classes: **Low**, **Normal**, **Medium**, and **High**.

- The classification is controlled by a QoS assigned to each port.

- A QCL consists of an ordered list of up to 12 QCEs.

- Each QCE can be used to classify certain frames to a specific QoS class.

- This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority.

  Frames not matching any of the QCEs are classified to the default QoS Class for the port.

The QoS Control List Configuration screen in Figure 4-8-1 appears.

Figure 4-8-1 QoS Control List Configuration page screenshot

The page includes the following fields:

Object	Description
• **QCL #**	Select a QCL to display a table that lists all the QCEs for that particular QCL.
• **QCE Type**	Specifies which frame field the QCE processes to determine the QoS class of the frame.The following QCE types are supported: • **Ethernet Type**: The Ethernet Type field. If frame is tagged, this is the Ethernet Type that follows the tag header. • **VLAN ID**: VLAN ID. Only applicable if the frame is VLAN tagged. • **TCP/UDP Port**: IPv4 TCP/UDP source/destination port. • **DSCP**: IPv4 and IPv6 DSCP. • **ToS**: The 3 precedence bit in the ToS byte of the IPv4/IPv6 header (also known as DS field). • **Tag Priority**: User Priority. Only applicable if the frame is VLAN tagged or priority tagged.

- **Type Value**   Indicates the value according to its QCE type.

  - **Ethernet Type**: The field shows the Ethernet Type value.

  - **VLAN ID**: The field shows the VLAN ID.

  - **TCP/UDP Port**: The field shows the TCP/UDP port range.

  - **DSCP**: The field shows the IPv4/IPv6 DSCP value.

- **Traffic Class**   The QoS class associated with the QCE.

- **Modification Buttons**   You can modify each QCE in the table using the following buttons:

  ⊕: Inserts a new QCE before the current row.

  ℮: Edits the QCE.

  ⊙: Moves the QCE up the list.

  ⊙: Moves the QCE down the list.

  ⊗: Deletes the QCE.

  ⊕: The lowest plus sign adds a new entry at the bottom of the list of QCL.

4.8.2.1 QoS Control Entry Configuration

Configure a new QoS Control Entry on this page.

- ■   Frames can be classified by up to 4 different QoS classes: **Low**, **Normal**, **Medium**, and **High**.

- ■   The classification is controlled by a QCL assigned to each port.

- ■   A QCL consists of an ordered list of up to **12** QCEs.

- ■   Each QCE can be used to classify certain frames to a specific QoS Class.

- ■   This classification can be based on parameters such as **VLAN ID**, **UDP/TCP port**, **IPv4/IPv6 DSCP** or **Tag Priority.**

     Frames not matching any of the QCEs are classified to the default QoS Class for the port.

The QCE Configuration screen in Figure 4-8-2 appears.
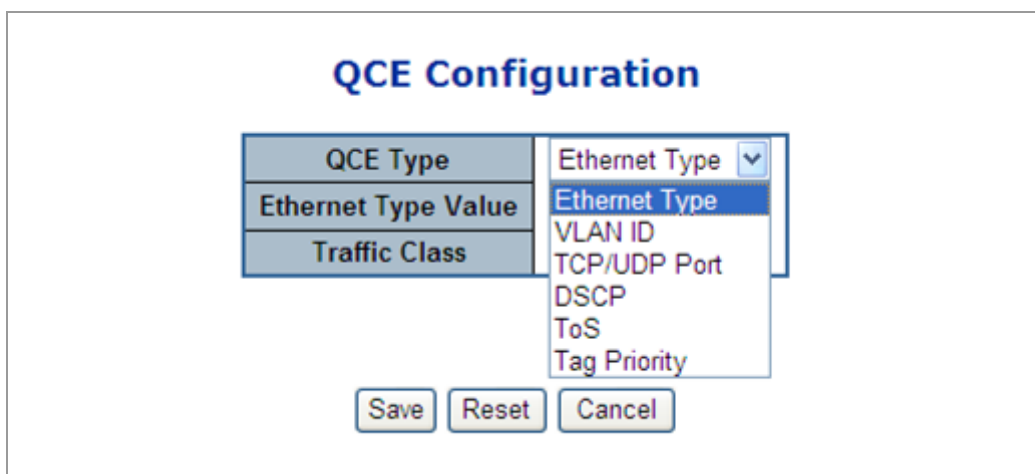
Figure 4-8-2 QCE Configuration page screenshot

The page includes the following fields:

Object	Description
• **QCE Type**	Select the available type for the specific QCE. • **Ethernet Type**: Matches the received frame's EtherType against the QCE Key. • **VLAN ID**: Matches the frame's VID against the QCE Key. • **TCP/UDP Port**: Matches the destination port and the source port against the QCE Key. • **DSCP**: Matches the received IPv4/IPv6 DSCP value (6 bits) against the two DSCP values in the QCE Key. • **ToS**: Uses the precedence part of the IPv4/IPv6 ToS (3 bits) as an index to the eight QoS Class values in the QCE Key. • **Tag Priority**: Uses the User Priority value (3 bits) as an index to the eight QoS Class values in the QCE Key.
• **Type Value**	Configure the values according to the QCE type you select. • **Ethernet Type**: The allowed values for this type range from 0x600 (1536) to 0xFFFF (65535). • **VLAN ID**: The allowed values for this type range from 1 to 4095. • **TCP/UDP Port Range**: Specify whether there is a range or a specific port number. The port range allowed is from 0 to 65535. • **DSCP**: The allowed range is 0 to 63. ToS or Tag Priority do not have type value settings.
• **Traffic Class**	Select a traffic class of Low, Normal, Medium, or High to apply to the QCE. If the QCE type is ToS or Tag Priority, there are 8 rows of traffic class that can be configured for each priority.

4.8.3 Port QoS Configuration

This page allows you to configure QoS settings for each port.

- Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

- The classification is controlled by a QCL that is assigned to each port.

- A QCL consists of an ordered list of up to 12 QCEs.

- Each QCE can be used to classify certain frames to a specific QoS class.

- This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority.

- Frames not matching any of the QCEs are classified to the default QoS class for the port.

- The settings relate to the currently selected stack unit, as reflected by the page header.

The Port QoS Configuration screen in Figure 4-8-3 appears.

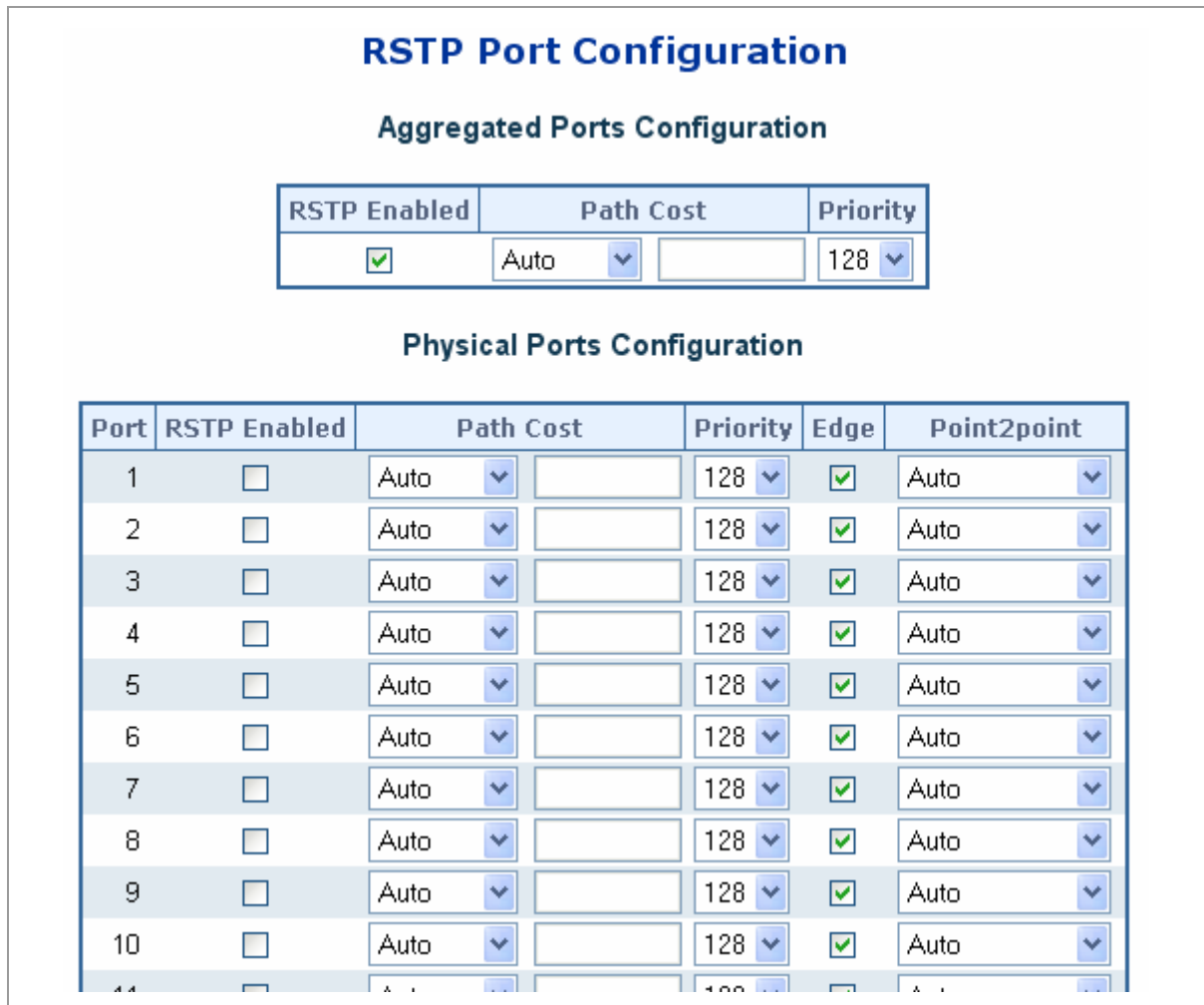**Figure 4-8-3** Port QoS Configuration page screenshot

The page includes the following fields:

Object	Description
• **Number of Classes**	Configure the number of traffic classes as "1", "2", or "4". The default value is "4".
• **Port**	The logical port for the settings contained in the same row.
• **Default Class**	Configure the default QoS class for the port, that is, the QoS class for frames not matching any of the QCEs in the QCL.
• **QCL #**	Select which QCL to use for the port.
• **User Priority**	Select the default user priority for this port when adding a Tag to the untagged frames.
• **Queuing Mode**	Select which Queuing mode for this port.
• **Queue Weighted**	Setting Queue weighted(Low:Normal:Medium:High) if the "Queuing Mode" is "Weighted".

4.8.4 QCL Configuration Wizard

This handy wizard helps you set up a QCL quickly.

The QCL Configuration Wizard screen in Figure 4-8-5 appears.
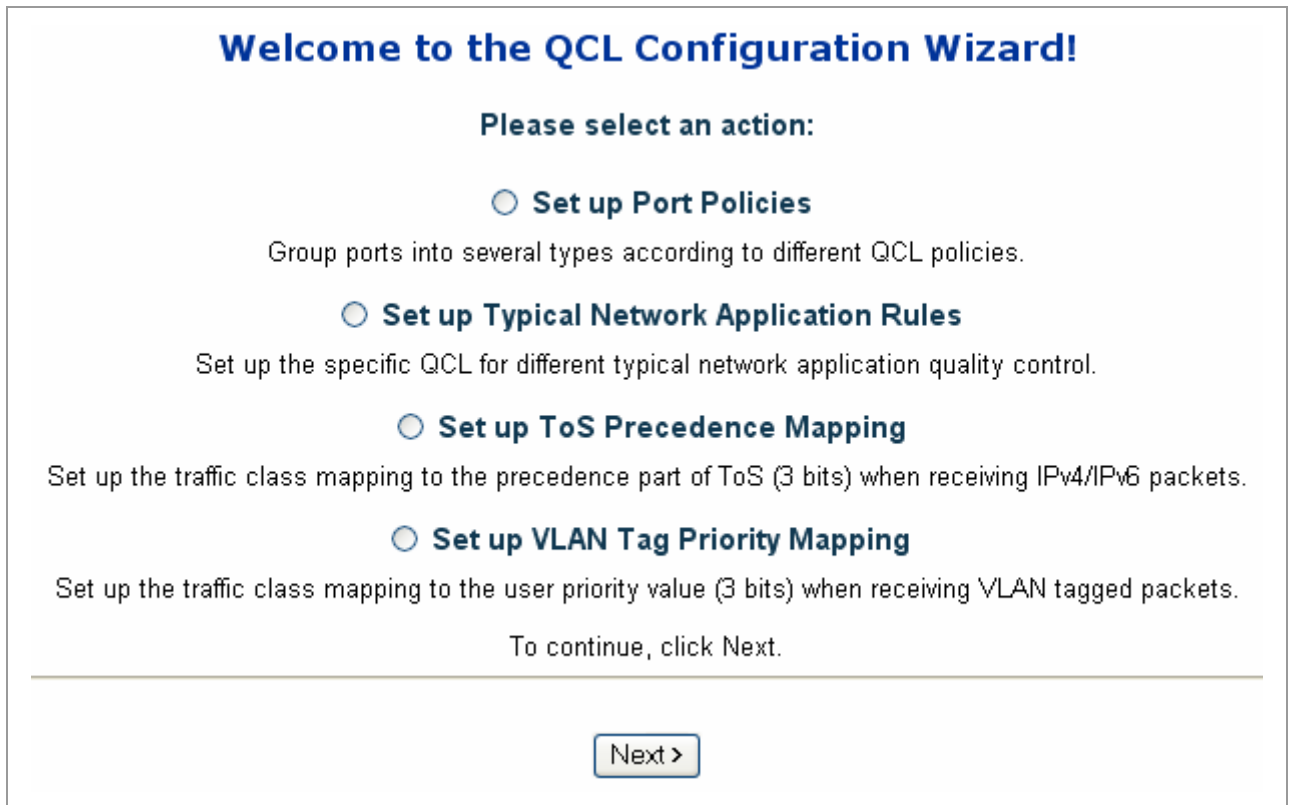
Figure 4-8-5 Welcome to the QCL Configuration Wizard page screenshot

The page includes the following fields:

Object	Description
• **Set up Port Policies**	Group ports into several types according to different QCL policies.
• **Set up Typical Network Application Rules**	Set up the specific QCL for different typical network application quality control.
• **Set up ToS Precedence Mapping**	Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
• **Set up VLAN Tag Priority Mapping**	Set up the traffic class mapping to the User Priority value (3 bits) when receiving VLAN tagged packets.

4.8.4.1 Set up Policy Rules

Group ports into several types according to different QCL policies. The settings relate to the currently selected stack unit, as reflected by the page header. The screen in Figure 4-8-6 appears..
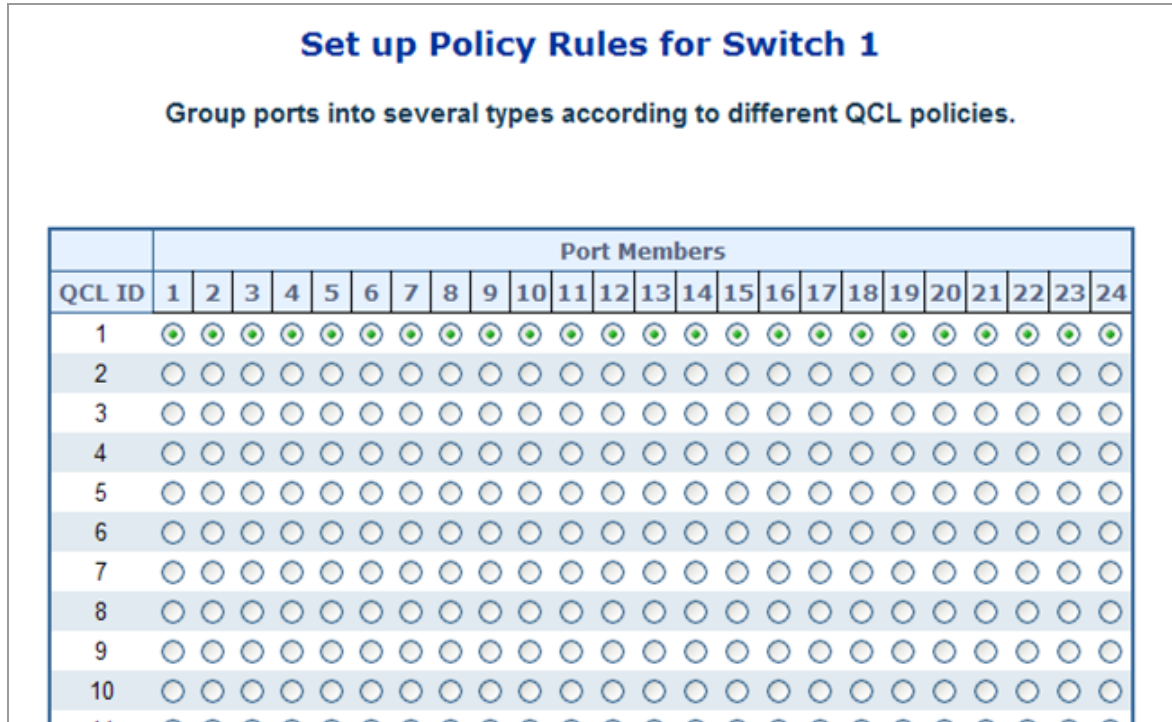
Figure 4-8-6 Set up Policy Rules page screenshot

The page includes the folling fileds:

Object	Description
• **QCL ID**	Frames that hit this QCE are set to match this specific QCL.
• **Port Members**	A row of radio buttons for each port is displayed for each QCL ID. To include a port in a QCL member, click the radio button.

Once the QCL configuration wizard is finished, the below screen appears.
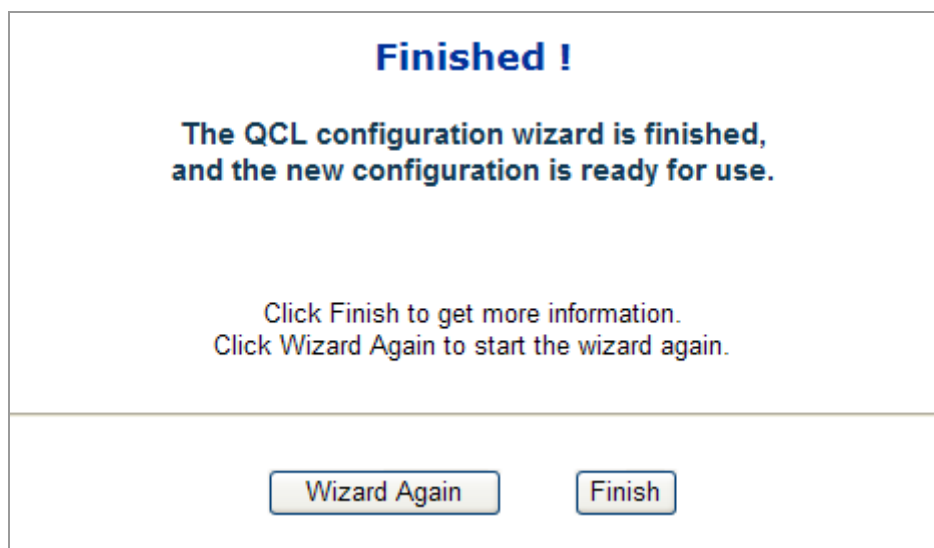
4.8.4.2 Set up Typical Network Application Rules

Set up the specific QCL for different typical network application quality control.

■ **STEP-1**

Set up the specific QCL for different typical network application quality control by selecting the network application type for your rule:

Figure 4-8-7 Set up Typical Netowrk Application Rules page screenshot

The page includes the folling fileds:

Object	Description
• **Audio and Video**	Indicates the common servers that apply to the specific QCE .
	The common servers are:
	• **QuickTime 4 Server**
	• **MSN Messenger Phone**
	• **Yahoo Messenger Phone**
	• **Napster**
	• **Real Audio**
• **Games**	Indicates the common games that apply to the specific QCE.

- **User Definition**   Indicates the user definition that applies to the specific QCE. The user definitions are:

  - **Ethernet Type:** Specify the Ethernet Type filter for this QCE. The allowed range is 0x600 to 0xFFFF.
  - **VLAN ID:** VLAN ID filter for this QCE. The allowed range is 1 to 4095.
  - **UDP/TCP Port:** Specify the TCP/UDP port filter for this QCE. The allowed range is 0 to 65535.
  - **DSCP:** Specify the DSCP filter for this QCE. The allowed range is 0 to 63.

Buttons

Cancal Wizard : Click to cancel the wizard.

< Back : Click to go back to the previous wizard step.

Netx > : Click to continue the wizard.

■   **STEP-2**

According to your selection on the previous page, this wizard will create specific QCEs (QoS Control Entries) automatically. First select the QCL ID for these QCEs, and then select the traffic class. Different parameter options are displayed depending on the frame type that you selected.
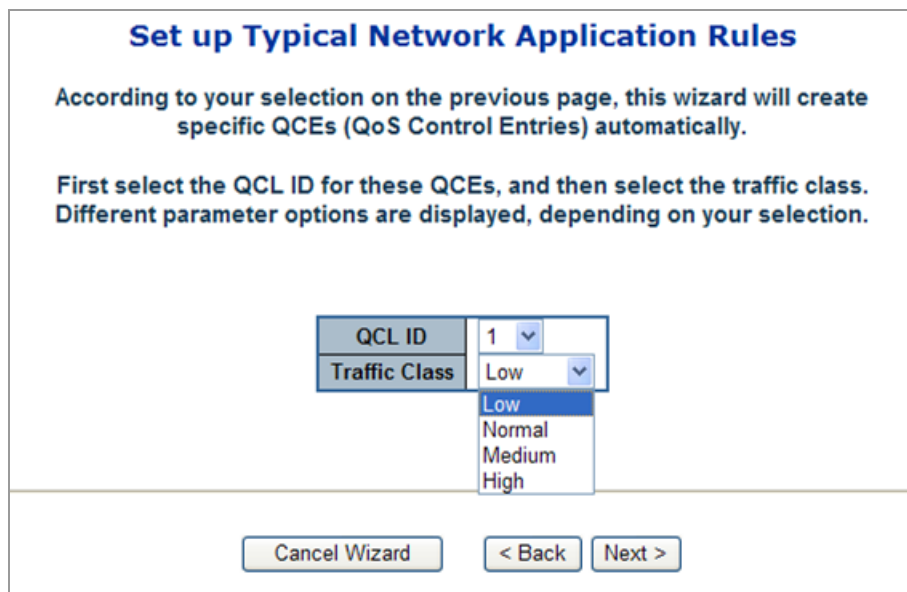
Figure 4-8-9 Set up Typical Netowrk Application Rules page 2 screenshot

The page includes the folling fileds:

Object	Description
• **QCL ID**	Select the QCL ID to which these QCEs apply,
• **Traffic Class**	Select a traffic class of Low, Normal, Medium, or High to apply to the QCE.

4.8.4.3 Set up ToS Precedence Mapping

Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets. The screen in Figure 4-8-10 appears.
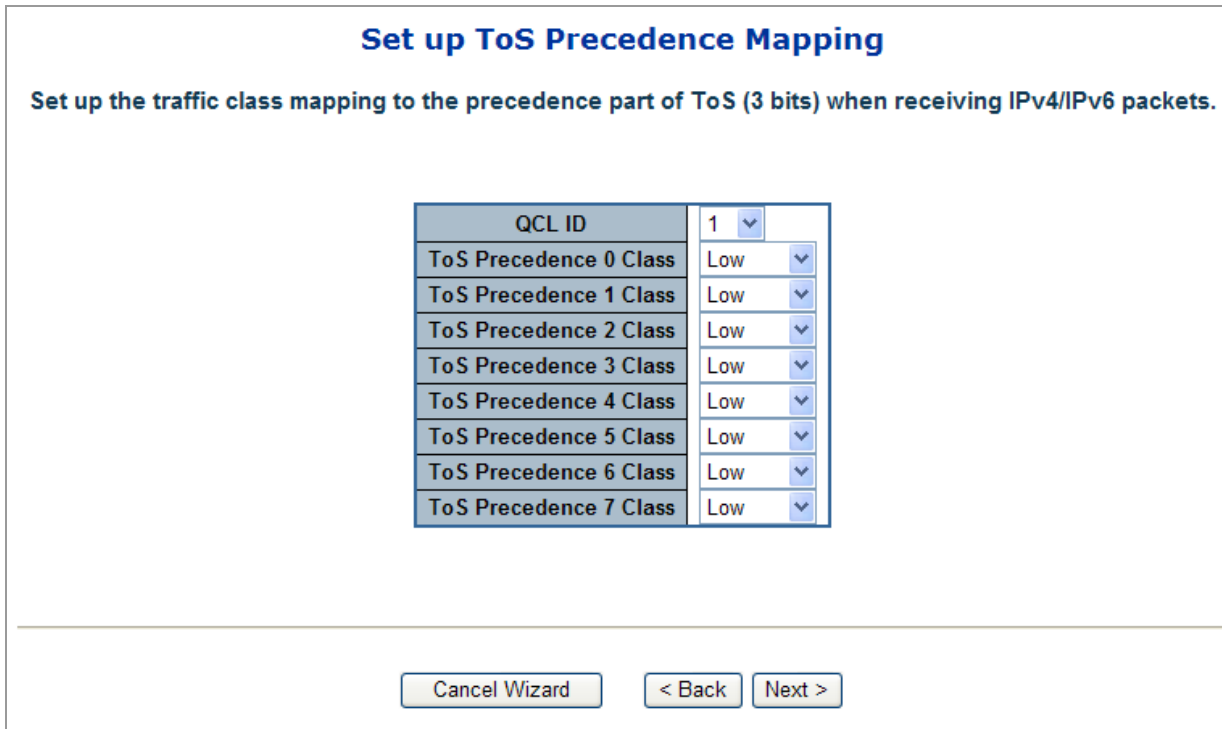
Figure 4-8-10 Set up ToS Precedence Mapping page screenshot

The page includes the folling fileds:

Object	Description
• **QCL ID**	Select the QCL ID to which this QCE applies.
• **ToS Precedence Class**	Select a traffic class of Low, Normal, Medium, or High to apply to the QCE.

The QCL configuration wizard is finished, and the new configuration is ready for use.

4.8.4.4 Set up VLAN Tag Priority Mapping

Set up the traffic class mapping to the User Priority value (3 bits) when receiving VLAN tagged packets.

The screen in Figure 4-8-11 appears.

Figure 4-8-11 Set up VLAN Tag Priority Mapping page screenshot

The page includes the folling fileds:

Object	Description
• **QCL ID**	Select the QCL ID to which this QCE applies.
• **VLAN Priority Class**	Select a traffic class of Low, Normal, Medium, or High to apply to the QCE.

The QCL configuration wizard is finished, and the new configuration is ready for use.

4.8.5 QoS Statistics

This page provides statistics for the different queues for all switch ports. The ports belong to the currently selected stack unit, as reflected by the page header. The QoS Statistics screen in Figure 4-8-12 appears.

QoS Statistics

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	2296	0	0	0	0	0	0	1817
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0

Auto-refresh ☐ [Refresh] [Clear]

Figure 4-8-12 QoS Statistics page screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Low Queue**	There are 4 QoS queues per port with strict or weighted queuing scheduling. This is the lowest priority queue.
• **Normal Queue**	This is the normal priority queue of the 4 QoS queues. It has higher priority than the "Low Queue".
• **Medium Queue**	This is the medium priority queue of the 4 QoS queues. It has higher priority than the "Normal Queue".
• **High Queue**	This is the highest priority queue of the 4 QoS queues.
• **Receive/Transmit**	The number of received and transmitted packets per port.

4.8.6 Bandwidth Control

Configure the switch port rate limit for Policers and Shapers on this page. The settings relate to the currently selected stack unit, as reflected by the page header. The screen Bandwidth Control in Figure 4-8-13 appears.

Figure 4-8-13 XXXXXXX page screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Policer Enabled**	Enable or disable the port policer. The default value is "Disabled".
• **Policer Rate**	Configure the rate for the port policer. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
• **Policer Unit**	Configure the unit of measure for the port policer rate as kbps or Mbps. The default value is "kbps".
• **Shaper Enabled**	Enable or disable the port shaper. The default value is "Disabled".
• **Shaper Rate**	Configure the rate for the port shaper. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
• **Shaper Unit**	Configure the unit of measure for the port shaper rate as kbps or Mbps. The default value is "kbps".

4.8.7 Storm Control Configuration

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

- **Unicast** storm rate control

- **Multicast** storm rate control

- **Broadcast** storm rate control.

The rate is 2^n, where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

The Storm Control Configuration screen in Figure 4-8-14 appears.

Figure 4-8-14 Storm Control Configuration page screenshot

The page includes the following fields:

Object	Description
• **Frame Type**	The settings in a particular row apply to the frame type listed here: • **unicast** • **multicast** • **broadcast.**
• **Status**	Enable or disable the storm control status for the given frame type.
• **Rate**	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

4.9 Multicast

4.9.1 IGMP Snooping

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

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.
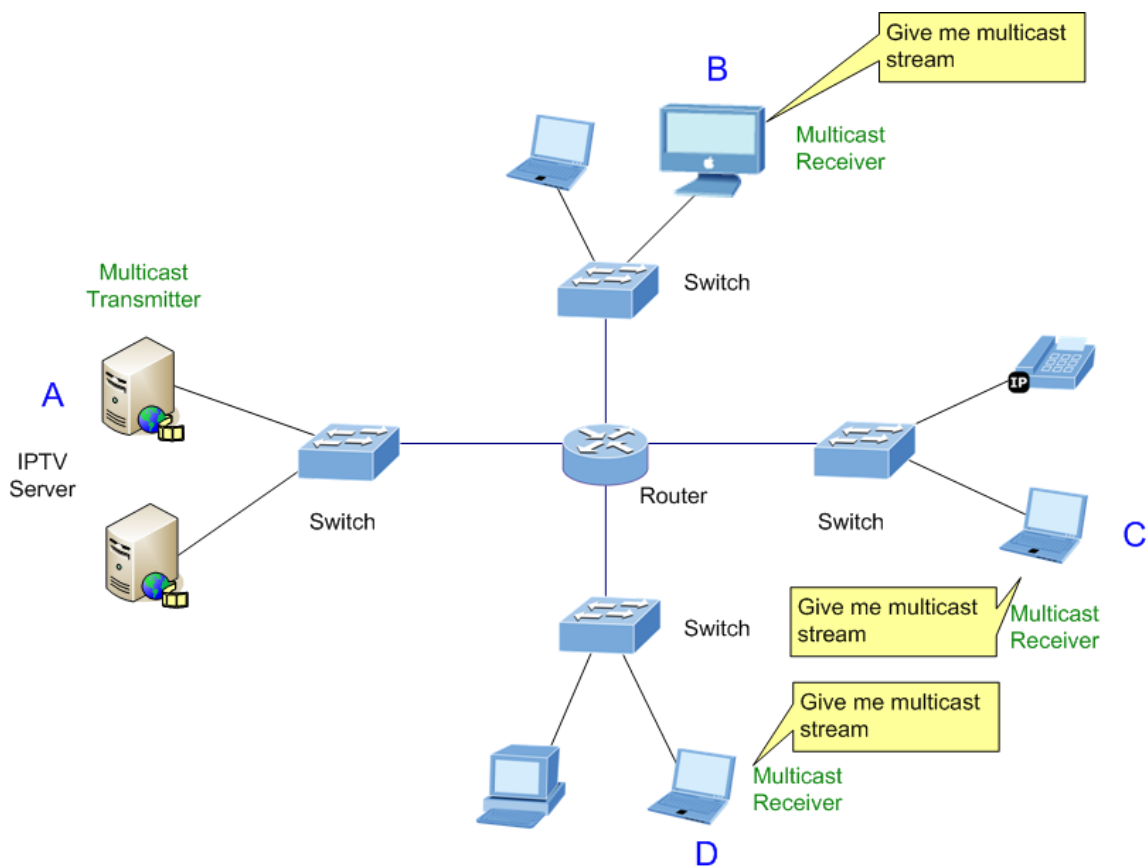
Figure 4-9-1 Multicast Service
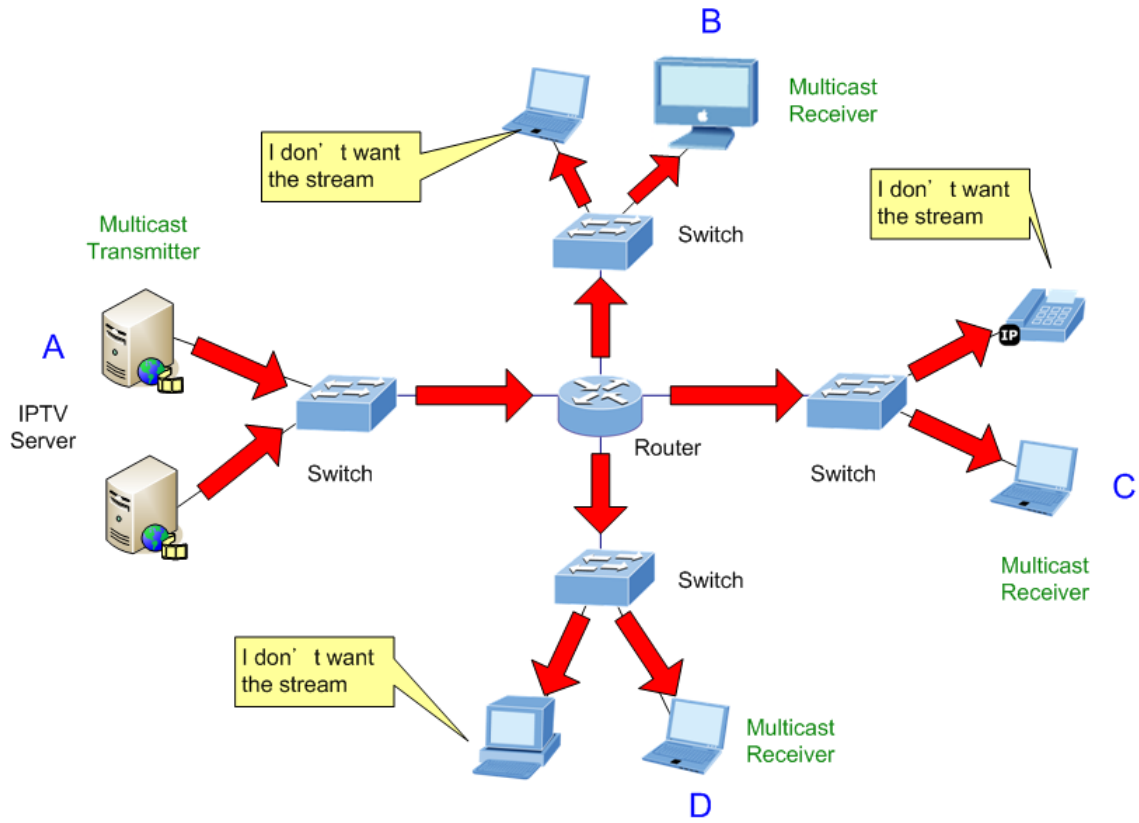
Figure 4-9-2 Multicast flooding
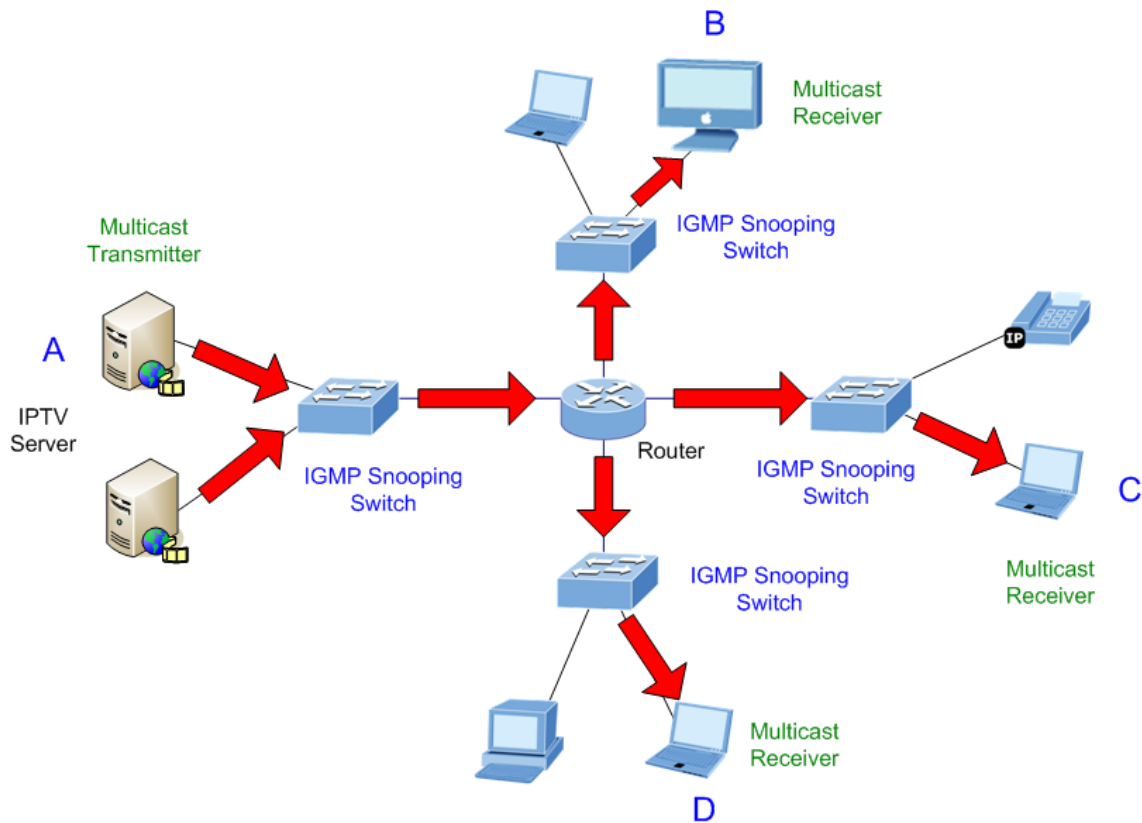
Figure 4-9-3 IGMP Snooping multicast stream control

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)		
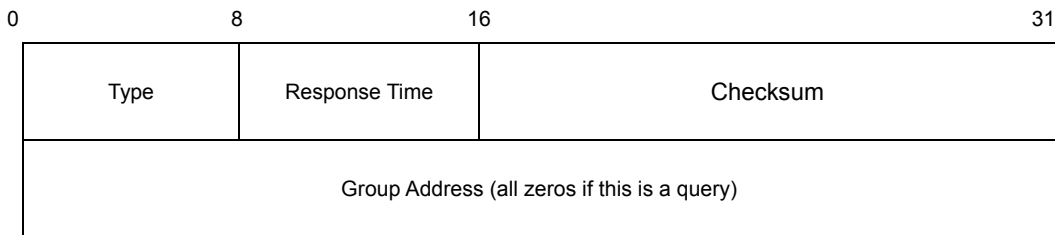
The IGMP Type codes are shown below:

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:
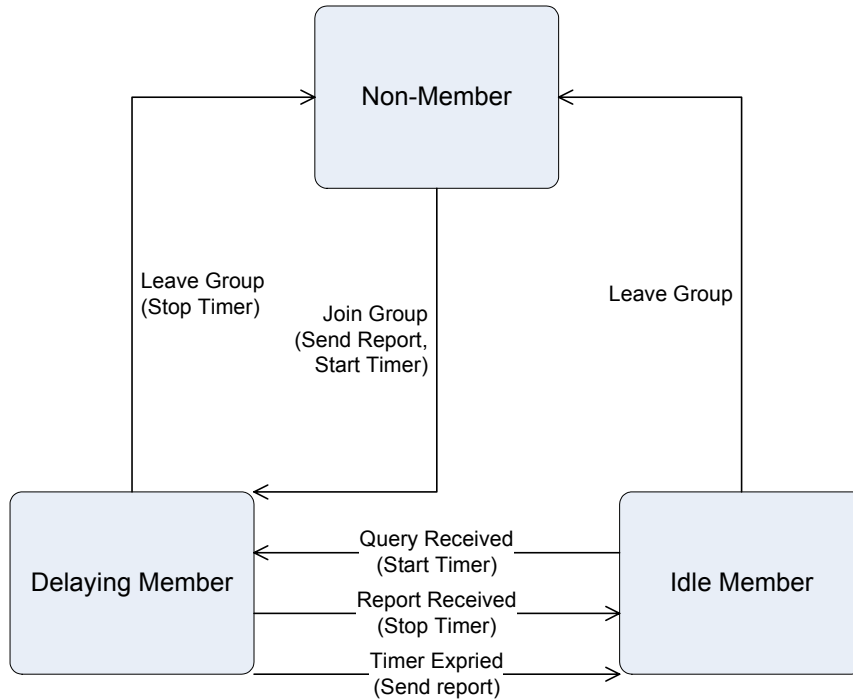
Figure 4-9-4 IGMP State Transitions

- **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.

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

4.9.2 IGMP Snooping Configuration

This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header.

The IGMP Snooping Configuration screen in Figure 4-9-5 appears.

Figure 4-9-5 IGMP Snooping Configuration page screenshot

The page includes the following fields:

Object	Description
• **Snooping Enabled**	Enable the Global IGMP Snooping.
• **Unregistered IPMC Flooding enabled**	Enable unregistered IPMC traffic flooding.
• **VLAN ID**	The VLAN ID of the entry.
• **IGMP Snooping Enabled**	Enable the per-VLAN IGMP Snooping.
• **IGMP Querier**	Enable the IGMP Querier in the VLAN. The Querier will send out if no Querier received in 255 seconds after IGMP Querier Enabled. Each Querier's interval is 125 second, and it will stop act as an IGMP Querier if received any Querier from other devices.

4.9.3 IGMP Port Related Configuration

This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header.

The IGMP Port Related Configuration screen in Figure 4-9-6 appears.

Figure 4-9-6 IGMP Port Related Configuration page screenshot

The page includes the following fields:

Object	Description
• **Router Port**	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. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
• **Fast Leave**	Enable the Fast Leave on the port.

4.9.4 IGMP Snooping Status

This page provides IGMP Snooping status.

The status relate to the currently selected stack unit, as reflected by the page header.

The IGMP Snooping status screen in Figure 4-9-7 appears.

Figure 4-9-7 IGMP Snooping status page screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **Groups**	The present IGMP groups. Max. are 128 groups for each VLAN.
• **Port Members**	The ports that are members of the entry.
• **Querier Status**	Show the Querier status is "ACTIVE" or "IDLE".
• **Querier Transmit**	The number of Transmitted Querier.
• **Querier Receive**	The number of Received Querier.
• **V1 Reports Receive**	The number of Received V1 Reports.
• **V2 Reports Receive**	The number of Received V2 Reports.
• **V3 Reports Receive**	The number of Received V3 Reports.
• **V2 Leave Receive**	The number of Received V2 Leave.

4.9.5 Multicast Address Table

The Multicast Address Table screen in Figure 4-9-8 appears.
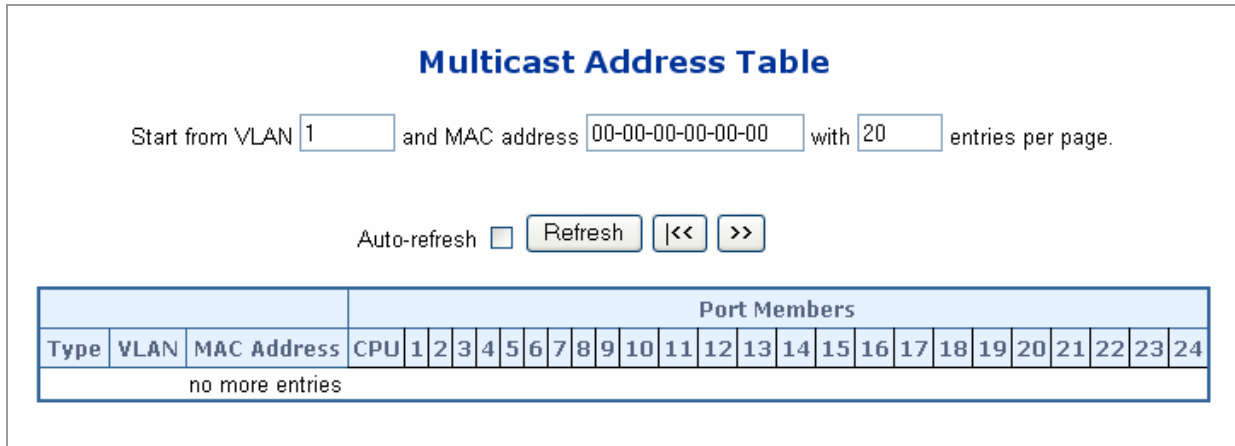
Figure 4-9-8 Multicast Address Table page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **VLAN ID**	The VLAN ID for the entry.
• **MAC Address**	The MAC address for the entry.
• **Port Members**	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

4.10 IEEE 802.1X Network Access Control

Overview of 802.1X (Port-Based) Authentication

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

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

Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide.

4.10.1 Understanding IEEE 802.1X Port-Based Authentication

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

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

This section includes this conceptual information:

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

■   **Device Roles**

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.
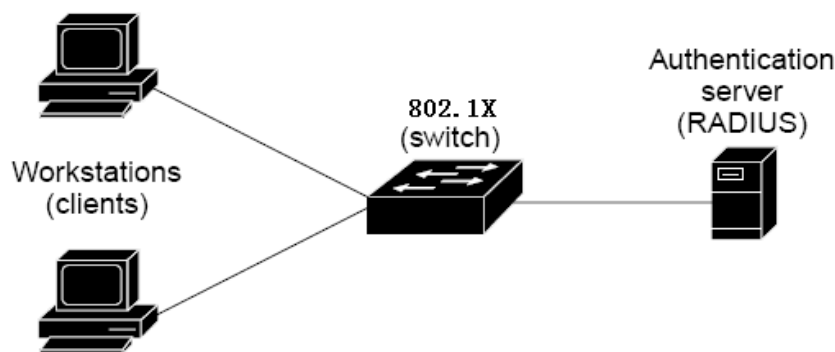
Figure 4-10-1

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

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

145

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

■ **Authentication Initiation and Message Exchange**

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

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

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

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

The specific exchange of EAP frames depends on the authentication method being used. "Figure 4-10-1" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.
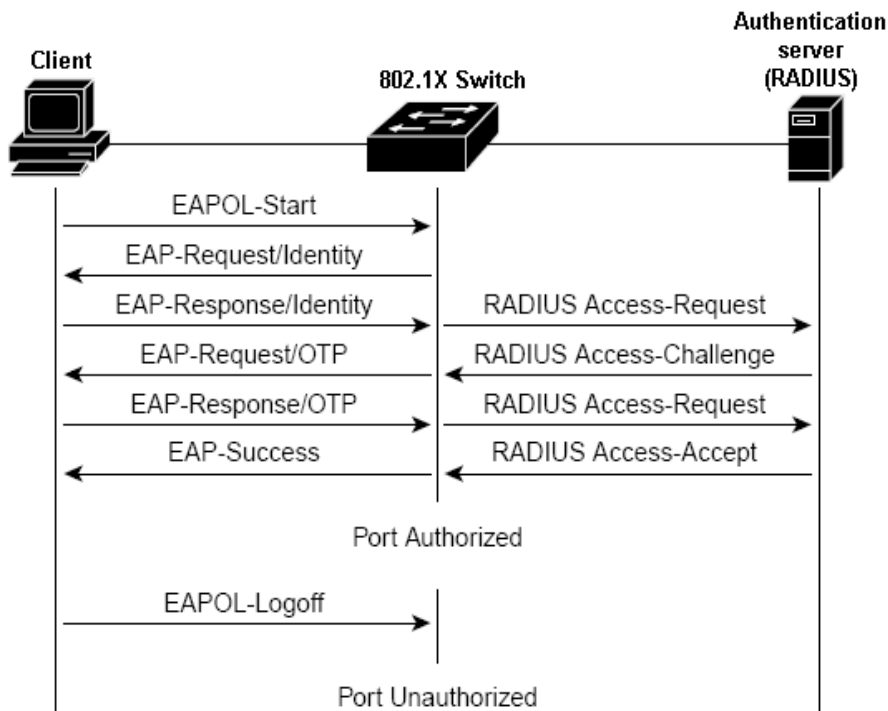
Figure 4-10-2 EAP message exchange

■ **Ports in Authorized and Unauthorized States**

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

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

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

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

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

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

4.10.2 802.1X System Configuration

This page allows you to configure the **IEEE 802.1X** and **MAC-based** authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. A central server, the RADIUS server, determines whether the user is allowed access to the network.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X software installed on his system. The Managed Switch uses the user's MAC address to authenticate against the RADIUS server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

The 802.1X System Configuration screen in Figure 4-10-3 appears.

Figure 4-10-3 802.1X Configuration page screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switchstack. If globally disabled, all ports are allowed forwarding of frames.
• **RADIUS IP**	The IP address of the RADIUS Server expressed in dotted decimal notation. If the RADIUS IP changes while the protocol is globally enabled, then all ports/clients will get reinitialized.
• **RADIUS Secret**	The secret - up to 29 characters long - shared between the RADIUS Server and the switchstack.

• **Reauthentication Enabled**	If checked, clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age Period below).
• **Reauthentication Period**	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
• **EAP Timeout**	Determines the time the switch shall wait for the supplicant response before retransmitting a packet. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.
• **Age Period**	This setting applies to ports running MAC-based authentication, only. Suppose a client is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch that runs MAC-based authentication, and suppose the client gets successfully authenticated. Now assume that the client powers down his PC. What should make the switch forget about the authenticated client? Reauthentication will not solve this problem, since this doesn't require the client to be present, as discussed under Reauthentication Enabled above. The solution is aging of authenticated clients. The Age Period, which can be set to a number between 10 and 1000000 seconds, works like this: A timer is started when the client gets authenticated. After half the age period, the switch starts looking for frames sent by the client. If another half age period elapses and no frames are seen, the client is considered removed from the system, and it will have to authenticate again the next time a frame is seen from it. If, on the other hand, the client transmits a frame before the second half of the age period expires, the switch will consider the client alive, and leave it authenticated, and restart the age timer.
• **Hold Time**	This setting applies to ports running MAC-based authentication, only. If the RADIUS server denies a client access, or a RADIUS server request times out (after 40 seconds with two retries), the client is put on hold in the Unauthorized state. In this state, frames from the client will not cause the switch to attempt to reauthenticate the client. The Hold Time, which can be set to a number between 10 and 1000000 seconds, determines the time after an EAP Failure indication or RADIUS timeout that a client is not allowed access.

4.10.3 802.1X and MAC-Based Authentication Port Configuration

When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

The 802.1X Port Configuration screen in Figure 4-10-4 appears.

Figure 4-10-4 802.1X Port Configuration page screenshot

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Admin State**	Sets the authentication mode to one of the following options (only used when 802.1X or MAC-based authentication is <u>globally enabled</u>): • **Auto:** Requires an 802.1X-aware client (supplicant) to be authorized by the authentication server. Clients that are not 802.1X-aware will be denied access. • **Authorized:** Forces the port to grant access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Success frame when the port links up. • **Unauthorized:** Forces the port to deny access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Failure frame when the port links up. • **MAC-Based:** Enables MAC-based authentication on the port. The switch doesn't transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic against an unsuccessfully authenticated client will be dropped. Clients that are not (yet) successfully authenticated will not be allowed to transmit frames of any kind.
• **Port State**	The current state of the port. It can undertake one of the following values: • **802.1X Disabled:** 802.1X and MAC-based authentication is globally disabled. • **Link Down:** 802.1X or MAC-based authentication is enabled, but there is no link on the port. • **Authorized:** The port is authorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto" and the supplicant is authenticated or the Admin State is "Authorized". • **Unauthorized:** The port is unauthorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto", but the supplicant is not (yet) authenticated or the Admin State is "Unauthorized". • **X Auth/Y Unauth:** X clients are currently authorized and Y are unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to "MAC-Based".
• **Max Clients**	This setting applies to ports running MAC-based authentication, only. The maximum number of clients allowed on a given port can be configured through the list-box and edit-control for this setting. Choosing the value "All" from the list-box allows the port to consume up to 104 client state-machines. Choosing

the value "Specific" from the list-box opens up for entering a specific number of maximum clients on the port (1 to 104).

The stackswitch is "born" with a pool of state-machines, from which all ports draw whenever a new client is seen on the port. When a given port's maximum is reached (both authorized and unauthorized clients count), further new clients are disallowed access. 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 state-machines.

• **Restart**	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is "Auto" or "MAC-Based". Clicking these buttons will not cause settings changed on the page to take effect. • **Reauthenticate:** Schedules a reauthentication to whenever the quiet-period of the port runs out (port-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated ports/clients and will not cause the port/client to get temporarily unauthorized. • **Reinitialize:** Forces a reinitialization of the port/clients and thereby a reauthentication immediately. The port/clients will transfer to the unauthorized state while the reauthentication is ongoing.

4.10.4 802.1X Port Status

This page provides an overview of the current IEEE 802.1X port states for the selected switch. The 802.1X Port Status screen in Figure 4-10-5 appears.

802.1X Status

Port	State	Last Source	Last ID
1	802.1X Disabled		
2	802.1X Disabled		
3	802.1X Disabled		
4	802.1X Disabled		
5	802.1X Disabled		
6	802.1X Disabled		
7	802.1X Disabled		
8	802.1X Disabled		
9	802.1X Disabled		
10	802.1X Disabled		
11	802.1X Disabled		
12	802.1X Disabled		
13	802.1X Disabled		
14	802.1X Disabled		
15	802.1X Disabled		
16	802.1X Disabled		
17	802.1X Disabled		
18	802.1X Disabled		
19	802.1X Disabled		
20	802.1X Disabled		
21	802.1X Disabled		
22	802.1X Disabled		
23	802.1X Disabled		
24	802.1X Disabled		

Auto-refresh ☐ [Refresh]

Figure 4-10-5 802.1X Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number. Click to navigate to detailed 802.1X statistics for this port.
• **State**	The current state of the port. Refer to IEEE 802.1X Port State for a description of the individual states.
• **Last Source**	The source MAC address carried in the most recently received EAPOL frame for port-based authentication, and the most recently received frame from a new client for MAC-based authentication.
• **Last ID**	The user name (supplicant identity) carried in the most recently received Resp/ID

EAPOL frame for port-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

4.10.5 802.1X and MAC-Based Authentication Statistics

This page provides detailed IEEE 802.1X statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows selected RADIUS statistics, only. Use the port select box to select which port details to be displayed. The 802.1X and MAC-Based Authentication Statistics screen in Figure 4-10-6 appears.
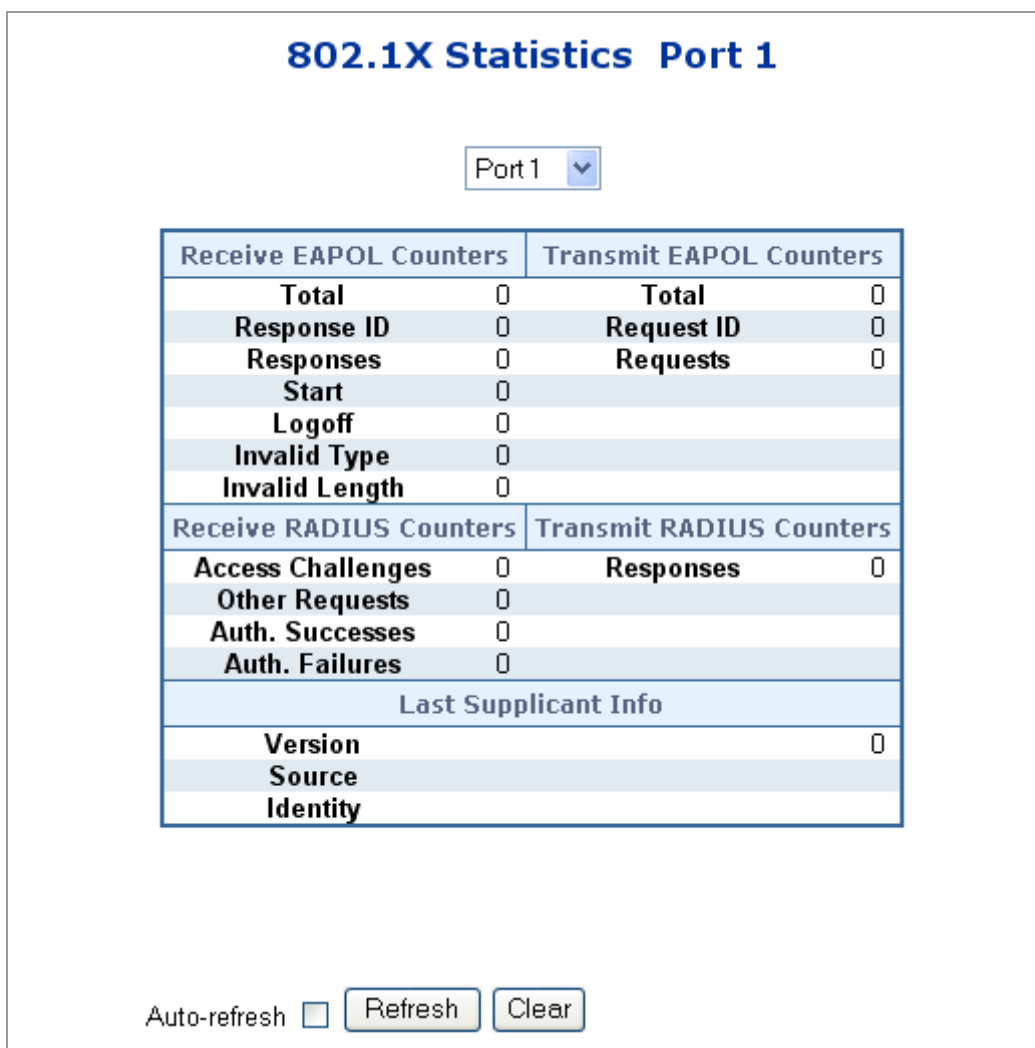
Figure 4-10-6 802.1X Statistics Port 1 page screenshot

The selected port belongs to the currently selected stack unit as reflected by the table header.

■ **EAPOL Counters**

These counters are not available for MAC-based ports.

Supplicant frame counter statistics. There are seven receive frame counters and three transmit frame counters.

EAPOL Counters			
Direction	Name	IEEE Name	Description
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAP Resp/ID frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL logoff frames that have been received by the switch.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAP initial request frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.

■ **RADIUS Counters**

RADIUS Server frame counter statistics.

For MAC-based ports there are two tables containing RADIUS counters. The left-most shows a summary of all RADIUS counters on this port. The right-most shows RADIUS counters for the currently selected client, or dashes if no client is selected or available. A client can be selected from the list of authorized/unauthorized clients below the two counter tables.

There are slight differences in the interpretation of the counters between port- and MAC-based authentication as shown below.

RADIUS Counters			
Direction	**Name**	**IEEE Name**	**Description**
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	**Port-based**: Counts the number of times that the switch receives the first request from the RADIUS server following the first response from the supplicant. Indicates that the RADIUS server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the RADIUS server for this port (left-most table) or client (right-most table).
Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	**Port-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the RADIUS server chose an EAP-method. **MAC-based**: Not applicable.
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	**Port- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the RADIUS server.
Rx	Auth. Failures	dot1xAuthBackendAuthFails	**Port- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the RADIUS server.
Tx	Responses	dot1xAuthBackendResponses	**Port-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the RADIUS server. Indicates the switch attempted communication with the RADIUS server. Possible retransmissions are not counted.

			MAC-based:
			Counts all the RADIUS packets sent from the switch towards the RADIUS server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

■ **Last Supplicant/Client Info**

For MAC-based ports, this section is embedded in the RADIUS counter's section.

Information about the last supplicant/client that attempted to authenticate.

Last Supplicant/Client Info		
Name	**IEEE Name**	**Description**
Version	dot1xAuthLastEapolFrame Version	**Port-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.
Source	dot1xAuthLastEapolFrame Source	**Port-based**: The source MAC address carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.
Identity or (Last) Client	-	**Port-based**: The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame. **MAC-based**: The MAC address of the last client that attempted to authenticate (left-most table), or the MAC address of the currently selected client (right-most table).

■ **Clients attached to this port**

This table is only available for MAC-based ports

Each row in the table represents a MAC-based client on the port, and there are three parameters for each client:

- **MAC Address**: Shows the MAC address of the client, which is also used as the password in theauthentication process against the RADIUS server. Clicking the link causes the client's RADIUS counters to be shown in the right-most RADIUS counters table above. If no clients are attached, it shows *No clients attached*.
- **State**: Shows whether the client is authorized or unauthorized. As long as the RADIUS server hasn't successfully authenticated a client, it is unauthorized.

Last Authentication: Show the date and time of the last authentication of the client. This gets updated for every re-authentication of the client.

4.10.6 Windows Platform RADIUS Server Configuration

1. Setup the RADIUS server and assign the client IP address to the Managed switch. In this case, field in the default IP Address of the Managed Switch with 192.168.0.100. And also make sure the shared secret key is as same as the one you had set at the switch RADIUS server – **12345678** at this case.
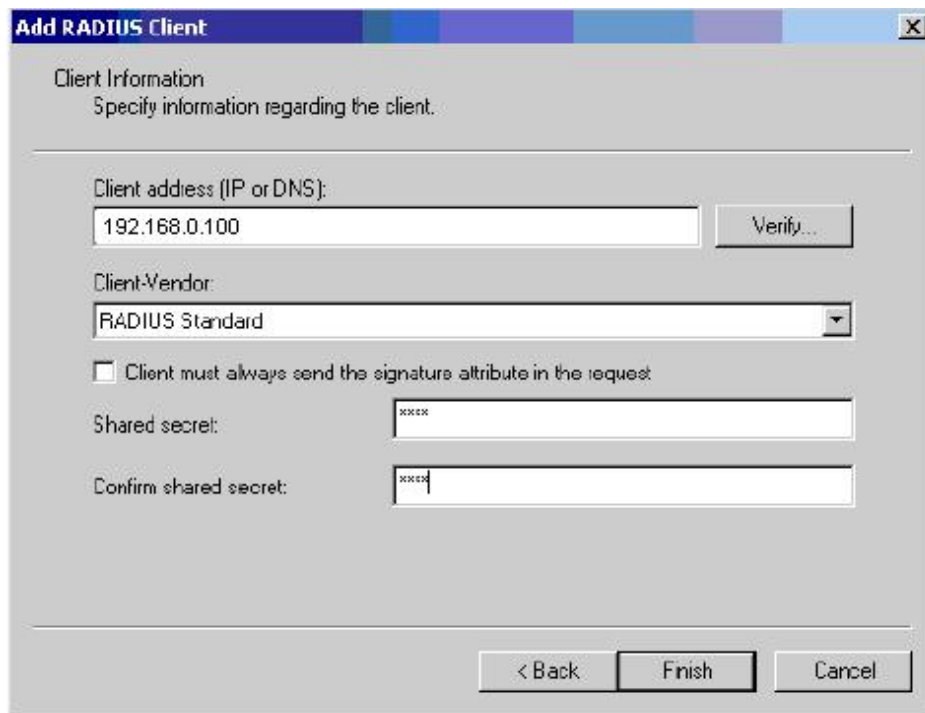
Figure 4-10-7 Windows Server RADIUS Server setting

2. Configure ports attribute of 802.1X, the same as "802.1X Port Configuration".

Figure 4-10-8 802.1x Port Configuration

3. Create user data. That step are different of "**Local Authenticate**", the establishment of the user data needs to be created on the Radius Server PC. For example, the Radius Server founded on Win2000 Server, and then:
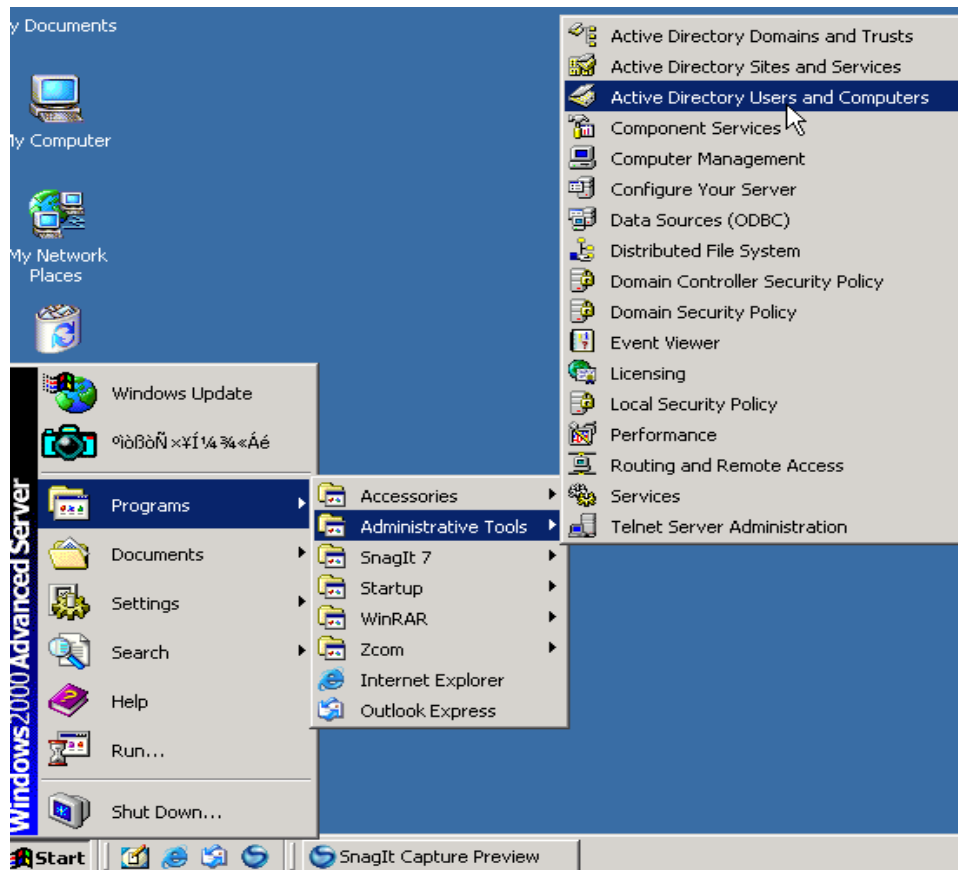
Figure 4-10-9 Windows Server RADIUS Server setting path

5. Enter " **Active Directory Users and Computers**", create legal user data, the next, right-click a user what you created to enter properties, and what to be noticed:
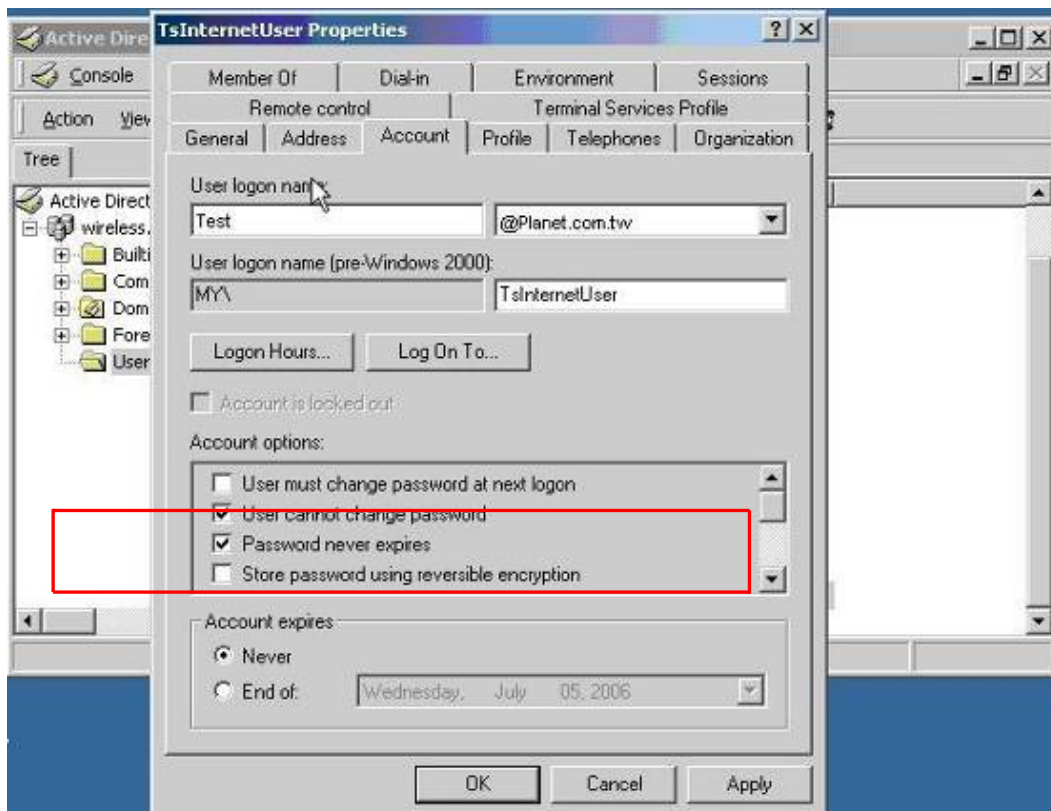
Figure 4-10-10 TsInternetUser Properties screen

159

Set the Ports Authenticate Status to "**Force Authorized**" if the port is connected to the RADIUS server or the port is a uplink port that is connected to another switch. Or once the 802.1X stat to work, the switch might not be able to access the RADIUS server.

4.10.7 802.1X Client Configuration

Windows XP is originally 802.1X support. As to other operating systems (windows 98SE, ME, 2000), an 802.1X client utility is needed. The following procedures show how to configure 802.1X Authentication in Windows XP.

Please note that if you want to change the 802.1x authentication type of a wireless client, i.e. switch to EAP-TLS from EAP-MD5, you must remove the current existing wireless network from your preferred connection first, and add it in again.

■ **Configure Sample: EAP-MD5 Authentication**

1. Go to **Start** > **Control Panel,** double-click on "**Network Connections**".

2. Right-click on the Local Network Connection.

3. Click "**Properties**" to open up the Properties setting window.
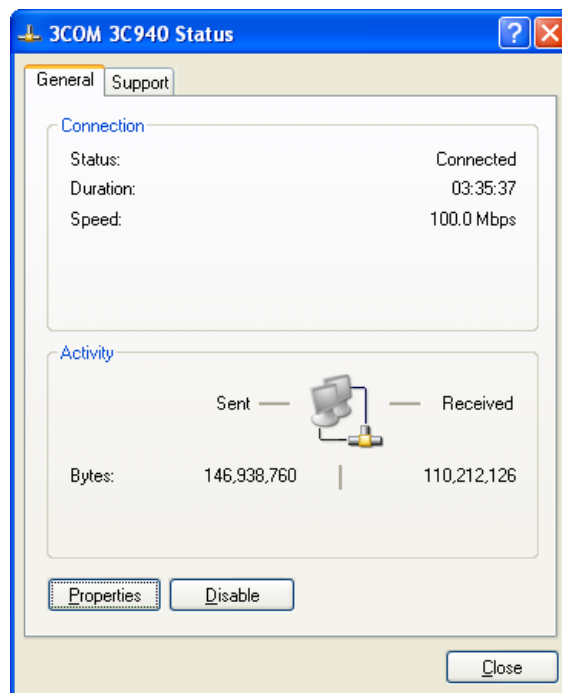
Figure 4-10-11

4. Select "**Authentication**" tab.

5. Select "**Enable network access control using IEEE 802.1X**" to enable 802.1x authentication.

6. Select "**MD-5 Challenge**" from the drop-down list box for EAP type.
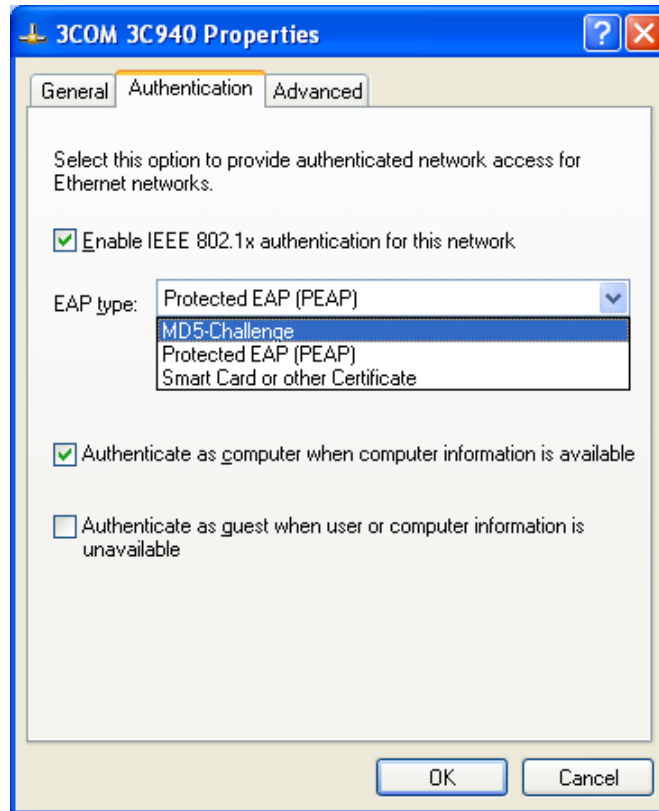
Figure 4-10-12

7. Click "**OK**".

8. When client has associated with the Managed Switch, a user authentication notice appears in system tray. Click on the notice to continue.

Figure 4-10-13

161
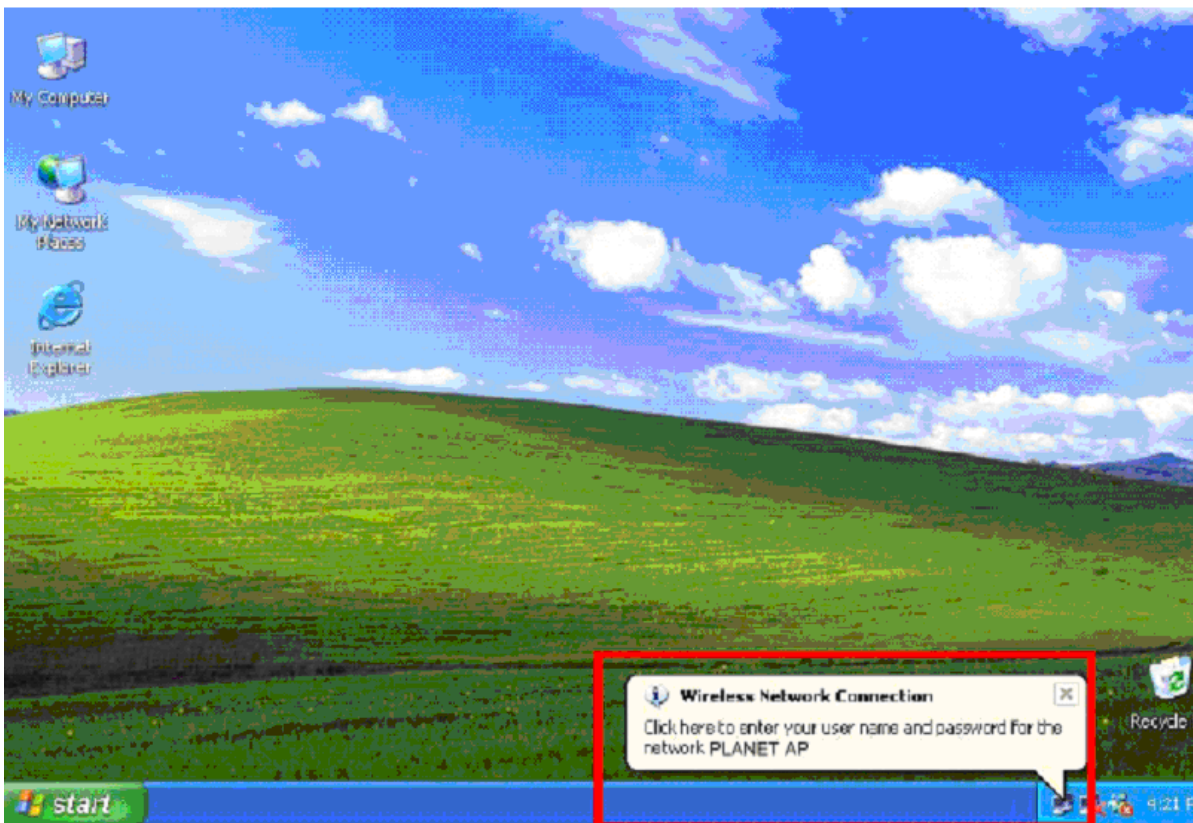
9. Enter the user name, password and the logon domain that your account belongs.

10. Click "**OK**" to complete the validation process.

Figure 4-10-14

162
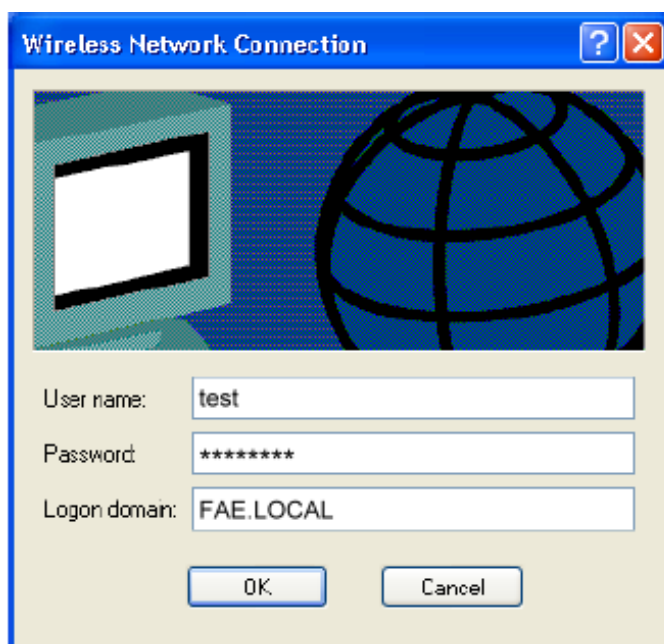
4.11 Access Control Lists

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

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

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

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

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

4.11.1 Access Control List Configuration

This page shows the Access Control List (ACL), which is made up of the ACEs defined for this Managed Switch. Each row describes the ACE that is defined.

■ The maximum number of ACEs is 128.

■ Click on the lowest plus sign to add a new ACE to the list.

The Access Control List Configuration screen in Figure 4-11-1 appears.
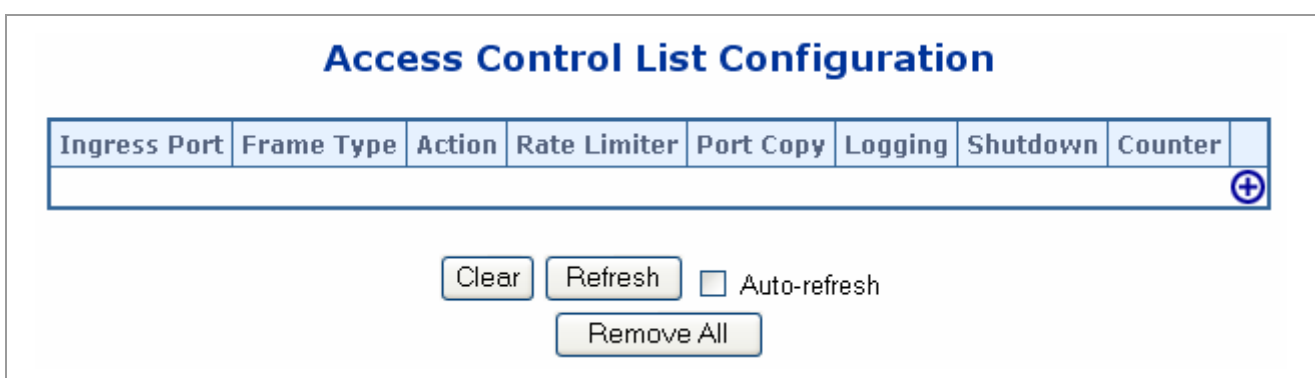
Figure 4-11-1 Access Control List Configuration page screenshot

The page includes the following fields:

Object	Description
● **Ingress Port**	Indicates the ingress port of the ACE. Possible values are: ● **Any:** The ACE will match any ingress port.

		• **Policy**: The ACE will match ingress ports with a specific policy.
		• **Port:** The ACE will match a specific ingress port.
• **Frame Type**		Indicates the frame type of the ACE. Possible values are:
		• **Any:** The ACE will match any frame type.
		• **EType:** The ACE will match Ethernet Type frames.
		• **ARP:** The ACE will match ARP/RARP frames.
		• **IPv4:** The ACE will match all IPv4 frames.
		• **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol.
		• **IPv4/UDP:** The ACE will match IPv4 frames with UDP protocol.
		• I**Pv4/TCP:** The ACE will match IPv4 frames with TCP protocol.
		• **IPv4/Other:** The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
• **Action**		Indicates the forwarding action of the ACE.
		• **Permit:** Frames matching the ACE may be forwarded and learned.
		• **Deny:** Frames matching the ACE are dropped.
• **Rate Limiter**		Indicates the rate limiter number of the ACE. The allowed range is 1 to 15. When Disabled is displayed, the rate limiter operation is disabled.
• **Port Copy**		Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
• **Logging**		Indicates the logging operation of the ACE. Possible values are:
		• **Enabled:** Frames matching the ACE are stored in the System Log.
		• **Disabled:** Frames matching the ACE are not logged.
		Please note that the System Log memory size and logging rate is limited.
• **Shutdown**		Indicates the port shut down operation of the ACE. Possible values are:
		• **Enabled:** If a frame matches the ACE, the ingress port will be disabled.
		• **Disabled:** Port shut down is disabled for the ACE.
• **Counter**		The counter indicates the number of times the ACE was hit by a frame.
• **Modification Buttons**		You can modify each ACE (Access Control Entry) in the table using the following buttons:

You can modify each ACE (Access Control Entry) in the table using the following buttons:

⊕: Inserts a new ACE before the current row.

ⓔ: Edits the ACE row.

⬆: Moves the ACE up the list.

⬇: Moves the ACE down the list.

⊗: Deletes the ACE.

⊕: The lowest plus sign adds a new entry at the bottom of the ACE listings.

4.11.2 ACE Configuration

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type that you selected.

A frame that hits this ACE matches the configuration that is defined here.

Object	Description
• **Ingress Port**	Select the ingress port for which this ACE applies.
	Any: The ACE applies to any port.
	Port n: The ACE applies to this port number, where n is the number of the switch port.
	Policy n: The ACE applies to this policy number, where n can range from 1 through 8.
• **Switch**	Select the switch to which this ACE applies.
	Any: The ACE applies to any port.
	Switch n: The ACE applies to this switch number, where n is the number of the switch.
• **Frame Type**	Select the frame type for this ACE.
	Any: Any frame can match this ACE.
	Ethernet Type: Only Ethernet Type frames can match this ACE.
	ARP: Only ARP frames can match this ACE.
	IPv4: Only IPv4 frames can match this ACE.
• **Action**	Specify the action to take with a frame that hits this ACE.
	Permit: The frame that hits this ACE is granted permission for the ACE operation.
	Deny: The frame that hits this ACE is dropped.
• **Rate Limiter**	Specify the rate limiter in number of base units. The allowed range is 1 to 15. Disabled indicates that the rate limiter operation is disabled.
• **Port Copy**	Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.
• **Logging**	Specify the logging operation of the ACE. The allowed values are:
	Enabled: Frames matching the ACE are stored in the System Log.
	Disabled: Frames matching the ACE are not logged.
	Please note that the System Log memory size and logging rate is limited.
• **Shutdown**	Specify the port shut down operation of the ACE. The allowed values are:
	Enabled: If a frame matches the ACE, the ingress port will be disabled.
	Disabled: Port shut down is disabled for the ACE.
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.

■ **MAC Parameters**

Object	Description
• **SMAC Filter**	(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. Any: No SMAC filter is specified. (SMAC filter status is "don't-care".) Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.
• **SMAC Value**	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.
• **DMAC Filter**	Specify the destination MAC filter for this ACE. **Any**: No DMAC filter is specified. (DMAC filter status is "don't-care".) **MC**: Frame must be multicast. **BC**: Frame must be broadcast. **UC**: Frame must be unicast. **Specific**: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
• **DMAC Value**	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.

■ **VLAN Parameters**

Object	Description
• VLAN ID **Filter**	Specify the VLAN ID filter for this ACE. Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
• **VLAN ID**	When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
• **Tag Priority**	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

■ **ARP Parameters**

The ARP parameters can be configured when Frame Type "ARP" is selected.

Object	Description
• **ARP**/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. • **Any**: No ARP/RARP OP flag is specified. (OP is "don't-care".) • **ARP**: Frame must have ARP/RARP opcode set to ARP. • **RARP**: Frame must have ARP/RARP opcode set to RARP. • **Other**: Frame has unknown ARP/RARP Opcode flag.
• **Request/Reply**	Specify the available ARP/RARP opcode (OP) flag for this ACE. • **Any**: No ARP/RARP OP flag is specified. (OP is "don't-care".) • **Request**: Frame must have ARP Request or RARP Request OP flag set. • **Reply**: Frame must have ARP Reply or RARP Reply OP flag.
• **Sender IP Filter**	Specify the sender IP filter for this ACE. • **Any**: No sender IP filter is specified. (Sender IP filter is "don't-care".) • **Host**: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. • **Network**: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.
• **Sender IP Address**	When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
• **Sender IP Mask**	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
• **Target IP Filter**	Specify the target IP filter for this specific ACE. • **Any**: No target IP filter is specified. (Target IP filter is "don't-care".) • **Host**: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. • **Network**: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.
• **Target IP Address**	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
• **Target IP Mask**	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
• **ARP SMAC Match**	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. **0**: ARP frames where SHA is not equal to the SMAC address. **1**: ARP frames where SHA is equal to the SMAC address. **Any**: Any value is allowed ("don't-care").
• **RARP SMAC Match**	Specify whether frames can hit the action according to their target hardware

	address field (THA) settings.
	0: RARP frames where THA is not equal to the SMAC address.
	1: RARP frames where THA is equal to the SMAC address.
	Any: Any value is allowed ("don't-care").
• **IP/Ethernet Length**	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.
	0: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry.
	1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry.
	Any: Any value is allowed ("don't-care").
• **IP**	Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.
	0: ARP/RARP frames where the HLD is equal to Ethernet (1) must not match this entry.
	1: ARP/RARP frames where the HLD is equal to Ethernet (1) must match this entry.
	Any: Any value is allowed ("don't-care").
• **Ethernet**	Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.
	0: ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry.
	1: ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry.
	Any: Any value is allowed ("don't-care").

■ **IP Parameters**

The IP parameters can be configured when Frame Type "IPv4" is selected.

Object	Description
• **IP Protocol Filter**	Specify the IP protocol filter for this ACE.
	• **Any**: No IP protocol filter is specified ("don't-care").
	• **Specific**: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.
	• **ICMP**: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.
	• **UDP**: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.
	• **TCP**: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining

		TCP parameters will appear. These fields are explained later in this help file.
•	**IP Protocol Value**	When "Specific" is selected for the IP protocol value, you can enter a specific value.. The allowed range is **0** to **255**. A frame that hits this ACE matches this IP protocol value.
•	**IP TTL**	Specify the Time-to-Live settings for this ACE. • **zero**: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. • **non-zero**: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. • **Any**: Any value is allowed ("don't-care").
•	**IP Fragment**	Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. • **No**: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. • **Yes**: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. • **Any**: Any value is allowed ("don't-care").
•	**IP Option**	Specify the options flag setting for this ACE. • **No**: IPv4 frames where the options flag is set must not be able to match this entry. • **Yes**: IPv4 frames where the options flag is set must be able to match this entry. • **Any**: Any value is allowed ("don't-care").
•	**SIP Filter**	Specify the source IP filter for this ACE. • **Any**: No source IP filter is specified. (Source IP filter is "don't-care".) • **Host**: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. • **Network**: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.
•	**SIP Address**	When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
•	**SIP Mask**	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
•	**DIP Filter**	Specify the destination IP filter for this ACE. • **Any**: No destination IP filter is specified. (Destination IP filter is "don't-care".) • **Host**: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. • **Network**: Destination IP filter is set to Network. Specify the destination IP

	address and destination IP mask in the DIP Address and DIP Mask fields that appear.
• **DIP Address**	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
• **DIP Mask**	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

■ **ICMP Parameters**

Object	Description
• **ICMP Type Filter**	Specify the ICMP filter for this ACE. • `Any`: No ICMP filter is specified (ICMP filter status is "don't-care"). • `Specific`: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.
• **ICMP Type Value**	When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is `0` to `255`. A frame that hits this ACE matches this ICMP value.
• **ICMP Code Filter**	Specify the ICMP code filter for this ACE. • `Any`: No ICMP code filter is specified (ICMP code filter status is "don't-care"). • `Specific`: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.
• **ICMP Code Value**	When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is `0` to `255`. A frame that hits this ACE matches this ICMP code value.

■ **TCP/UDP Parameters**

Object	Description
• **TCP/UDP Source Filter**	Specify the TCP/UDP source filter for this ACE. • `Any`: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). • `Specific`: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. • `Range`: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.
• **TCP/UDP Source No.**	When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is `0` to `65535`. A frame that

hits this ACE matches this TCP/UDP source value.

• **TCP/UDP Source Range**	When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is `0` to `65535`. A frame that hits this ACE matches this TCP/UDP source value.
• **TCP/UDP Destination Filter**	Specify the TCP/UDP destination filter for this ACE. • `Any`: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care"). • `Specific`: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. • `Range`: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.
• **TCP/UDP Destination Number**	When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is `0` to `65535`. A frame that hits this ACE matches this TCP/UDP destination value.
• **TCP/UDP Destination Range**	When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is `0` to `65535`. A frame that hits this ACE matches this TCP/UDP destination value.
• **TCP FIN**	Specify the TCP "No more data from sender" (FIN) value for this ACE. • `0`: TCP frames where the FIN field is set must not be able to match this entry. • `1`: TCP frames where the FIN field is set must be able to match this entry. • `Any`: Any value is allowed ("don't-care").
• **TCP SYN**	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. • `0`: TCP frames where the SYN field is set must not be able to match this entry. • `1`: TCP frames where the SYN field is set must be able to match this entry. • `Any`: Any value is allowed ("don't-care").
• **TCP PSH**	Specify the TCP "Push Function" (PSH) value for this ACE. • `0`: TCP frames where the PSH field is set must not be able to match this entry. • `1`: TCP frames where the PSH field is set must be able to match this entry. • `Any`: Any value is allowed ("don't-care").
• **TCP ACK**	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. • `0`: TCP frames where the ACK field is set must not be able to match this entry. • `1`: TCP frames where the ACK field is set must be able to match this entry. • `Any`: Any value is allowed ("don't-care").
• **TCP URG**	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. • `0`: TCP frames where the URG field is set must not be able to match this entry. • `1`: TCP frames where the URG field is set must be able to match this entry. • `Any`: Any value is allowed ("don't-care").

■ **Ethernet Type Parameters**

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

Object	Description
• **EtherType Filter**	Specify the Ethernet type filter for this ACE. `Any`: No EtherType filter is specified (EtherType filter status is "don't-care"). `Specific`: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.
• **Ethernet Type Value**	When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is `0x600` to `0xFFFF`. A frame that hits this ACE matches this EtherType value.

4.11.3 ACL Configuration wizard

This handy wizard helps you set up an ACL quickly.

The ACL Configuration wizard screen in appears.

Figure 4-11-2 welcome to the ACL Configuration wizard page screenshot

The page includes the following fields:

Object	Description
• **Set up Policy Rules**	Set up the default policy rules for Client ports, Server ports, Network ports and Guest ports.
• **Set up Port Policies**	Group ports into several types according to different ACL policies.
• **Set up Typical Network Application Rules**	Set up the specific ACL for different typical network application access control.
• **Set up Source MAC and Source IP Binding**	Strictly control the network traffic by only allowing incoming frames that match the source IP and source MAC on specific port.
• **Set up DoS Attack Detection Rules**	Set up the specific ACL to detect DoS attack.

4.11.3.1 Set up Policy Rules

Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.

Policy 2 for client ports: Limit the allowed rate of broadcast and multicast frames.

Policy 3 for server ports: Common server access only. (DHCP, FTP, Mail, and WEB server)

Policy 4 for network ports: Limit the allowed rate of TCP SYN flooding and ICMP flooding.

Policy 5 for guest ports: Internet access only.

The screen in Figure 4-11-3 appears.
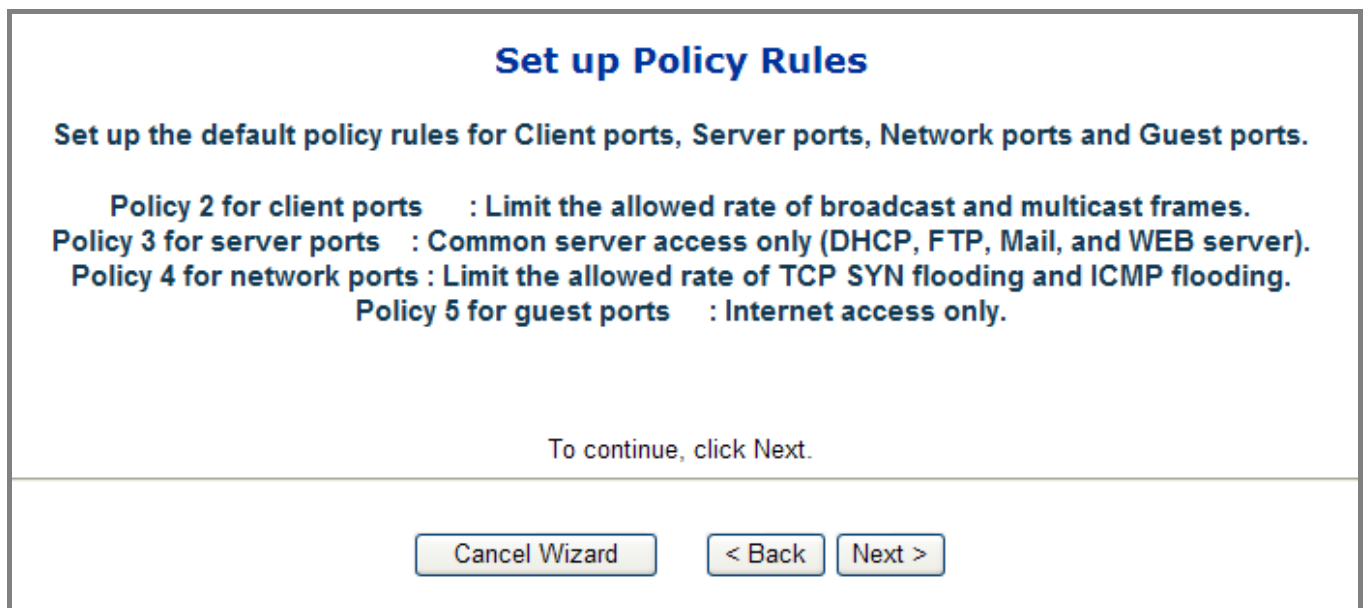
Figure 4-11-3 Set up Policy Rules page screenshot

173

4.11.3.2   Set up Port Policies

Group ports into several types according to different ACL policies.

The settings relate to the currently selected stack unit, as reflected by the page header.

The screen in Figure 4-11-4 appears.
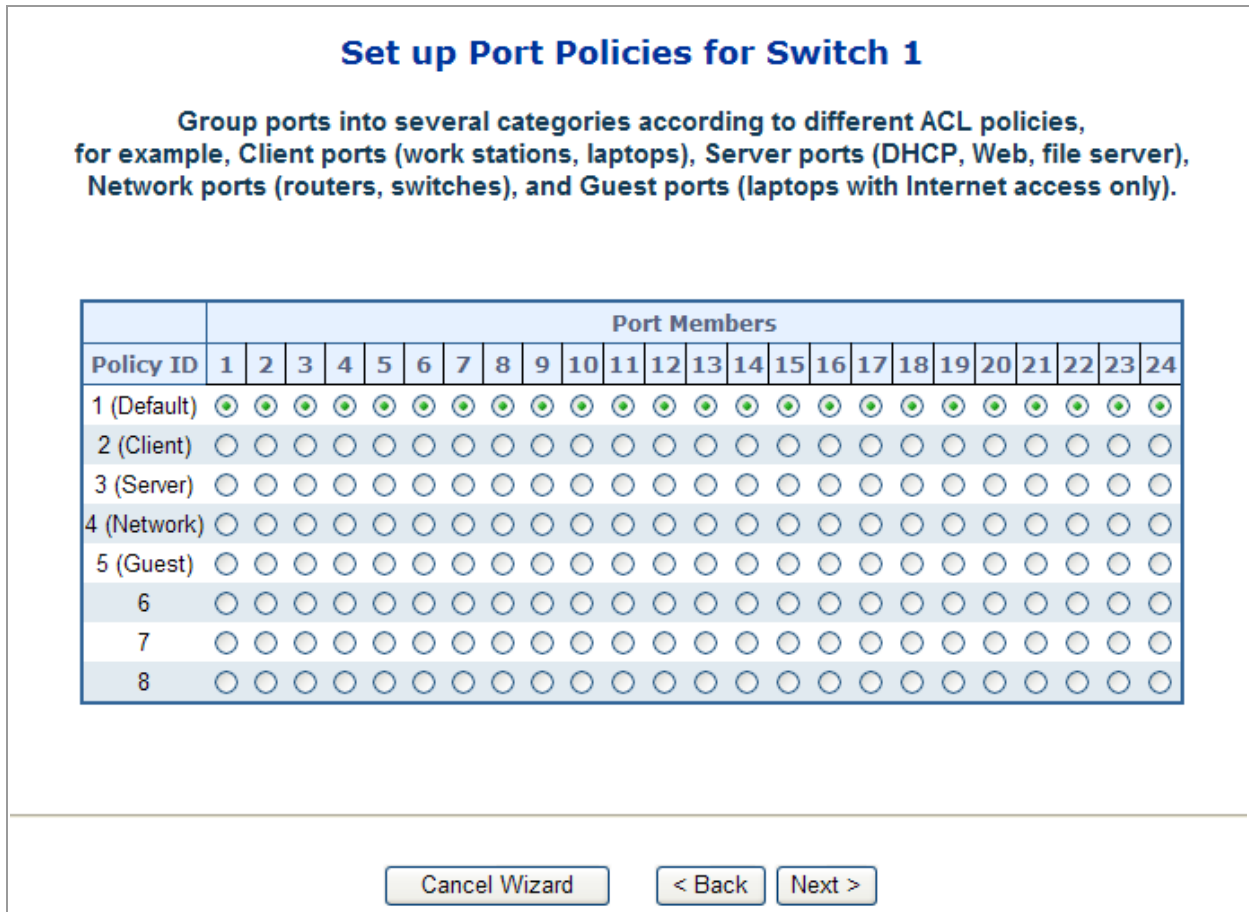
Figure 4-11-4 Set up Port Policies page screenshot

The page includes the following fields:

Object	Description
• **Policy ID**	Frames that hit this ACE are set to match this specific policy.
• **Port Members**	A row of radio buttons for each port is displayed for each Policy ID. To include a port in a policy member, click the radio button.

4.11.3.3 Set up Typical Network Application Rules

Set up the specific ACL for different typical network application access control. The screen in Figure 4-11-5 appears.

■ **STEP-1: Selecting the Network Application Type:**
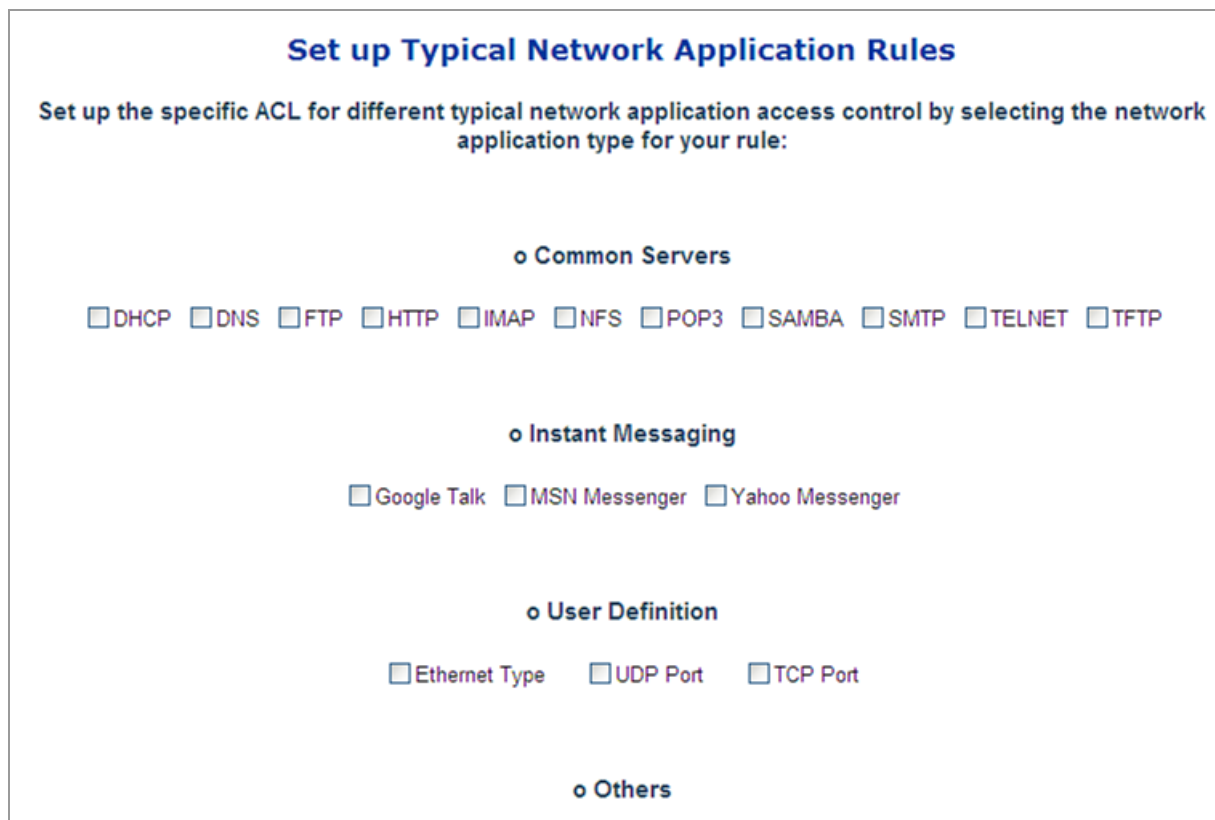
Figure 4-11-5 Set up Typical network Application Rules page screenshot

The page includes the following fields:

Object	Description
• **Common Servers**	Indicates the common servers that applies to the specific ACE. The common servers are: **DHCP**, **DNS**, **FTP**, **HTTP**, **IMAP**, **NFS**, **POP3**, **SAMBA**, **SMTP**, **TELNET**, **TFTP**.
• **Instant Messaging**	Indicates the instant messaging service that applies to the specific ACE. The instant messengers are: **Google Talk**, **MSN Messenger**, **Yahoo Messenger**.
• **User Definition**	Indicates the user definition that applies to the specific ACE. The user definitions are: • **Ethernet Type**: Specify the Ethernet Type filter for this ACE. The allowed range is **0x600** to **0xFFFF**. • **UDP Port**: Specify the UDP destination port filter for this ACE. The allowed range is **0** to **65535**. • **TCP Port**: Specify the TCP destination port filter for this ACE. The allowed

range is **0** to **65535**.

• **Others**	Indicates the other application that applies to the specific ACE. The other applications are: **HTTPS**, **ICMP**, **Multicast IP Stream**, **NetBIOS**, **PING Request**, **Ping Reply**, **SNMP**, **SNMP Traps**.

■ **STEP-2: Define and Apply the Typeical Netowrk Application Rules:**

According to your decision on the previous page, this wizard will create specific ACEs (Access Control Entries) automatically.

First select the ingress port for the ACEs, and then select the action, rate limiter ID, logging and shutdown.

Different parameter options are displayed depending on the frame type that you selected.

The screen in Figure 4-11-6 appears.
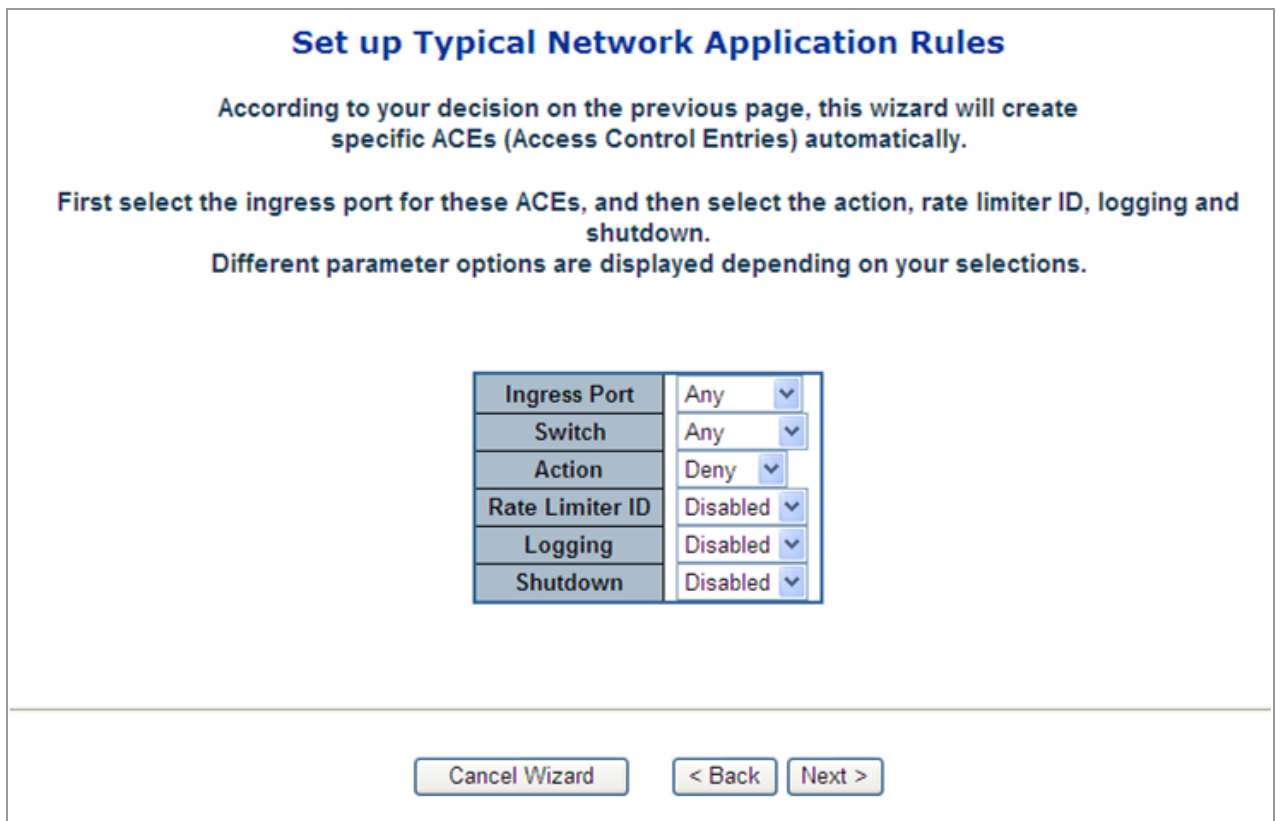
Figure 4-11-6 Set up Typical network Application Rules screenshot

The page includes the following fields:

Object	Description
• **Ingress Port**	Select the ingress port to which this ACE applies. • **Any:** The ACE applies to any port. • **Port n:** The ACE applies to this port number, where *n* is the number of the switch port. • **Policy n:** The ACE applies to this policy number, where n can range from 1

		through 8.
•	**Switch**	Select the switch to which this ACE applies. • **Any:** The ACE applies to any port. • **Switch n:** The ACE applies to this switch number, where n is the number of the switch.
•	**Action**	Specify the action to take with a frame that hits this ACE. • **Permit:** The frame that hits this ACE is granted permission for the ACE operation. • **Deny:** The frame that hits this ACE is dropped.
•	**Rate Limiter**	Specify the rate limiter in number of base units. The allowed range is **1** to **15.** Disabled indicates that the rate limiter operation is disabled.
•	**Logging**	Specify the logging operation of the ACE. The allowed values are: • **Enabled:** Frames matching the ACE are stored in the System Log. • **Disabled:** Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
•	**Shutdown**	Specify the port shut down operation of the ACE. The allowed values are: • **Enabled:** If a frame matches the ACE, the ingress port will be disabled. • **Disabled:** Port shut down is disabled for the ACE.

The ACL configuration wizard is finished, and the new configuration is ready for use.

Figure 4-11-7 Access Control List Configuration page screenshot

4.11.3.4   Set up Source MAC and Source IP Binding

Strictly control the network traffic by only allowing incoming frames that match the source IP and source MAC on specific port.

The settings relate to the currently selected stack unit, as reflected by the page header.

The screen in Figure 4-11-8 appears.

Figure 4-11-8 Set up Source MAC and Secure IP Binding page screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Binding Enabled**	Enable or disable the source IP and source MAC binding status for the given logical port.
• **Source MAC Address**	The source MAC address for the source IP and source MAC binding.
• **Source IP Address**	The source IP address for the source IP and source MAC binding.

The ACL configuration wizard is finished, and the new configuration is ready for use.

Figure 4-11-9

4.11.3.5   Set up DoS Attack Detection Rules

Set up the specific ACL for different typical network application access control.

The screen in Figure 4-11-10 appears.

Figure 4-11-10 Set up DoS Attack Detection Rules page screenshot

The page includes the following fields:

Object	Description
• **UDP DoS - Fraggle**	A malicious attacker sending a large number of UDP packets with random ports to the target system. When the target system receives these packets, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP

	packet of destination unreachable to the spoofed source address. Eventually leading it to be unreachable by other clients and the system will go down.
• **ICMP DoS - Ping of Death**	A malicious attacker sending a malformed ICMP request packet larger than the 65,536 bytes to the target system. Some target systems cannot handle the packet larger than the maximum IP packet size, which often causes target system froze, crashed or rebooted.
• **ICMP DoS - Smurf**	A malicious attacker sending a malformed ICMP request packet with broadcast destination addresses to the target system. After receiving the packet, all reachable hosts send an ICMP echo reply packet back to the spoofed source address. Thus, the target host will suffer from a larger amount of traffic generated.

4.11.3.6 Set up DoS Attack Detection Rules

According to your decision on the previous page, this wizard will create specific ACEs (Access Control Entries) automatically. First select the ingress port for the ACEs, and then select the action, rate limiter ID, logging and shutdown. Different parameter options are displayed depending on the frame type that you selected.
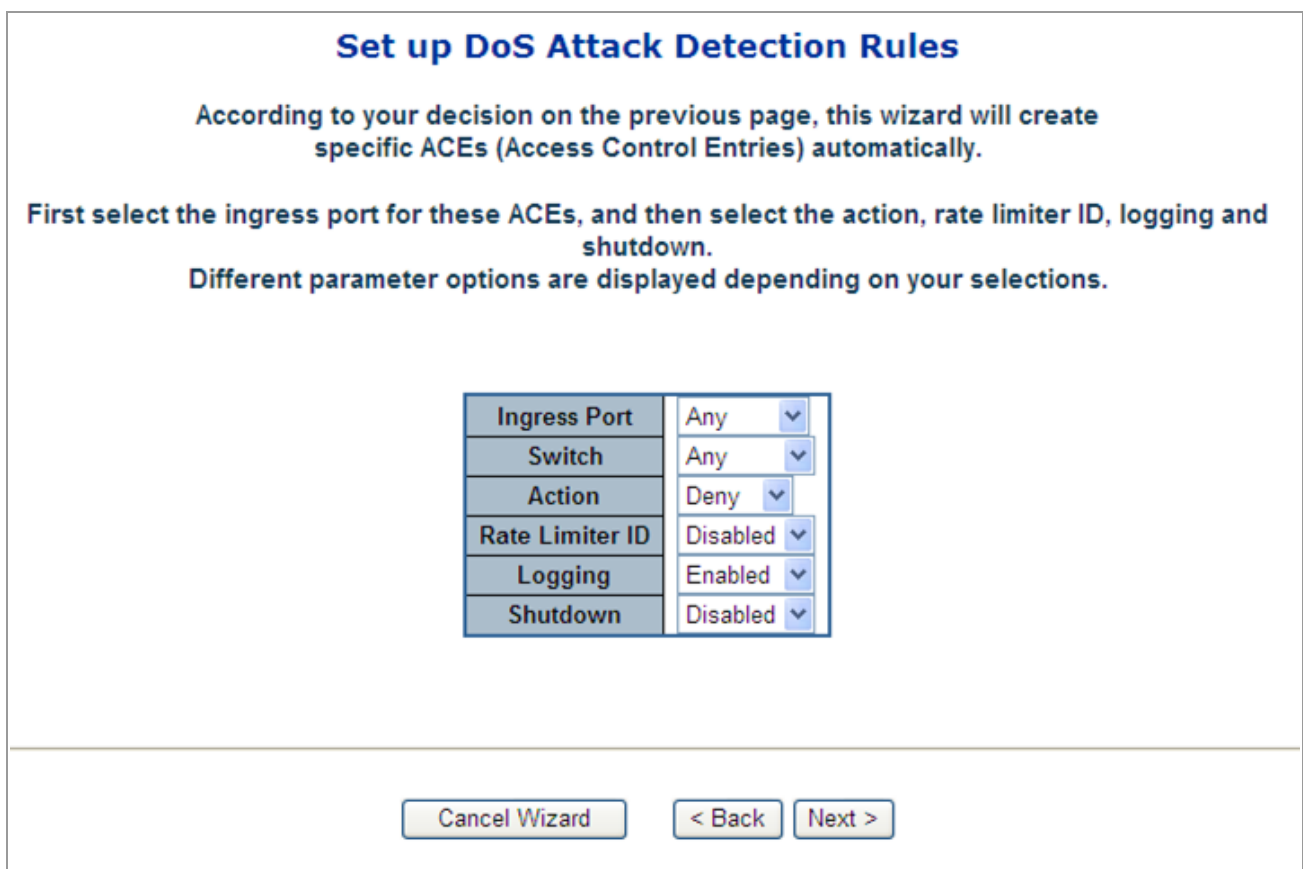
Figure 4-11-11 Set up DoS Attack Detection Rules page screenshot

The page includes the following fields:

Object	Description
• **Ingress Port**	Select the ingress port to which this ACE applies.
	• **Any**: The ACE applies to any port.
	• **Port *n***: The ACE applies to this port number, where *n* is the number of the switch port.
	• **Policy *n***: The ACE applies to this policy number, where *n* can range from 1 through 8.
• **Switch**	Select the switch to which this ACE applies.
	• **Any**: The ACE applies to any port.
	• **Switch *n***: The ACE applies to this switch number, where *n* is the number of the switch.
• **Action**	Specify the action to take with a frame that hits this ACE.
	• **Permit**: The frame that hits this ACE is granted permission for the ACE operation.
	• **Deny**: The frame that hits this ACE is dropped.
• **Rate Limiter**	Specify the rate limiter in number of base units. The allowed range is **1** to **15**. **Disabled** indicates that the rate limiter operation is disabled.
• **Logging**	Specify the logging operation of the ACE. The allowed values are:
	• **Enabled**: Frames matching the ACE are stored in the System Log.
	• **Disabled**: Frames matching the ACE are not logged.
• **Shutdown**	Specify the port shut down operation of the ACE. The allowed values are:
	• **Enabled**: If a frame matches the ACE, the ingress port will be disabled.
	• **Disabled**: Port shut down is disabled for the ACE.

Note   Please note that the System Log memory size and logging rate is limited.

The ACL configuration wizard is finished, and the new configuration is ready for use.

Figure 4-11-12

181

4.11.4 ACL Rate Limiter Configuration

Configure the rate limiter for the ACL of the switch.

The ACL Rate Limiter Configuration screen in Figure 4-11-13 appears.
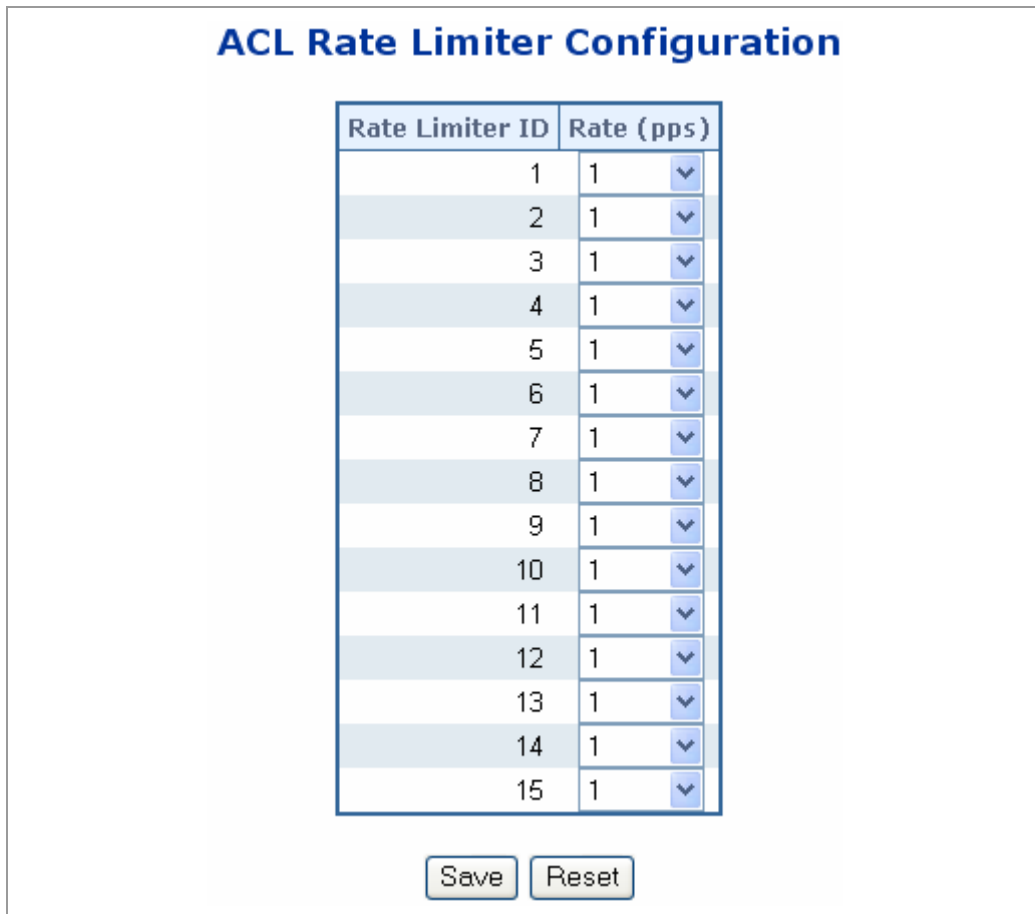
Figure 4-11-13 ACL Rate Limiter Configuration page screenshot

The page includes the following fields:

Object	Description
• **Rate Limiter ID**	The rate limiter ID for the settings contained in the same row.
• **Rate**	The rate unit is packet per second (pps), configure the rate as **1**, **2**, **4**, **8**, **16**, **32**, **64**, **128**, **256**, **512**, **1K**, **2K**, **4K**, **8K**, **16K**, **32K**, **64K**, **128K**, **256K**, **512K**, or **1024K**. The 1 kpps is actually 1002.1 pps.

4.11.5 ACL Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE. The settings relate to the currently selected stack unit, as reflected by the page header. The ACL Ports Configuration screen in Figure 4-11-14 appears.

Figure 4-11-14 ACL Ports Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.

• **Policy ID**	Select the policy to apply to this port. The allowed values are `1` through `8`. The default value is 1.
• **Action**	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
• **Rate Limiter ID**	Select which rate limiter to apply to this port. The allowed values are `Disabled` or the values `1` through `15`. The default value is "Disabled".
• **Port Copy**	Select which port frames are copied to. The allowed values are `Disabled` or a specific port number. The default value is "Disabled".
• **Logging**	Specify the logging operation of this port. The allowed values are: • **Enabled**: Frames received on the port are stored in the System Log. • **Disabled**: Frames received on the port are not logged. The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.
• **Shutdown**	Specify the port shut down operation of this port. The allowed values are: `Enabled`: If a frame is received on the port, the port will be disabled. `Disabled`: Port shut down is disabled. The default value is "Disabled".
• **Counter**	Counts the number of frames that match this ACE.

4.12 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 have been seen after a configurable age time.

4.12.1 MAC Address Table Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here. The MAC Address Table Configuration screen in Figure 4-12-1 appears.

Figure 4-12-1 MAC Address Table Configuration page screenshot

Aging Configuration

Object	Description
• **Disable Automatic Aging**	Enables/disables the the automatic aging of dynamic entries
• **Aging Time**	The time after which a learned entry is discarded. By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging. (Range: 10-10000000 seconds; Default: 300 seconds)

4.12.2 Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

The Static MAC Table Configuration screen in Figure 4-12-2 appears.

Figure 4-12-2 Static MAC Table Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **VLAN ID**	The VLAN ID for the entry.
• **MAC Address**	The MAC address for the entry.
• **Port Members**	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
• **Adding a New Static Entry**	Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

4.12.3 MAC Address Table Status

Dynamic MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to **8192** entries, and is sorted first by VLAN ID, then by MAC address.

Figure 4-12-3 MAC Address Table Status

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "**entries per page**" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "**Start from MAC address**" and "**VLAN**" input fields allow the user to select the starting point in the MAC Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next MAC Table match.

In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The "**>>**" will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table. Use the "**|<<**"button to start over.

MAC Table Columns

Object	Description
• **Type**	Indicates whether the entry is a static or dynamic entry.
• **VLAN**	The VLAN ID of the entry.
• **MAC address**	The MAC address of the entry.
• **Port Members**	The ports that are members of the entry.

Buttons

Auto-refresh ☐ : Check this box to enable an automatic refresh of the page at regular intervals.

Refreshe: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

Clear : Flushes all dynamic entries.

|<<: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

>>|: Updates the table, starting with the entry after the last entry currently displayed.

4.13 Port Security (To be Continued)

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the Managed Switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

<source MAC address, VLAN> pair for frames received on the port.

Note that you can also manually add secure addresses to the port using the **Static Address Table**. The selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.

MAC Table Learning
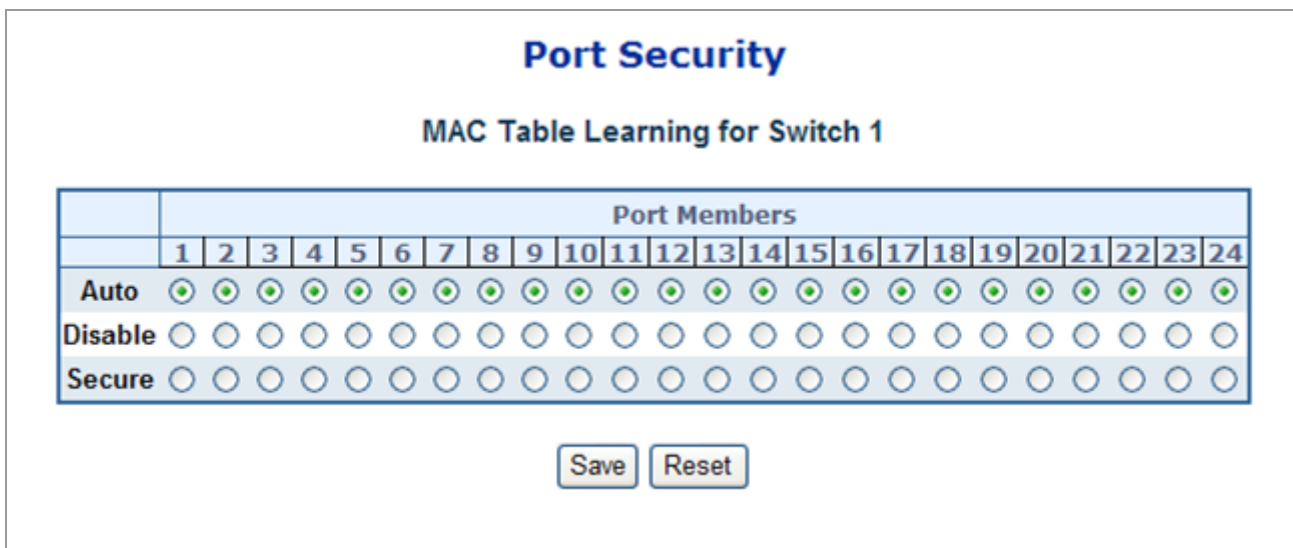
Figure 4-13-1 Port Security Settings screenshot

The page includes the following fields:

Object	Description
• **Auto**	Learning is done automatically as soon as a frame with unknown SMAC is received.
• **Disable**	No learning is done.
• **Secure**	Only static MAC entries are learned, all other frames are dropped.

	Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.
Note	

4.14 LLDP

4.14.1 Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in **Type Length Value (TLV)** format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

4.14.2 LLDP Configuration

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Configuration screen in Figure 4-14-1 appears.

Figure 4-14-1 LLDP Configuration page screenshot

■ **LLDP Parameters**

Object	Description
• **Tx Interval**	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds. Default: **30** seconds

	This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)
• **Tx Hold**	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
• **Tx Delay**	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval
• **Tx Reinit**	When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

■ **4.14.2.2 LLDP Port Configuration**

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.

Object	Description
• **Port**	The switch port number of the logical LLDP port.
• **Mode**	Select LLDP mode. • **Rx only** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. • **Tx only** The switch will drop LLDP information received from neighbors, but will send out LLDP information. • **Disabled** The switch will not send out LLDP information, and will drop LLDP information received from neighbors. • **Enabled** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

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

4.14.3 LLDP Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an

LLDP neighbor is detected. The LLDP Neighbor screen in appears.

Figure 4-14-3 LLDP Neighbor Information page screenshot

The columns hold the following information:

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

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

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

4.14.4 LLDP Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refers to counters for the currently selected switch. The LLDP Statistics screen in Figure 4-14-4 appears.

Global Counters	
Neighbor entries were last changed at	- (5369 sec. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

Auto-refresh ☐ [Refresh] [Clear]

LLDP Statistics

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0

Figure 4-14-4 LLDP Statistics page screenshot

■ **Global Counters**

Object	Description
• **Neighbor entries were last changed at**	Shows the time for when the last entry was last deleted or added. It is also shows the time elapsed since last change was detected.
• **Total Neighbors Entries Added**	Shows the number of new entries added since switch reboot.
• **Total Neighbors Entries Deleted**	Shows the number of new entries deleted since switch reboot.

• **Total Neighbors Entries Dropped**	Shows the number of LLDP frames dropped due to that the entry table was full.
• **Total Neighbors Entries Aged Out**	Shows the number of entries deleted due to Time-To-Live expiring.

■   **Local Counters**

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

Object	Description
• **Local Port**	The port on which LLDP frames are received or transmitted.
• **Tx Frames**	The number of LLDP frames transmitted on the port.
• **Rx Frames**	The number of LLDP frames received on the port.
• **Rx Errors**	The number of received LLDP frames containing some kind of error.
• **Frames Discarded**	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
• **TLVs Discarded**	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
• **TLVs Unrecognized**	The number of well-formed TLVs, but with an unknown type value.
• **Org. Discarded**	The number of organizationally TLVs received.
• **Age-Outs**	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.

4.15 Network Diagnastics

4.15.1 Cable Diagnostics

This page is used for running the Cable Diagnostics.

Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running cable diagnostic. Therefore, running cable diagnastic on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete. The ports belong to the currently selected stack unit, as reflected by the page header.

Cable Diagnostics for Switch 1

Port [6 ∨]

[Start]

Cable Status

Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	OK	4	OK	4	OK	4	OK	4
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--
9	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--
11	--	--	--	--	--	--	--	--
12	--	--	--	--	--	--	--	--
13	--	--	--	--	--	--	--	--
14	--	--	--	--	--	--	--	--
15	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--
17	--	--	--	--	--	--	--	--
18	--	--	--	--	--	--	--	--
19	--	--	--	--	--	--	--	--
20	--	--	--	--	--	--	--	--
21	--	--	--	--	--	--	--	--
22	--	--	--	--	--	--	--	--
23	--	--	--	--	--	--	--	--
24	--	--	--	--	--	--	--	--

Figure 4-15-1 Cable Diagnostics page screenshot

Object	Description
• **Port**	The port where you are requesting Cable Diagnostics.
• **Cable Status**	**Port**: Port number. **Pair**: The status of the cable pair. **Length**: The length (in meters) of the cable pair.

4.15.2 Ping

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

After you press , 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-15-1 appears.
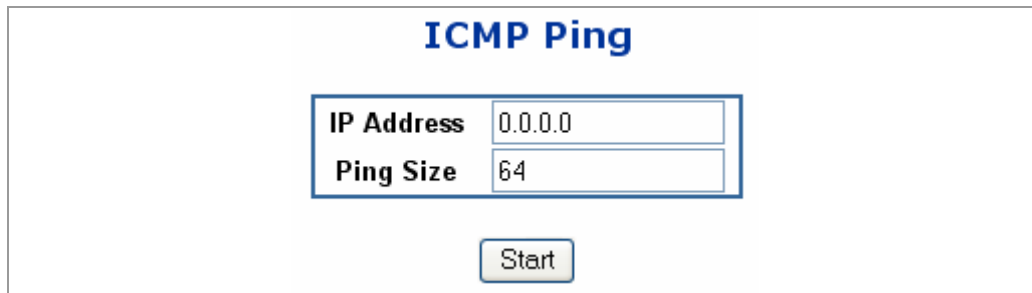
Figure 4-15-1 ICMP Ping page screenshot
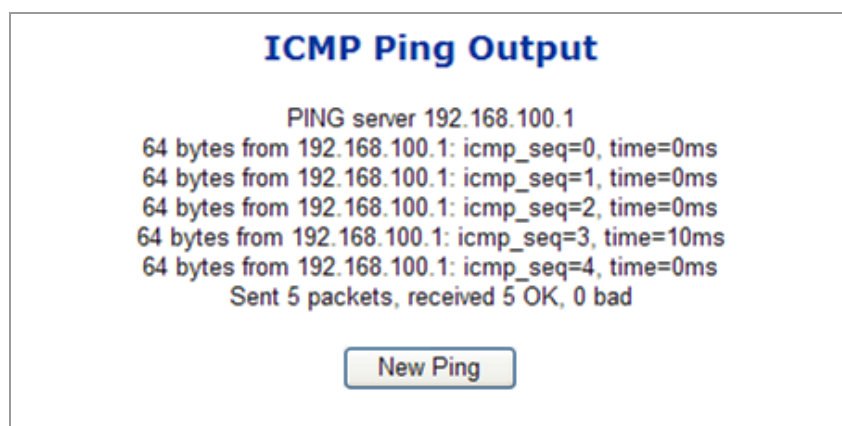
The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address.
• **Ping Size**	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

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

After field the parameter and press "**Start**" to execute the Ping function. The Ping result shows at the next tabl

4.16 Stacking – SGSW-24040 / SGSW-24040R

Using Stacking, it is possible to connect a number of switches together in a stack, which behaves as a single switch as seen from outside the stack.

Two types of stack topologies are supported:

- **Ring topology**
- **Chain topology (same as a disconnected ring)**

Multiple PLANET SGSW-24040 / SGSW-24040R devices may be connected together to constitute a ring or chain stack topology using the STX / 5Gbps ports as interconnect links. Dedicated stacking features built into SGSW-24040 / SGSW-24040R makes all devices in the stack operate together as a single, much larger switch. Among the stacking features are:

- Hardware controlled stack wide learning and continuous automatic MAC table synchronization
- Shortest path forwarding, providing low latency and optimal use of stacking link bandwidth
- QoS consistency across stack
- Single point of management for simple stack administration
- Low Cost and Flexible HDMI-like Stacking cables
- Real Plug and Play connectivity
-

The following figure shows an example with five devices in a ring topology stack. Each device in the stack is, in a stack context, called a unit. The ports connecting the units are called stack ports, and the ports connecting to external hosts and switches are called front ports.

■ **Chain Stack:** A chain of switches, that is, no redundant forwarding paths.

Figure 4-16-1 Chain Stack topology

■ **Ring Stack:** A ring of switches, thereby providing redundant forwarding paths.
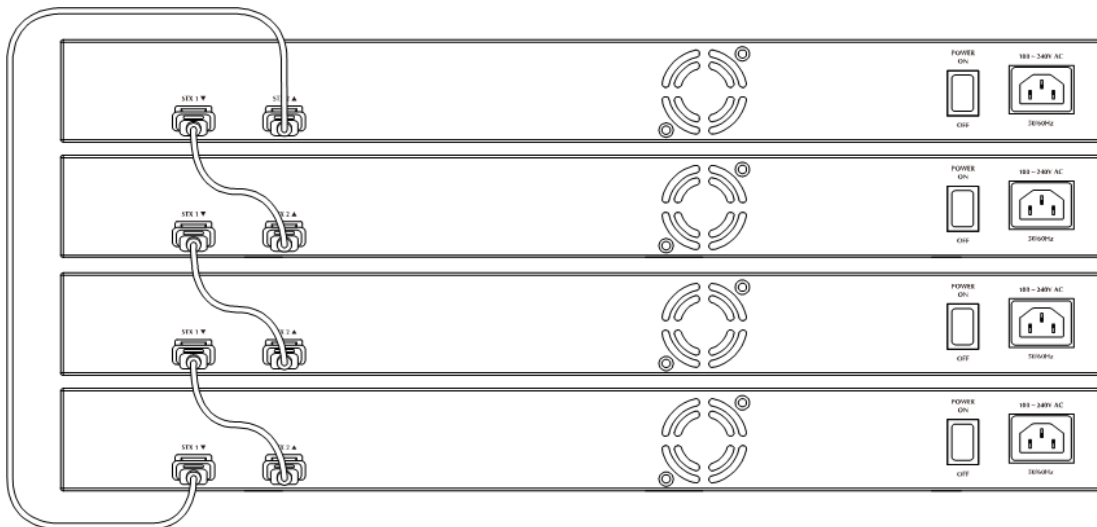
Figure 4-16-2 Ring Stack topology

■ **Back-to-Back Stack** : Two switches interconnected on both stacking ports.
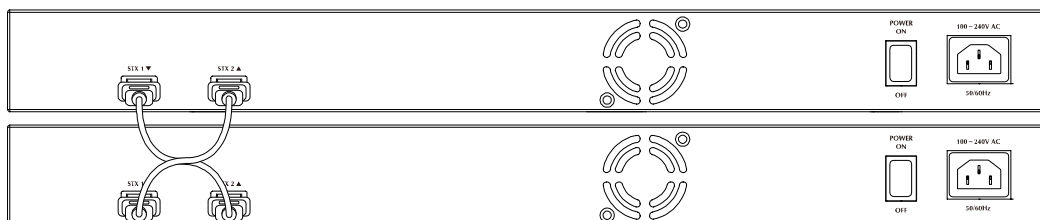
Figure 4-16-3 Back to back Stack topology

4.16.1 Stack

This section provides information for understand stacking architecture, include the below items:

- **Switch IDs**
  - **Assigning and Swapping Switch IDs**
  - **Removing a Switch From the Stack**
  - **Replacing a Switch**
  - **General Switch ID Assignment Rules**
- **Master Election**
- **Stack Redundancy**
- **Shortest Path Forwarding**

4.16.1.1 Switch IDs

The Switch ID (1-16) assigned to a SGSW Switch.

■ Assigning and Swapping Switch IDs

When a switch is added to the stack, a Switch ID is automatically assigned to the switch. The automatic SID assignment can be modified by choosing a different Switch ID on the Stack Configuration page. This method allows Switch IDs to be assigned so that it is easier for the user to remember the ID of each switch.

The Switch IDs of two switches can be swapped by simply interchanging the values in the Switch ID column.

Note	**Changing Switch IDs does not result in any interruption of the stack operation.**

■ Removing a Switch From the Stack

When a switch is removed from the stack, the configuration for the switch is preserved, and the switch still appears on the Stack Configuration page. If the configuration of the switch is not to be transferred to another switch, then the configuration may be deleted by choosing Delete, followed by "Save".

■ Replacing a Switch

If a switch is to be replaced with another switch (for example, replacing failing hardware), the following procedure must be used to assign the configuration of the failing switch to the new hardware:

1. Remove the failing switch from the stack. For example, assume that the failing switch had Switch ID 3.
2. Insert the new switch into the stack. The new switch is assigned an unused Switch ID.
3. To remove the automatic switch ID assignment, choose "Delete", followed by "Save". The new switch is then shown with Switch ID set to "-".
4. To assign the configuration of Switch ID 3 to the new hardware, simply choose 3 in the Switch ID column and click

"Save".

5. The new hardware has now taken over the configuration of the failing hardware.

■ **General Switch ID Assignment Rules**

When assigning Switch IDs to the devices in the stack, you must note the following:

1. Switches with assigned IDs can be changed to use any other switch ID (possibly by swapping Switch ID with another active switch).

2. When swapping two Switch IDs, the devices will retain their (own) configuration, except for the Switch ID.

3. Switches without an assigned Switch ID can only be assigned to any unused ID.

4. When assigning a Switch ID of an inactive switch to a new switch, the new switch will inherit the former's configuration (see "Replacing a Switch" above).

5. Deleting a switch will remove any configuration pertaining to it.

6. Deleting an active switch will leave it with an unassigned Switch ID until rebooted or manually assigning a Switch ID.

4.16.1.2 Master Election

Within a managed stack, one master switch (or just "**master**") must be elected. Any switch not being master is a slave switch (or just "**slave**").

To elect a master, the following criteria are evaluated sequentially:

1. If any switch already claims to have been master for more than 30 seconds, then that switch will become master.

2. If multiple switches claim to have been master for more than 30 seconds, then the switch which has been master for the longest period of time will become master.

3. The switch with the **smallest master priority**.

4. The switch with the **smallest MAC address**.

The above algorithm ensures that once a master has been elected and has been master for more than 30 seconds, it will remain master. However in some cases the user may want to enforce a new master election.

4.16.1.3 Stack Redundancy

In the unlikely event that a SGSW Switch fails in a stack, stack integrity is maintained if the redundant cable is connected to the stack. The affected switch within the sack can be replaced or removed without disrupting normal operation. The broken link is bypassed and data transmission continues uninterrupted. The single management IP address for the stack is also preserved for uninterrupted management and monitoring.
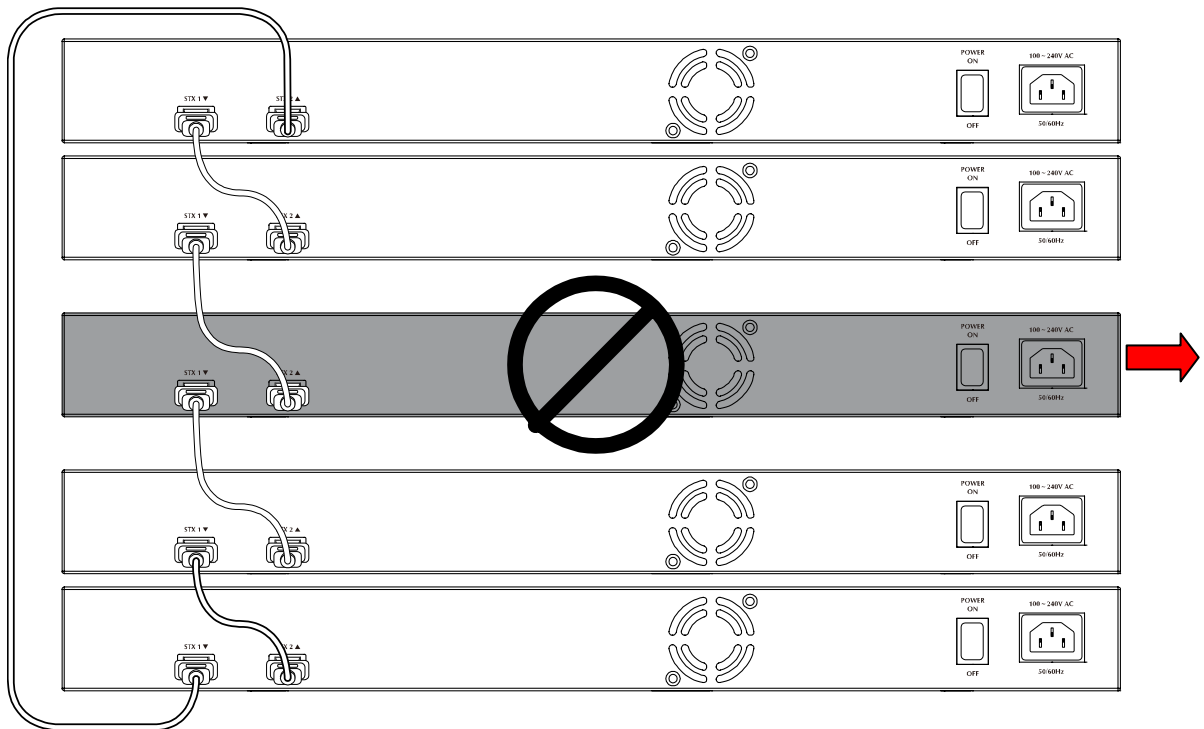
Figure 4-16-4 Remove or Replace a switch from the stack

4.16.1.4 Shortest Path Forwarding

The SGSW Swtich supports shortest path forwarding technology to optimal data flow across the stack. The advantage of shortest path forwarding as below:

■   **Automatic Loop Prevention** – Using Time To Live (TTL) information in the stack-header
■   **Utilize all stack links in the ring**.
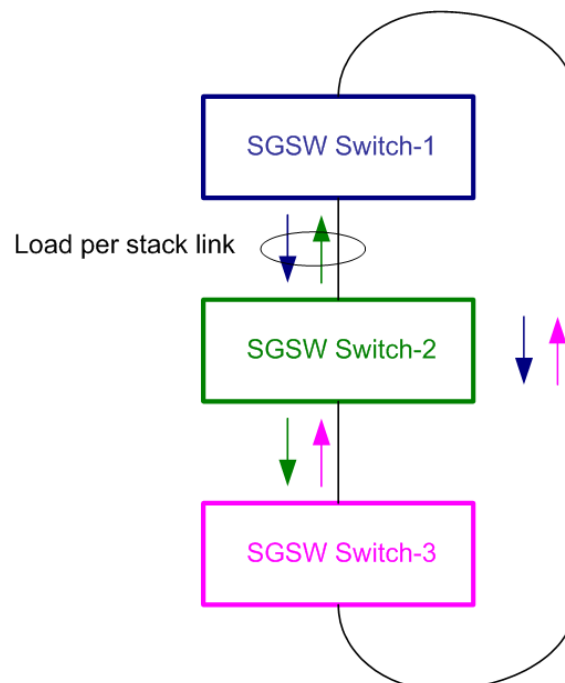
Figure 4-16-5 True Ring Topology

204

4.16.2 Stack Configuration

This page is used for configure the stack, include assign Switch ID, master priority and display the current stack member information. The screen in Figure 4-16-6appears.

Figure 4-16-6 Stack Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Deletes this switch from the stack configuration.
• **Stack Member**	The MAC address of the switch.
• **Switch ID**	The Switch ID (1-16) assigned to a switch. For more information, see description of Switch IDs
• **Master Capable**	Indicates whether a switch is capable of being master. An unmanaged switch, for example, will not be Master Capable.
• **Master Priority**	The priority that the switch has in the master election process. The smaller the priority, the more likely the switch will become master during the master election process.
• **Switch Type**	The product name of the switch.
• **Start Master Election**	By checking this option, the "Save" operation will also start the master election process. This is done by clicking "**Start Master Election**", followed by "Save". This causes the first two criteria to be ignored, thereby basing master election only on master priority and MAC address. When master election is enforced, the first two criteria are ignored for a period of 10-15 seconds.

On the Stack State Monitor web page, this is shown by "**Reelect**" being set to "Yes" for one of the switches in the stack.

4.16.3 Stack Information

This page provides an overview of the stack topology, as detected by SPROUT.

■ **Stack Topology**

The Stack Topology screen in Figure 4-16-7 appears.
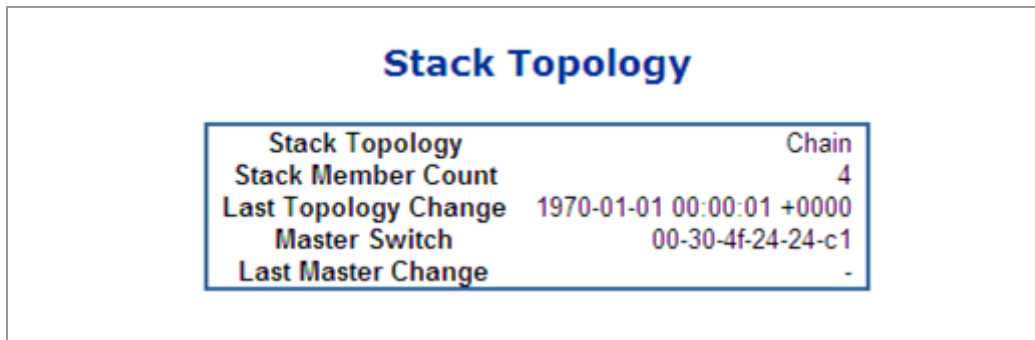
Figure 4-16-7 Stack Information page screenshot - Stack Topology

The page includes the following fields:

Object	Description
• **Stack Topology**	Specifies the type of topology for the stack: • **Chain**: A chain of switches, that is, no redundant forwarding paths. • **Ring**: A ring of switches, thereby providing redundant forwarding paths. • **Back-to-Back**: Two switches interconnected on both stacking ports.
• **Stack Member Count**	The number of switches in the stack.
• **Last Topology Change**	The time of the last topology change in the stack.
• **Master Switch**	The MAC address of the current stack master switch.
• **Last Master Change**	The time of the last master change in the stack.

■ **Stack List**

For each switch in the stack, the following information is shown: The **MAC address**, **Switch ID**, **product name** and **version**, and master election state. The master election state is normally "No". Only when a forced master election is enforced by the user, the master election state takes the value "Yes". For details about the master election algorithm, see Stack Configuration. The Stack List screen in Figure 4-16-8 appears.

Figure 4-16-8 Stack Information page screenshot - Stack List

The page includes the following fields:

Object	Description
• **Delete**	Deletes this switch from the stack configuration.
• **Stack Member**	The MAC address of the switch.
• **Switch ID**	The Switch ID (1-16) assigned to a switch. For more information, see description of Switch IDs
• **Master Capable**	Indicates whether a switch is capable of being master. An unmanaged switch, for example, will not be Master Capable.
• **Master Priority**	The priority that the switch has in the master election process. The smaller the priority, the more likely the switch will become master during the master election process.
• **Switch Type**	The product name of the switch.
• **Start Master Election**	By checking this option, the "Save" operation will also start the master election process. This is done by clicking "**Start Master Election**", followed by "Save". This causes the first two criteria to be ignored, thereby basing master election only on master priority and MAC address. When master election is enforced, the first two criteria are ignored for a period of 10-15 seconds.

■   **Master Forwarding Table**

As the heading suggests, the information in the table is as seen from the master view.

For each switch in the stack, the following information is shown:

- The MAC address, switch ID, distance information, and the primary forwarding path to the switch.

- For ring topology, a backup path is also provided.

Master Forwarding Table

Stack Member	Switch ID	Distance		Forwarding	
		Port 25	Port 26	Port 25	Port 26
00-30-4f-24-24-c1	1	0	0	Local	Local
00-30-4f-24-04-01	2	2	-	Primary	-
00-30-4f-24-04-76	3	3	-	Primary	-
00-30-4f-24-04-a1	4	1	-	Primary	-

Auto-refresh ☐ Refresh

Figure 4-16-9 Stack Information page screenshot - Master Forwarding Table

4.16.4 Stack Port State Ovewview

This page provides an overview of the current switch port states. Clicking on the image of a port opens the **Port Statistics** page.The port states are illustrated as follows:
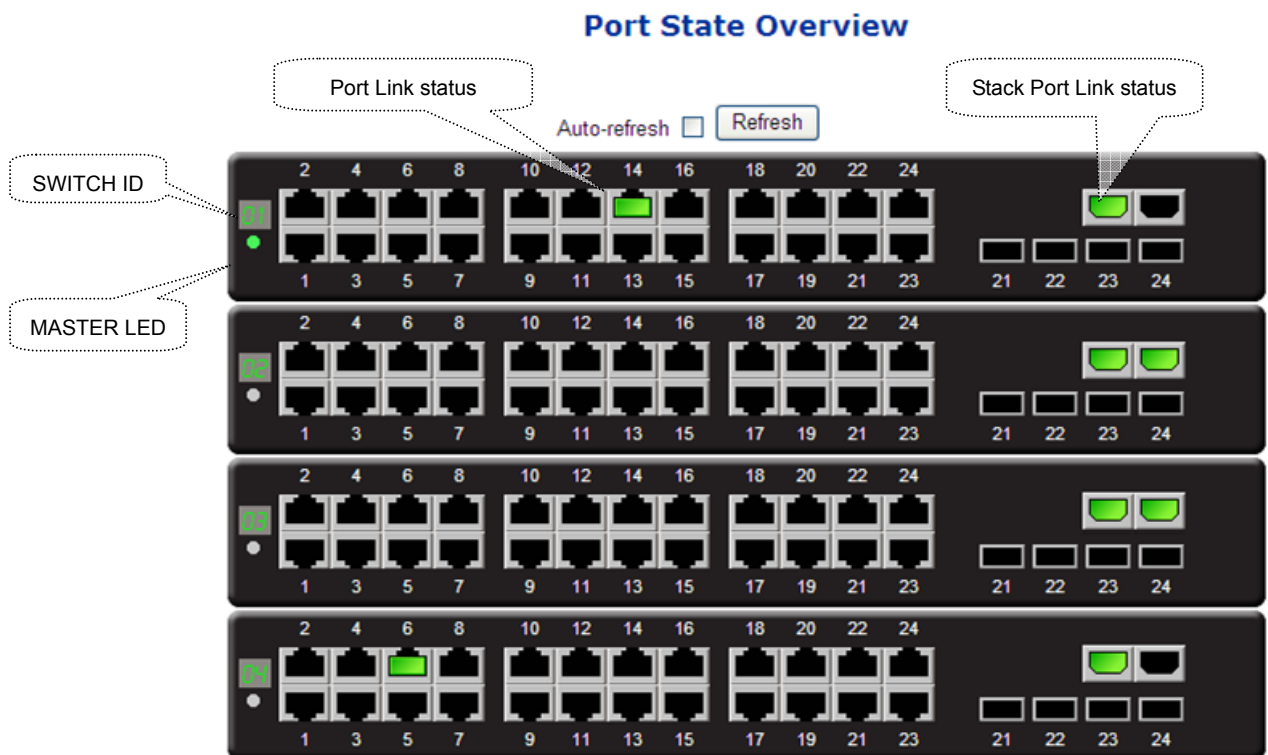
Figure 4-16-10 Port State Overview page screenshot

208

4.16.5 Stack Example

Stacking function is convenient for administrator to manage multiple switches by single IP. Basically, you got to have min. 2 units. The SGSW Switch supports auto stack configuration. Once the stack cable is connect to the stack port of each SGSW switch and power on them, the stack is builded automatically and the Switch ID is automatically assigned to the switch. It is also easy to add or delete stackable switch to the stack without service interruption. The key point of the Stack management are:

- **Identify the MASTER SWITCH**
- Assign / re-assing **Switch ID** for each management purpose

Step 1: linking the switches by CB-STX50 stack cable.

Step 2: Check the Master LED of each SGSW switch to find out the Master Switch that is elected automatically by the stack operation.

Step 3: Use the Web browser such as IE 6.0 to login the Master Switch, the default IP address is 192.168.0.100. Or you can use the PLANET Smart Discovery Utility to find out the IP address of the stack group.
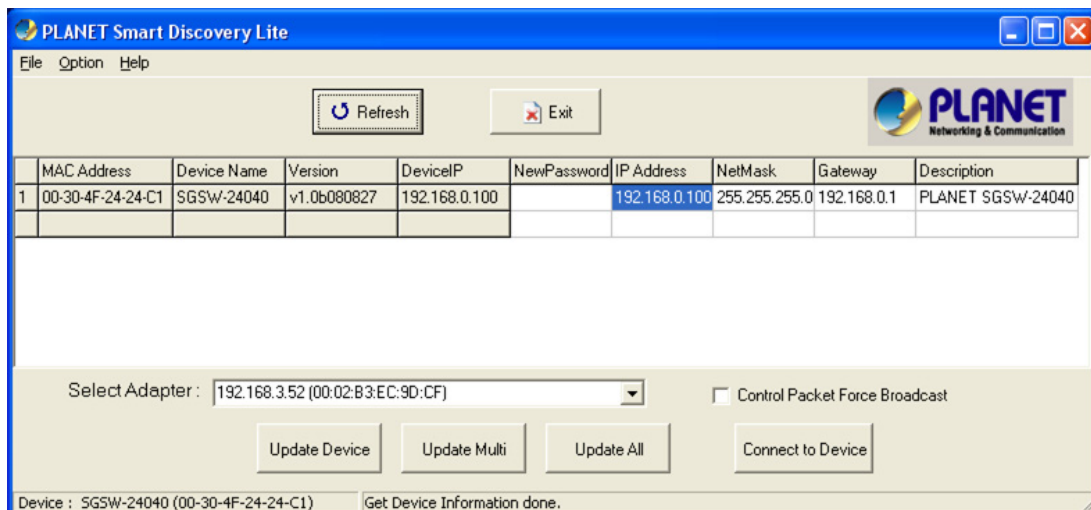
Figure 4-16-11 Use PLANET Smart Discovery Utility to display the IP address of stack master

Step 4: Choose "Stack \ Stack Configuration" from menu tree. You can see the Stack had established automaticatlly. As the below screen appears:

1. The Switch ID is automatically assigned to the switches
2. All switches with same Priority value "3".
3. The one can't be delete is the Stack master.

Figure 4-16-12 Stack Configuration

Step 5: We wish to make the SGSW switch with MAC "00-30-4f-24-04-76" / Switch ID=2 to become the Stack Master and swap the Switch ID to 1.

■ Select the switch with ID=1 and assign a new ID for this unit, for example: ID=4

Figure 4-16-13 Assing new ID for current master

■ Select the target switch and set up with lower priority "1", also re-assing the Switch ID=1 for it. After click Save, click "Start Master Election" and save again.

Figure 4-16-14 Assing lower priority value fo the target switch

■ Reflash the web browser, the switch with MAC address "00-30-4f-24-04-76" become the stack master now.
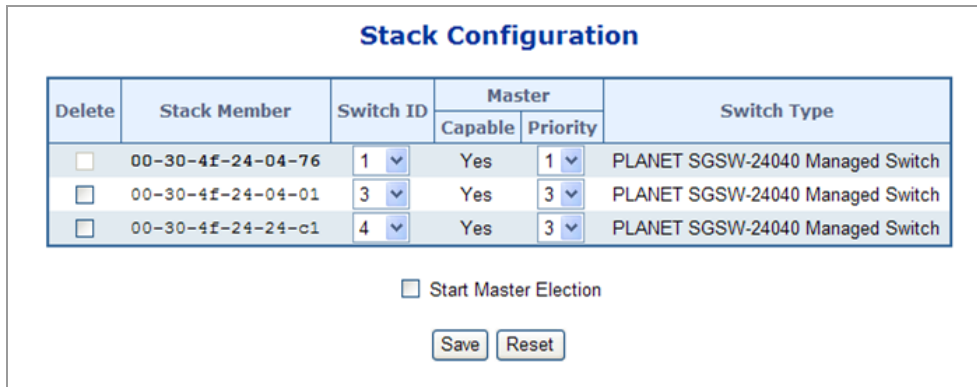
Figure 4-16-14 The result after master election

Step 6: After the Stack Master and Members have been configured, any switch in the stack can be managed from the web agent by choosing the desired Member ID from the Switch drop down menu.

Figure 4-16-15 To manage the member switch

Note	Slave switch IP will be covered by Master one, and disappear temporarily. The slave IP address can be the same as Master IP address. Thus, if master switch is malfunction, you can still access the other switch by same IP address.

Note	If you have difficulty on selecting another switch, you may be connecting to the slave switch's web, please close the browser window, use the "**arp –d** * " DOS command to clear the ARP table and then reopen the web.

4.17 Power over Ethernet (SGSW-24040P / SGSW-24040P4)

Providing up to 24 PoE, in-line power interface, the SGSW-24040P / SGSW-24040P PoE Switch can easily build a power central-controlled IP phone system, IP Camera system, AP group for the enterprise. For instance, 24 camera / AP can be easily installed around the corner in the company for surveillance demands or build a wireless roaming environment in the office. Without the power-socket limitation, the PoE Switch makes the installation of cameras or WLAN AP more easily and efficiently.
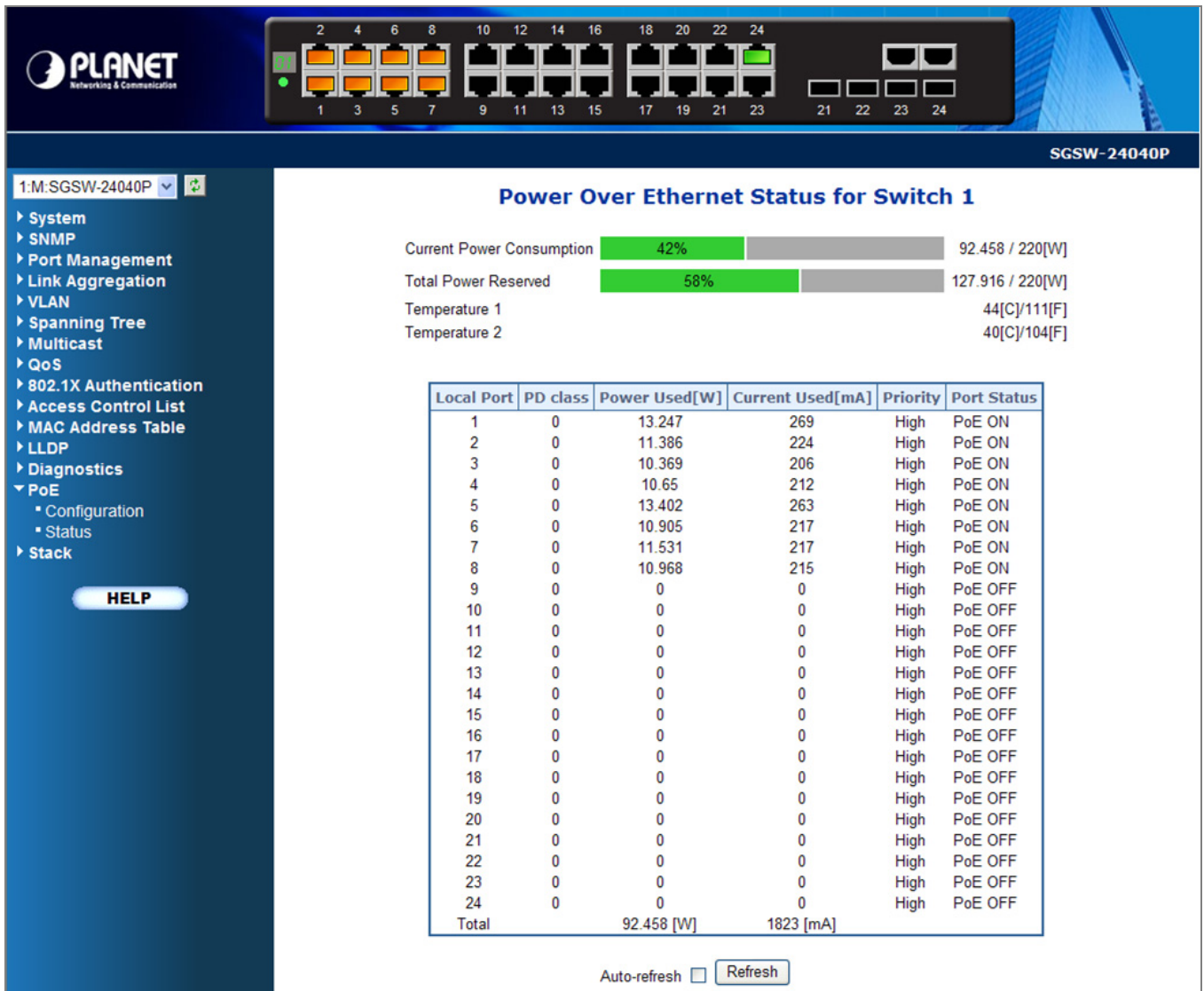
Figure 4-17-1 Power over Ethernet Status

4.17.1 Power over Ethernet Powered Device

3~5 watts	**Voice over IP phones** Enterprise can install POE VoIP Phone, ATA and other Ethernet/non-Ethernet end-devices to the central where UPS is installed for un-interrupt power system and power control system.
6~12 watts	**Wireless LAN Access Points** Museum, Sightseeing, Airport, Hotel, Campus, Factory, Warehouse can install the Access Point any where with no hesitation
10~12 watts	**IP Surveillance** Enterprise, Museum, Campus, Hospital, Bank, can install IP Camera without limits of install location – no need electrician to install AC sockets.
3~12 watts	**PoE Splitter** PoE Splitter split the PoE 48V DC over the Ethernet cable into 5/9/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.

4.17.2 Power Configuration

In a power over Ethernet system, operating power is applied from a power source (PSU-power supply unit) over the LAN infrastructure to **powered devices (PDs)**, which are connected to ports. Under some conditions, the total output power required by PDs can exceed the maximum available power provided by the PSU. The system may a prior be planed with a PSU capable of supplying less power than the total potential power consumption of all the PoE ports in the system. In order to maintain the majority of ports active, power management is implemented.

The PSU input power consumption is monitored by measuring voltage and current .The input power consumption is equal to the system's aggregated power consumption .The power management concept allows all ports to be active and activates additional ports, as long as the aggregated power of the system is lower than the power level at which additional PDs cannot be connected .When this value is exceeded, ports will be deactivated, according to user-defined priorities. The power budget is managed according to the following user-definable parameters: maximum available power, ports priority, maximum allowable power per port.

Reserved Power determined by

There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports.

■   **Classification mode**

In this mode each port automatic determines how much power to reserve according to the class the connected PD belongs

to, and reserves the power accordingly. Three different port classes exist and one for 4, 7 and 15.4 Watts.

Class	Usage	Range of maximum power used by the PD
0	Default	0.44 to 12.95 Watts
1	Optional	0.44 to 3.84 Watts
2	Optional	3.84 to 6.49 Watts
3	Optional	6.49 to 12.95 Watts (or to 15.4Watts)
4	Not Allowed	Reserved for Future Use

> **Note** In this mode the **Maximum Power fields** have no effect.

■   **Allocation mode**

In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each

port/PD is specified in the Maximum Power fields. The ports are shut down when total reserved powered exceeds the

amount of power that the power supply can deliver.

> **Note** In this mode the port power is not turned on if the PD requests more power the available.

■   **Auto mode**

The Power Management function will **automatically** select the mode of operation, according to the following sequence:

● **Port class, if available**

● **Power allocation, if available**

● **Port power consumption.**

■   **Consumption**

In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the

power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The

ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number

is shut down.

■   **Priority mode**

In this mode the user assign the priority to the ports/PD. When the total PoE power consumption request is over the allowed

power supply limitation, the system shut down PoE ports by port priority setting.

Ethernet Port Configuration

This section allows the user to inspect and configure the current PoE port settings, screen in Figure 4-17-2 appears.

Figure 4-17-2 PoE Configuration screenshot

The page includes the following fields:

Object	Description
• **Mode**	There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports. ■ **Classification mode**

- ■ **Allocation mode**

- ■ **Auto mode**

  - Port class, if available

  - Power allocation, if available

  - Port power consumption.

- ■ **Consumption**

- ■ **Priority mode**

The default PoE management mode is "**Auto mode**".

• **Power Supply**	Set limit value of the total PoE port provided power to the PDs. For **SGSW-24040P**, the available max. value is **220**, and for **SGSW-24040P4**, the available max. value is **380**.
• **Local Port**	This is the logical port number for this row.
• **PoE Enabled**	The PoE Enabled represents whether the PoE is enable for the port.
• **Priority**	The Priority represents the ports priority. There are three levels of power priority named **Low**, **High** and **Critical**. The priority is used in the case where the remote devices requires uses more power than power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the lowest port number.
• **Maximum Power**	The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delived to a remote device.
• **Power Allocation**	It can limit the port PoE supply watts. Per port maximum value must less 15.4, total ports values must less than the Power Reservation value. Once power overload detected, the port will auto shut down and keep on detection mode until PD's power consumption lower than the power limit value. Note. The system PoE mode have to set to **Allocation** mode then it effect.

For **SGSW-24040P**, the total PoE power reservation from Port-1~24 is up to **220W**

For **SGSW-24040P4**, the total PoE power reservation from Port-1~24 is up to **380W**

PD Classifications

A PD may be classified by the PSE based on the classification information provided by the PD. The intent of PD classification is to provide information about the maximum power required by the PD during operation. **Class 0** is the default for PDs. However, to improve power management at the PSE, the PD may opt to provide a signature for **Class 1 to 3**.

The PD is classified based on power. The classification of the PD is the maximum power that the PD will draw across all input voltages and operational modes.

A PD shall return Class 0 to 3 in accordance with the maximum power draw as specified by Table 4-17-1.

Class	Usage	Range of maximum power used by the PD
0	Default	0.44 to 12.95 Watts
1	Optional	0.44 to 3.84 Watts
2	Optional	3.84 to 6.49 Watts
3	Optional	6.49 to 12.95 Watts
4	Not Allowed	Reserved for Future Use

Table 4.17-1 Device class

Class 4 is defined but is reserved for future use. A Class 4 signature cannot be provided by a compliant PD.

4.17.3 PoE Status

This page allows the user to inspect the total power consumption, total power reserved and current status for all PoE ports.
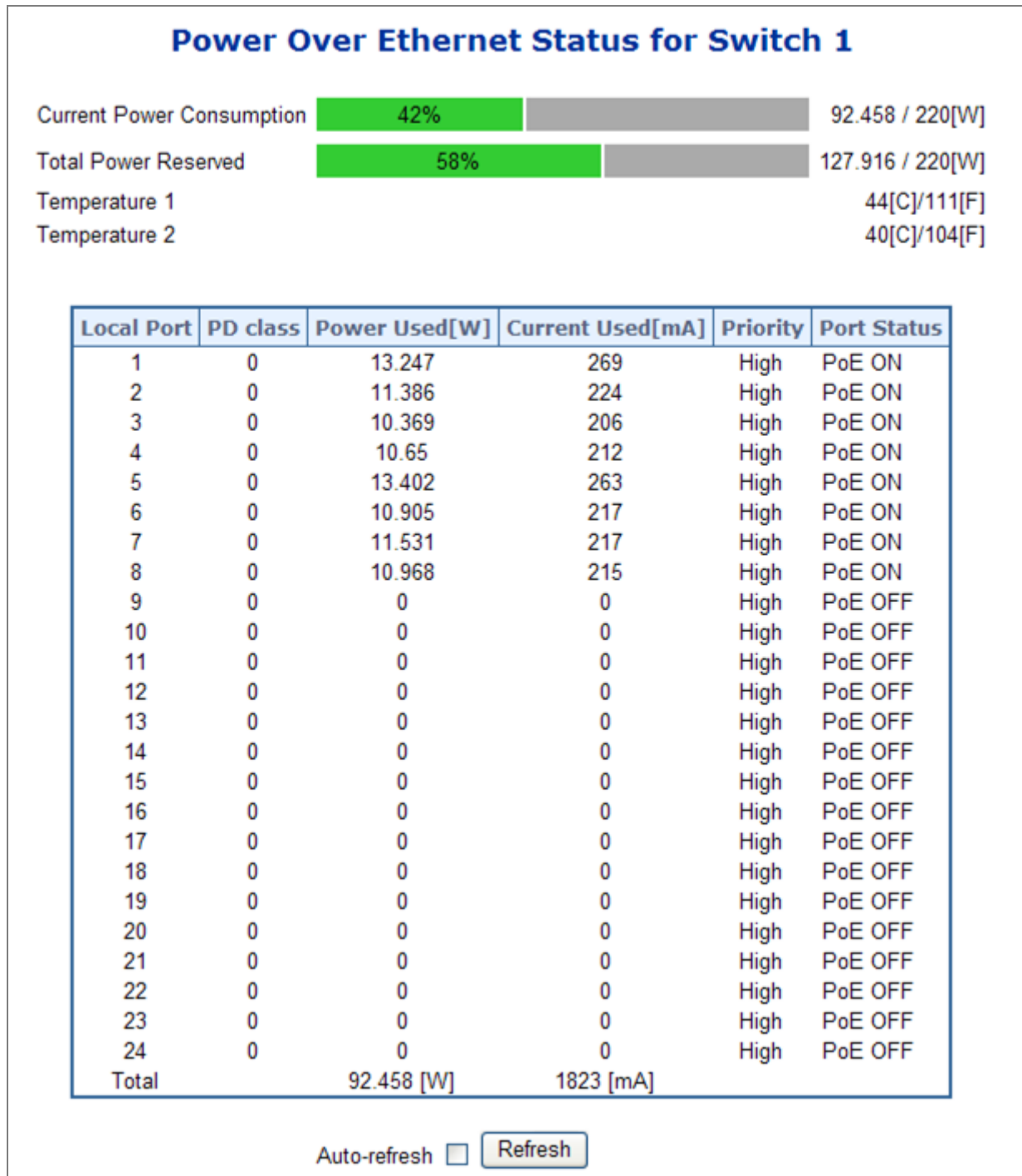
The page includes the following fields:

Object	Description
• **Current Power Consumption**	Show the total watts usage of PoE Switch.

• **Total Power Reserved**	Shows how much the total power be reserved for all PDs.
• **PoE Temperature Unit 1**	Display the current operating temperature of PoE chip unit 1. The unit 1 is in charge of PoE Port-1~Port-12
• **PoE Temperature Unit 2**	Display the current operating temperature of PoE chip unit 2. The unit 1 is in charge of PoE Port-13~Port-24
• **Local Port**	This is the logical port number for this row.
•	Display the class of the PD attached to the port, as established by the classification process. Class 0 is the default for PDs. The PD is classified based on power. The classification of the PD is the maximum power that the PD will draw across all input voltages and operational modes. A PD shall return Class 0 to 3 in accordance with the maximum power draw as specified by **Table 4-17-1**.
• **Power Reserved**	The **Power Reserved** shows how much the power the PD has reserved.
• **Power Used**	The **Power Used** shows how much power the PD currently is using.
• **Current Used**	The **Power Used** shows how much current the PD currently is using.
• **Priority**	The **Priority** shows the port's priority configured by the user.
• **Port Status**	The **Port Status** shows the port's status.
• **Total**	Show the total watts usage of all PDs.

5. COMMAND LINE INTERFACE

5.1 Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

This chapter describes how to use the Command Line Interface (CLI).

Logon to the Console

Once the terminal has connected to the device, power on the WGSW / SGSW Managed Switch, the terminal will display that it is running testing procedures.

Then, the following message asks the login password. The factory default password as following and the login screen in Figure 5-1 appears.

Password: **admin**

Figure 5-1 WGSW / SGSW Managed Switch Console Login screen

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

Configure IP address

The WGSW / SGSW Managed Switch is shipped with default IP address as following.

IP Address : **192.168.0.100**

Subnet Mask : **255.255.255.0**

To check the current IP address or modify a new IP address for the Switch, please use the procedures as follow:

■ **Show the current IP address**

1. On **"Switch/> "** prompt, enter **"show ip".**

2. The screen displays the current IP address, Subnet Mask and Gateway. As show in Figure 5-2.

Figure 5-2 Show IP information screen

■ **Configure IP address**

221

3.   On "**Switch/>** " prompt, enter the following command and press **<Enter>.** As show in Figure 5-3.

> **Switch/> ip setup 192.168.1.100 255.255.255.0 192.168.1.1**

The previous command would apply the follow settings for the Switch.

   IP: 192.168.1.100
   Subnet Mask: 255.255.255.0
   Gateway: 192.168.1.1
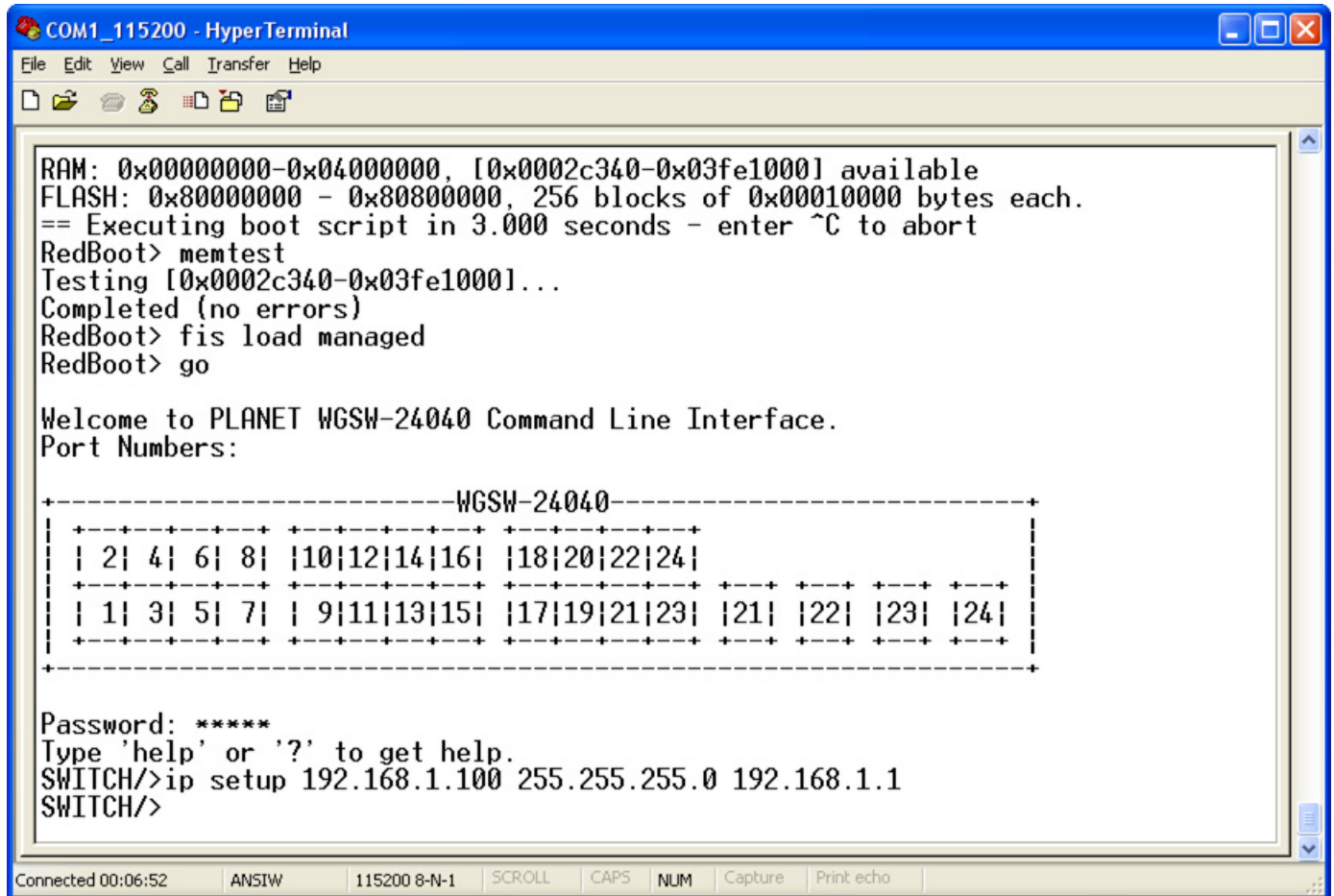
Figure 5-3 Set IP address screen

4.   Repeat Step 1 to check if the IP address is changed.

If the IP is successfully configured, the Managed Switch will apply the new IP address setting immediately. You can access the Web interface of WGSW / SGSW Managed Switch through the new IP address.
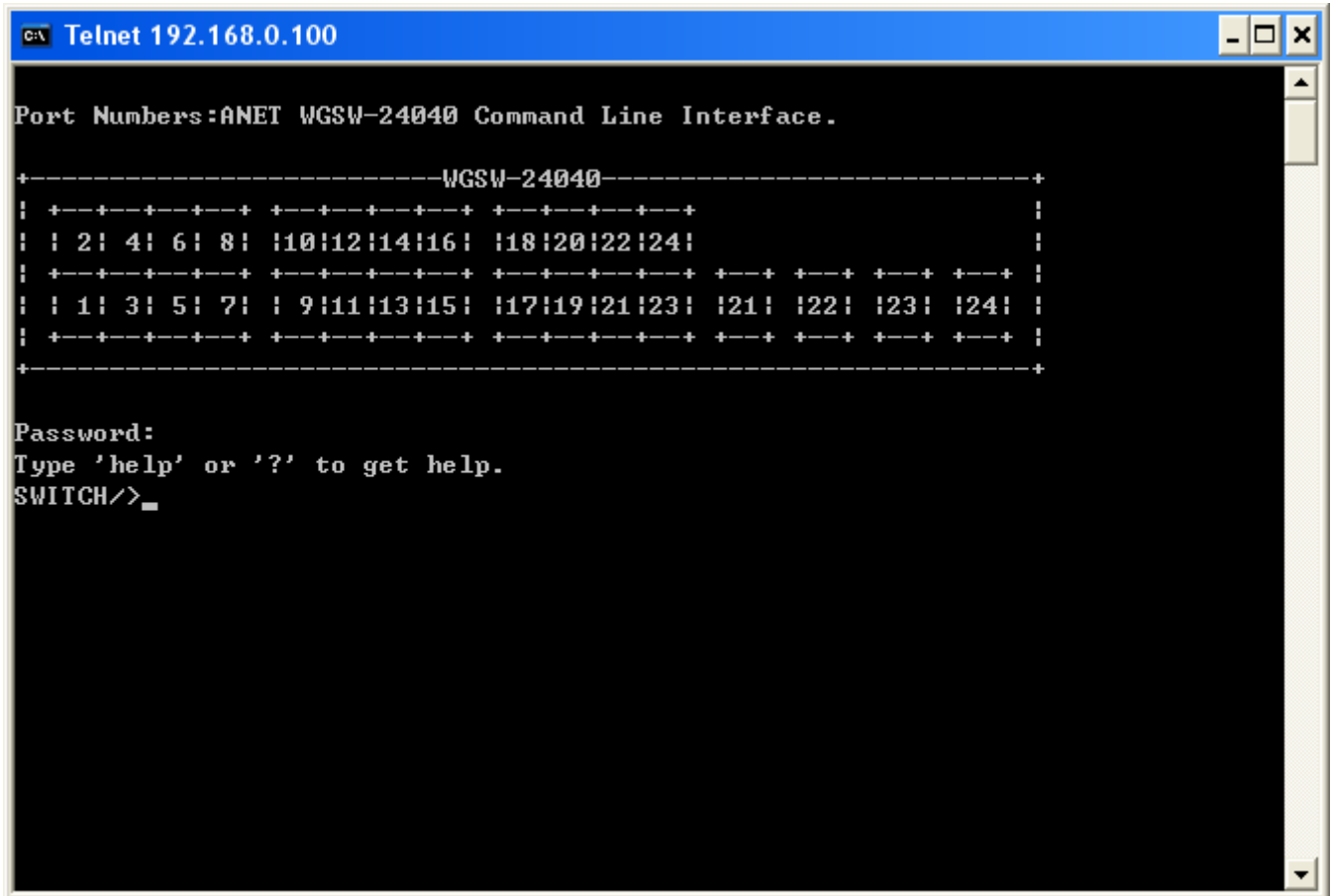
Note	If you do not familiar with console command or the related parameter, enter "**help**" anytime in console to get the help description.

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

5.2 Telnet login

The Managed Switch also supports telnet for remote management. The switch asks for user name and password for remote login when using telnet, please use **"admin"** for password.

6. Command Line Mode

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes supports specific software commands.

Command Groups:

System	System settings and reset options
IP	IP configuration and Ping
Port	Port management
Aggr	Link Aggregation
LACP	Link Aggregation Control Protocol
RSTP	Rapid Spanning Tree Protocol
Dot1x	IEEE 802.1X port authentication
IGMP	Internet Group Management Protocol snooping
LLDP	Link Layer Discovery Protocol
MAC	MAC address table
VLAN	Virtual LAN
PVLAN	Private VLAN
QoS	Quality of Service
ACL	Access Control List
Mirror	Port mirroring
SNMP	Simple Network Management Protocol
Stack	Stack management
Firmware	Download of firmware via TFTP

6.1 System Command

System Configuration

Description:

Show system configuration.

Syntax:

System Configuration [all] [<port_list>]

Parameters:

all   : Show all switch configuration, default: Show system configuration

<port_list>: Port list or 'all', default: All ports

Example:

To display system information:

```
Switch/>system configuration

System Name       : SGSW-24040

System Password: admin

CLI Prompt        : Switch

Timezone Offset: 0

MAC Address       : 00-30-4f-24-04-03

System Time       : 1970-01-01 03:13:21 +0000

System Uptime    : 03:13:21


SID    Software Version

---    ---------------

3      Beta_080813
```

System Reboot

Description:

Reboot the system.

Syntax:

System Reboot

Example:

To reboot device without changing any of the settings:

```
Switch/>system reboot
```

System Restore Default

Description:

Restore factory default configuration.

Syntax:

System Restore Default [keep_ip]

Parameters:

keep_ip: Keep IP configuration, default: Restore full configuration

Example:

To restore default value but not reset IP address:

Switch/>system restore default keep_ip

System Name

Description:

Set or show the system name.

Syntax:

System Name [<name>]

Parameters:

<name>: System name or 'clear' to clear

System name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No blank or space characters

are permitted as part of a name. The first character must be an alpha character, and the first or last character must not be

a minus sign.

Default Setting:

SGSW-24040

Example:

To set device title:

Switch/>System name SGSW-24040-LAB

System Prompt

Description:

Set the CLI prompt string.

Syntax:

System Prompt <prompt>

Parameters:

<prompt>: CLI prompt string

Default Setting:

SWITCH

Example:

To change CLI title:

Switch/>system prompt SGSW-24040

SGSW-24040/>

System Password

Description:

Set or show the system password.

Syntax:

System Password [<password>]

Parameters:

<password>: System password or 'clear' to clear

Default Setting:

admin

Example:

To set password:

Switch/>system password admin

System SNTP

Description:

Set or show the SNTP Time server address.

Syntax:

System SNTP [<ip_addr>]

Parameters:

    <ip_addr>: IP address (a.b.c.d), default: Show IP address

Default Setting:

    0.0.0.0

Example:

    Set SNTP server:

SWITCH/>system sntp 220.130.158.52

System Timezone

Description:

    Set or show the system timezone offset.

Syntax:

    System Timezone [<offset>]

Parameters:

    <offset>: Time zone offset in minutes (-720 to 720) relative to UTC

Default Setting:

    0

Example:

    To set timezone:

Switch/>system timezone 0

System Firmware Load

Description:

    Load new firmware from TFTP server.

Syntax:

    System Firmware Load <ip_server> <file_name>

Parameters:

<ip_server>: TFTP server IP address (a.b.c.d)

<file_name>: Firmware file name

229

IP Configuration

Description:

Show IP configuration.

Syntax:

IP Configuration

Example:

Show IP configuration:

```
Switch/>ip configuration
DHCP Client: Disabled
IP Address : 192.168.100.105
IP Mask      : 255.255.255.0
IP Router   : 192.168.100.1
VLAN ID      : 1
SNTP Server: 0.0.0.0
```

IP DHCP

Description:

Set or show the DHCP client mode.

Syntax:

IP DHCP [enable|disable]

Parameters:

enable : Enable or renew DHCP client

disable: Disable DHCP client

Default Setting:

Disable

Example:

Disable DHCP sever:

```
SWITCH/>ip dhcp disable
```

IP Setup

Description:

Set or show the IP setup.

Syntax:

IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

Parameters:

<ip_addr>   : IP address (a.b.c.d), default: Show IP address

<ip_mask>   : IP subnet mask (a.b.c.d), default: Show IP mask

<ip_router>: IP router (a.b.c.d), default: Show IP router

<vid>   : VLAN ID (1-4095), default: Show VLAN ID

Default Setting:

IP Address : 192.168.0.100

IP Mask   : 255.255.255.0

IP Router   : 192.168.0.1

VLAN ID   : 1

Example:

Set IP address:

SWITCH/>ip setup 192.168.0.100 255.255.255.0

IP Ping

Description:

Ping IP address (ICMP echo).

Syntax:

IP Ping <ip_addr> [<ping_length>]

Parameters:

<ip_addr>   : IP host address (a.b.c.d)

<ping_length>: Ping data length (8-1400), excluding MAC, IP and ICMP headers

Example:

```
SWITCH/>ip ping 192.168.0.51

PING server 192.168.0.51

60 bytes from 192.168.0.51: icmp_seq=0, time=0ms

60 bytes from 192.168.0.51: icmp_seq=1, time=0ms

60 bytes from 192.168.0.51: icmp_seq=2, time=10ms

60 bytes from 192.168.0.51: icmp_seq=3, time=0ms

60 bytes from 192.168.0.51: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad
```

6.2 Port Management Command

Port Configuration

Description:

Show port configuration.

Syntax:

Port Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Display port1~4 status

```
SWITCH/>port configuration 1-4

Port   State     Mode    Flow Control    MaxFrame        Power     Excessive    Link

------ --------  ------  ----------------  --------------  --------  -----------  ----

1      Enabled   Auto    Disabled          9600            Enabled   Discard      Down

2      Enabled   Auto    Disabled          9600            Enabled   Discard      Down

3      Enabled   Auto    Disabled          9600            Enabled   Discard      Down

4      Enabled   Auto    Disabled          9600            Enabled   Discard      100fdx
```

Port State

Description:

Set or show the port administrative state.

Syntax:

Port State [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable   : Enable port

disable   : Disable port

(default: Show administrative mode)

Default Setting:

Enable

Example:

Disable port1

```
SWITCH/>port state 1 disable
```

Port Mode

Description:

Set or show the port speed and duplex mode.

Syntax:

Port Mode [<port_list>] [10hdx|10fdx|100hdx|100fdx|1000fdx|auto]

Parameters:

<port_list>: Port list or 'all', default: All ports

10hdx   : 10 Mbps, half duplex

10fdx   : 10 Mbps, full duplex

100hdx   : 100 Mbps, half duplex

100fdx   : 100 Mbps, full duplex

1000fdx   : 1 Gbps, full duplex

auto   : Auto negotiation of speed and duplex

(default: Show configured and current mode)

Default Setting:

Auto

Example:

Set 10Mbps (half duplex) speed for port1

```
SWITCH/>port mode 1 10hdx
```

Port Flow Control

Description:

Set or show the port flow control mode.

Syntax:

Port Flow Control [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable   : Enable flow control

disable   : Disable flow control

(default: Show flow control mode)

Default Setting:

Disable

Example:

Enable flow control function for port1

SWITCH/>port flow control 1 enable

Port Maximum Frame

Description:

Set or show the port maximum frame size.

Syntax:

Port MaxFrame [<port_list>] [<max_frame>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<max_frame>: Port maximum frame size (1518-9600), default: Show maximum frame size

Default Setting:

9600

Example:

Set 2048 frame size for port1

SWITCH/>port maxframe 1 2048

Port Power

Description:

Set or show the port PHY power mode.

Syntax:

Port Power [<port_list>] [enable|disable|actiphy|dynamic]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable all power control

disable: Disable all power control

actiphy: Enable ActiPHY power control

dynamic: Enable Dynamic power control

Default Setting:

Enable

Example:

Disable port power function for port1-4

SWITCH/>port power 1-4 disable

Port Excessive

Description:

Set or show the port excessive collision mode.

Syntax:

Port Excessive [<port_list>] [discard|restart]

Parameters:

<port_list>: Port list or 'all', default: All ports

discard   : Discard frame after 16 collisions

restart   : Restart backoff algorithm after 16 collisions

(default: Show mode)

Default Setting:

Discard

Example:

SWITCH/>port excessive 1 restart

Port Statistics

Description:

Show port statistics.

Syntax:

Port Statistics [<port_list>] [<command>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<command> : The command parameter takes the following values:

clear : Clear port statistics

packets : Show packet statistics

bytes : Show byte statistics

errors : Show error statistics

discards : Show discard statistics

filtered : Show filtered statistics

low : Show low priority statistics

normal : Show normal priority statistics

medium : Show medium priority statistics

high : Show high priority statistics

(default: Show all port statistics)

Port VeriPHY

Description:

Run cable diagnostics.

Syntax:

Port VeriPHY [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Port Numbers   238

Description:

Show port numbering.

Syntax:

Port Numbers

Mirror Configuration

Description:

Show mirror configuration.

Syntax:

Mirror Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Mirror Port

Description:

Set or show the mirror port.

Syntax:

Mirror Port [<port>|disable]

Parameters:

<port>|disable: Mirror port or 'disable', default: Show port

Default Setting:

Disable

Mirror SID

Description:

Set or show the mirror switch ID.

Syntax:

Mirror SID [<sid>]

Parameters:

<sid>: Switch ID (1-16)

Default Setting:

1

Example:

Set mirror SID 2 for switch

SWITCH/>mirror sid 2

Mirror Mode

Description:

Set or show the mirror mode.

Syntax:

Mirror Mode [<port_list>] [enable|disable|rx|tx]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable Rx and Tx mirroring

disable: Disable Mirroring

rx   : Enable Rx mirroring

tx   : Enable Tx mirroring

(default: Show mirror mode)

Default Setting:

Disable

Example:

Enable mirror mode for port20

SWITCH/>mirror mode 20 enable

6.3 Link Aggregation Command

Aggregation Configuration

Description:

Show link aggregation configuration.

Syntax:

Aggr Configuration

Example:

SWITCH/>aggr configuration

Aggregation Mode:

SMAC   : Enabled

DMAC   : Disabled

IP   : Enabled

Port   : Enabled

Aggregation Add

Description:

Add or modify link aggregation.

Syntax:

Aggr Add <port_list> [<aggr_id>]

Parameters:

<port_list>: Port list

<aggr_id>   : Aggregation ID, global: 1-2, local: 3-14

Default Setting:

Disable

Example:

Add port 1~4 in Group1

SWITCH/>aggr add 1-4 1

Aggregation Delete

Description:

Delete link aggregation.

Syntax:

Aggr Delete <aggr_id>

Parameters:

<aggr_id>: Aggregation ID, global: 1-2, local: 3-14

Example:

Delete Group2

```
SWITCH/>aggr delete 2
```

Aggregation Lookup

Description:

Lookup link aggregation.

Syntax:

Aggr Lookup [<aggr_id>]

Parameters:

<aggr_id>: Aggregation ID, global: 1-2, local: 3-14

Example:

Show aggregation status

```
SWITCH/>aggr lookup 1


Aggr ID   Name      Type      Ports

----------   -------      -------      -------

1            GLAG1    Static     1-4
```

Aggregation Mode

Description:

Set or show the link aggregation traffic distribution mode.

Syntax:

Aggr Mode [smac|dmac|ip|port] [enable|disable]

Parameters:

>**smac**   : Source MAC address
>
>**dmac**   : Destination MAC address
>
>**ip**   : Source and destination IP address
>
>**port**   : Source and destination UDP/TCP port
>
>**enable**   : Enable field in traffic distribution
>
>**disable**   : Disable field in traffic distribution

Default Setting:

>SMAC   : Enabled
>
>DMAC   : Disabled
>
>IP   : Enabled
>
>Port   : Enabled

Example:

Disable SMAC mode

```
SWITCH/>Aggr mode smac disable
```

LACP Configuration

Description:

Show LACP configuration.

Syntax:

LACP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LACP configuration

```
SWITCH/>lacp configuration


Port  Mode      Key   Role

----  --------  ----  ------

1     Disabled  Auto  Active

2     Disabled  Auto  Active

3     Disabled  Auto  Active

4     Disabled  Auto  Active

5     Disabled  Auto  Active

6     Disabled  Auto  Active

7     Disabled  Auto  Active

8     Disabled  Auto  Active

9     Disabled  Auto  Active

10    Disabled  Auto  Active

11    Disabled  Auto  Active

12    Disabled  Auto  Active

13    Disabled  Auto  Active

14    Disabled  Auto  Active

15    Disabled  Auto  Active

16    Disabled  Auto  Active

17    Disabled  Auto  Active

18    Disabled  Auto  Active

19    Disabled  Auto  Active

20    Disabled  Auto  Active
```

```
21     Disabled   Auto   Active

22     Disabled   Auto   Active

23     Disabled   Auto   Active

24     Disabled   Auto   Active
```

LACP Mode

Description:

Set or show LACP mode.

Syntax:

LACP Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable LACP protocol

disable: Disable LACP protocol

(default: Show LACP mode)

Default Setting:

Disable

Example:

Enable LACP for port1~4

```
SWITCH/>lacp mode 1-4 enable
```

LACP Key

Description:

Set or show the LACP key.

Syntax:

LACP Key [<port_list>] [<key>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<key>   : LACP key (1-65535) or 'auto'

Default Setting:

Auto

Example:

Set key1 for port1~4

```
SWITCH/>lacp key 1-4 1
```

LACP Role

Description:

Set or show the LACP role.

Syntax:

LACP Role [<port_list>] [active|passive]

Parameters:

<port_list>: Port list or 'all', default: All ports

active : Initiate LACP negotiation

passive: Listen for LACP packets

(default: Show LACP role)

Default Setting:

Active

Example:

Set passive for port1~4

```
SWITCH/>lacp role 1-4 passive
```

LACP Status

Description:

Show LACP Status.

Syntax:

LACP Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LACP status of port1~4

```
SWITCH/>lacp status 1-4


Port  Mode         Key    Aggr ID   Partner System ID      Partner Port

------ ----------- -----  -------   ----------------------- -----------
1     Disabled     1      -         -                       -
2     Disabled     1      -         -                       -
3     Disabled     1      -         -                       -
4     Disabled     1      -         -                       -
```

LACP Statistics

Description:

Show LACP Statistics.

Syntax:

LACP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear   : Clear LACP statistics

Example:

Show LACP statistics of port1~4

```
SWITCH/>lacp statistics 1-4


Port  Rx Frames     Tx Frames     Rx Unknown    Rx Illegal

------ -------------- -------------- -------------- ---------
1      0             0             0             0
2      0             0             0             0
3      0             0             0             0
4      0             0             0             0
```

6.4 VLAN Configuration Command

VLAN Configuration

Description:

Show VLAN configuration.

Syntax:

VLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show VLAN status of port1

```
SWITCH/>vlan configuration 1


Mode : IEEE 802.1Q

Port PVID   IngrFilter   FrameType      LinkType    Q-in-Q Mode       Eth type
------------   ---------   --------------   -----------   -----------------   --------
1    1      Disabled     All            UnTag       Disable           N/A


VID    Ports
----     -----
1      1-26
```

VLAN Mode

Description:

Set or show the VLAN Mode.

Syntax:

VLAN Mode [portbased|dot1q]

Parameters:

portbased   : Port-Based VLAN Mode

dot1q   : 802.1Q VLAN Mode

Default Setting:

249

Dot1q

Example:

Set VLAN mode in port base

```
SWITCH/>vlan mode portbased
```

VLAV PVID

Description:

Set or show the port VLAN ID.

Syntax:

VLAN PVID [<port_list>] [<vid>|none]

Parameters:

<port_list>: Port list or 'all', default: All ports

<vid>|none : Port VLAN ID (1-4095) or 'none', default: Show port VLAN ID

Default Setting:

1

Example:

Set PVID2 for port20

```
SWITCH/>vlan pvid 20 2
```

VLAN Frame Type

Description:

Set or show the port VLAN frame type.

Syntax:

VLAN FrameType [<port_list>] [all|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports

all   : Allow tagged and untagged frames

tagged   : Allow tagged frames only

(default: Show accepted frame types)

Default Setting:

All

Example:

Set port20 that allow tagged frames only

```
SWITCH/>vlan frametype 20 tagged
```

VLAN Ingress Filter

Description:

Set or show the port VLAN ingress filter.

Syntax:

VLAN IngressFilter [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable   : Enable VLAN ingress filtering

disable   : Disable VLAN ingress filtering

(default: Show VLAN ingress filtering)

Default Setting:

Disable

Example:

Enable VLAN ingress filtering for port20

```
SWITCH/>vlan ingressfilter 20 enable
```

VLAN Link Type

Description:

Set or show the port VLAN link type.

Syntax:

VLAN LinkType [<port_list>] [untagged|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports

untagged   : VLAN Link Type Tagged

tagged   : VLAN Link Type Untagged

Default Setting:

Un-tagged

Example:

Enable tagged frame for port2

SWITCH/>vlan linktype 2 tagged

VLAN Q-in-Q Mode

Description:

Set or show the port Q-in-Q mode.

Syntax:

VLAN Qinqmode [<port_list>] [disable|man|customer]

Parameters:

<port_list>: Port list or 'all', default: All ports

disable   : Disable Q-in-Q VLAN Mode

man   : Q-in-Q MAN Port Mode

customer   : Q-in-Q Customer Port Mode

VLAN Ethernet Type

Description:

Set or show out layer VLAN tag ether type in Q-in-Q VLAN mode.

Syntax:

VLAN Ethtype [<port_list>] [man|dot1q]

Parameters:

<port_list>: Port list or 'all', default: All ports

man   : Set out layer VLAN tag ether type : MAN

dot1q   : Set out layer VLAN tag ether type : 802.1Q

Default Setting:

N/A

Example:

SWITCH/>vlan ethtype 10 man

VLAN Add

Description:

Add or modify VLAN entry.

Syntax:

VLAN Add <vid> [<port_list>]

Parameters:

<vid>   : VLAN ID (1-4095)

<port_list>: Port list or 'all', default: All ports

Default Setting:

1

Example:

Add port17 to port24 in VLAN10

SWITCH/>vlan add 10 17-24

VLAN Delete

Description:

Delete VLAN entry.

Syntax:

VLAN Delete <vid>

Parameters:

<vid>: VLAN ID (1-4095)

Example:

Delete port17 to port24 in VLAN10

SWITCH/>vlan delete 10 17-24

VLAN Lookup

Description:

Lookup VLAN entry.

Syntax:

VLAN Lookup [<vid>]

Parameters:

<vid>: VLAN ID (1-4095), default: Show all VLANs

Example:

Show VLAN status

SWITCH/>vlan lookup

PVLAN Configuration

Description:

Show Private VLAN configuration.

Syntax:

PVLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

PVLAN Isolate

Description:

Set or show the port isolation mode.

Syntax:

PVLAN Isolate [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable   : Enable port isolation

disable   : Disable port isolation

(default: Show port isolation port list)

Default Setting:

Promiscous

Example:

Enable isolate for port10

SWITCH/>pvlan isolate 10 enable

6.5 Spanning Tree Protocol Command

RSTP Configuration

Description:

Show RSTP configuration.

Syntax:

RSTP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

Default Setting:

Disable

Example:

Show RSTP status of port1

```
SWITCH/>rstp configuration 1
System Priority : 32768
Max Age          : 20
Forward Delay    : 15
Protocol Version: Normal


Port   Mode          Path Cost      Priority    Edge         Point2point
----   -------------  --------------  ----------  -----------  ---------------
1      Disabled       Auto            128         Enabled      Auto
```

RSTP SysPrio

Description:

Set or show the RSTP system priority.

Syntax:

RSTP SysPrio [<sys_prio>]

Parameters:

<sys_prio>: RSTP system priority (0/4096/8192/.../57344/61440)

Default Setting:

32768

Example:

Set RSTP system priority value in 4096

SWITCH/>rstp sysprio 4096

RSTP Age

Description:

Set or show the RSTP maximum age.

Syntax:

RSTP Age [<max_age>]

Parameters:

<max_age>: RSTP maximum age time (6-200)

Default Setting:

20

Example:

Set RSTP maximum age time in 200

SWITCH/>rstp age 200

RSTP Delay

Description:

Set or show the RSTP forward delay.

Syntax:

RSTP Delay [<delay>]

Parameters:

<delay>: RSTP forward delay (4-30)

Default Setting:

15

Example:

Set RSTP forward delay value in 25

SWITCH/>rstp delay 25

RSTP Version

Description:

Set or show the RSTP protocol version.

Syntax:

RSTP Version [compatible|normal]

Parameters:

compatible: Compatible with STP

normal   : RSTP

Default Setting:

Normal

Example:

Change RSTP version in compatible

SWITCH/>rstp version compatible

RSTP Mode

Description:

Set or show the RSTP mode.

Syntax:

RSTP Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

enable : Enable RSTP protocol

disable: Disable RSTP protocol

Default Setting:

Disable

Example:

Enable rstp mode for port1

```
SWITCH/>rstp mode 1 enable
```

RSTP Cost

Description:

Set or show the RSTP path cost.

Syntax:

RSTP Cost [<port_list>] [<path_cost>]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

<path_cost>: RSTP path cost (1-2000000000) or 'auto'

Default Setting:

Auto

Example:

Set RSTP cost value in 1 for port1

```
SWITCH/>rstp cost 1 1
```

RSTP Priority

Description:

Set or show the RSTP priority.

Syntax:

RSTP Priority [<port_list>] [<priority>]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

<priority> : RSTP priority (0/16/32/48/.../224/240)

Default Setting:

128

Example:

Set RSTP priority value in 16 for port1

SWITCH/>rstp priority 1 16

RSTP Edge

Description:

Set or show the RSTP edge parameter.

Syntax:

RSTP Edge [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable RSTP edge

disable: Disable RSTP edge

Default Setting:

Enable

Example:

Disable RSTP edge parameter for port1

SWITCH/>rstp edge 1 disable

RSTP P2P

Description:

Set or show the RSTP point2point parameter.

Syntax:

RSTP P2P [<port_list>] [enable|disable|auto]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable RSTP point2point

disable: Disable RSTP point2point

auto   : Automatic RSTP point2point detection

Default Setting:

Auto

Example:

Enable RSTP P2P mode for port1

```
SWITCH/>rstp p2p 1 enable
```

RSTP Status

Description:

Show RSTP status.

Syntax:

RSTP Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show RSTP status

```
SWITCH/>rstp status
===============================================================
VLAN ID      : 3
Bridge ID    : 32771:00-30-4f-24-24-c1
Root ID      : 32771:00-30-4f-24-24-c1
Root Port    : -
Root Cost    : 0
Topology Flag: Steady


Port     Port Role    State      Path Cost    Edge   P2P   Neigb
------   ------------  ---------- ------------ ------ ------ -------
1        Disabled     Disabled   1            No     Yes    RSTP
```

RSTP Statistics

Description:

Show RSTP statistics.

Syntax:

RSTP Statistics [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

RSTP mCheck

Description:

Set the RSTP mCheck (Migration Check) variable for ports.

Syntax:

RSTP Mcheck [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

6.6 Multicast Configuration Command

IGMP Configuration

Description:

Show IGMP snooping configuration.

Syntax:

IGMP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Default Setting:

IGMP Mode: Disabled

Flooding : Disabled

Example:

Enable IGMP mode

SWITCH/>igmp mode enable

IGMP Mode

Description:

Set or show the IGMP snooping mode.

Syntax:

IGMP Mode [enable|disable]

Parameters:

enable : Enable IGMP snooping

disable: Disable IGMP snooping

(default: Show IGMP snooping mode)

Default Setting:

Disabled

Example:

Enable IGMP mode

```
SWITCH/>igmp mode enable
```

IGMP State

Description:

Set or show the IGMP snooping state for VLAN.

Syntax:

IGMP State [<vid>] [enable|disable]

Parameters:

<vid>: VLAN ID (1-4095), default: Show all VLANs

enable : Enable IGMP snooping

disable: Disable IGMP snooping

(default: Show IGMP snooping mode)

Default Setting:

VID   State

----   ---------

1   Enabled

Example:

Enable IGMP mode

```
SWITCH/>igmp mode enable
```

IGMP State

Description:

Set or show the IGMP snooping state for VLAN.

Syntax:

IGMP State [<vid>] [enable|disable]

Parameters:

<vid>: VLAN ID (1-4095), default: Show all VLANs

enable : Enable IGMP snooping

disable: Disable IGMP snooping

(default: Show IGMP snooping mode)

Default Setting:

Enable

Example:

Disable VID 1

SWITCH/>igmp state 1 disable

IGMP Querier

Description:

Set or show the IGMP snooping querier mode for VLAN.

Syntax:

IGMP Querier [<vid>] [enable|disable]

Parameters:

<vid>: VLAN ID (1-4095), default: Show all VLANs

enable   : Enable IGMP querier

disable : Disable IGMP querier

(default: Show IGMP querier mode)

Default Setting:

Disable

Example:

SWITCH/>igmp querier 1 enable

IGMP Fast Leave

Description:

Set or show the IGMP snooping fast leave port mode.

Syntax:

IGMP Fastleave [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable   : Enable IGMP fast leave

disable : Disable IGMP fast leave

(default: Show IGMP fast leave mode)

Default Setting:

Disable

Example:

SWITCH/>igmp fastleave 1 enable

IGMP Router

Description:

Set or show the IGMP snooping router port mode.

Syntax:

IGMP Router [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable   : Enable IGMP router port

disable : Disable IGMP router port

(default: Show IGMP router port mode)

Default Setting:

Disable

Example:

Enable IGMP snooping function for port1~4

SWITCH/>igmp router 1-4 enable

IGMP Flooding

Description:

Set or show the IGMP snooping unregistered flood operation.

Syntax:

IGMP Flooding [enable|disable]

Parameters:

enable : Enable IGMP flooding

disable: Disable IGMP flooding

(default: Show IGMP flood mode)

Default Setting:

Disable

Example:

Enable IGMP flooding function

```
SWITCH/>igmp flooding enable
```

IGMP Groups

Description:

Show IGMP groups.

Syntax:

IGMP Groups [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

IGMP Status

Description:

Show IGMP status.

Syntax:

IGMP Status [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

Default Setting:

Disable

Example:

Enable IGMP flooding function

```
SWITCH/>igmp status 1

Switch 1:
---------


         Querier   Rx         Tx         Rx           Rx           Rx            Rx

VID      Status    Queries    Queries    V1 Reports   V2 Reports   V3 Reports    V2 Leave

----     --------  ----------  ----------  -----------  ------------  --------------  -----------
1        IDLE      0          0          0            0            0             0
```

6.7 Quality of Service Command

QoS Configuration

Description:

Show QoS Configuration.

Syntax:

QoS Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

QoS Classes

Description:

Set or show the number of traffic classes.

Syntax:

QoS Classes [<class>]

Parameters:

<class>: Number of traffic classes (1,2 or 4)

Default Setting:

4

Example:

Set QoS classes 2

SWITCH/>qos classes 2

QoS Default

Description:

Set or show the default port priority.

Syntax:

QoS Default [<port_list>] [<class>]

269

Parameters:

<port_list>: Port list or 'all', default: All ports

<class>   : Traffic class low/normal/medium/high or 1/2/3/4

Default Setting:

Low

Example:

Set high priority for port5

SWITCH/>qos default 5 high

QoS Tag Priority

Description:

Set or show the port VLAN tag priority.

Syntax:

QoS Tagprio [<port_list>] [<tag_prio>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<tag_prio> : VLAN tag priority (0-7)

Default Setting:

0

Example:

Set priority7 for VLAN3

SWITCH/>qos tagprio 3 7

QoS QCL Port

Description:

Set or show the port QCL ID.

Syntax:

QoS QCL Port [<port_list>] [<qcl_id>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<qcl_id>   : QCL ID

Default Setting:

1

Example:

Set QCL ID5 for port10

SWITCH/>qos qcl port 10 5

QoS QCL Add

Description:

Add or modify QoS Control Entry (QCE).

If the QCE ID parameter <qce_id> is specified and an entry with this QCE ID already exists, the QCE will be modified.

Otherwise, a new QCE will be added. If the QCE ID is not specified, the next available QCE ID will be used.

If the next QCE ID parameter <qce_id_next> is specified, the QCE will be placed before this QCE in the list. If the next

QCE ID is not specified, the QCE will be placed last in the list.

Syntax:

QoS QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>]

                   (etype <etype>) |

                   (vid <vid>) |

                   (port <udp_tcp_port>) |

                   (dscp <dscp>) |

                   (tos <tos_list>) |

                   (tag_prio <tag_prio_list>)

                   <class>

Parameters:

<qcl_id>   : QCL ID

<qce_id>   : QCE ID (1-24)

<qce_id_next>   : Next QCE ID (1-24)

etype   : Ethernet Type keyword

271

<etype>   : Ethernet Type

vid   : VLAN ID keyword

<vid>   : VLAN ID (1-4095)

port   : UDP/TCP port keyword

<udp_tcp_port> : Source or destination UDP/TCP port (0-65535)

dscp   : IP DSCP keyword

<dscp>   : IP DSCP (0-63)

tos   : IP ToS keyword

<tos_list>   : IP ToS list (0-7)

tag_prio   : VLAN tag priority keyword

<tag_prio_list>: VLAN tag priority list (0-7)

<class>   : Traffic class low/normal/medium/high or 1/2/3/4

QoS QCL Delete

Description:

Delete QCE.

Syntax:

QoS QCL Delete <qcl_id> <qce_id>

Parameters:

<qcl_id>: QCL ID

<qce_id>: QCE ID (1-24)

QoS QCL Lookup

Description:

Lookup QCE.

Syntax:

QoS QCL Lookup [<qcl_id>] [<qce_id>]

Parameters:

<qcl_id>: QCL ID

<qce_id>: QCE ID (1-24)

QoS Mode

Description:

Set or show the port egress scheduler mode.

Syntax:

QoS Mode [<port_list>] [strict|weighted]

Parameters:

<port_list>: Port list or 'all', default: All ports

strict   : Strict mode

weighted: Weighted mode

(default: Show QoS mode)

Default Setting:

 Strict

Example:

Set weighted mode for port15

```
SWITCH/>qos mode 15 weighted
```

QoS Weight

Description:

Set or show the port egress scheduler weight.

Syntax:

QoS Weight [<port_list>] [<class>] [<weight>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<class>   : Traffic class low/normal/medium/high or 1/2/3/4

<weight>   : Traffic class weight 1/2/4/8

QoS Rate Limiter

Description:

Set or show the port rate limiter.

Syntax:

QoS Rate Limiter [<port_list>] [enable|disable] [<bit_rate>]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable   : Enable rate limiter

disable   : Disable rate limiter

(default: Show rate limiter mode)

<bit_rate> : Rate in 1000 bits per second (500-1000000 kbps)

Default Setting:

Disabled, 500kbps

Example:

Set 1000kbps rate limiter for port17~24

SWITCH/>qos rate limiter 17-24 enable 1000

QoS Shaper

Description:

Set or show the port shaper.

Syntax:

QoS Shaper [<port_list>] [enable|disable] [<bit_rate>]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable   : Enable shaper

disable   : Disable shaper

(default: Show shaper mode)

<bit_rate> : Rate in 1000 bits per second (500-1000000 kbps)

Default Setting:

Disabled, 500kbps

Example:

Set 1000kbps shaper for port 9~16

```
SWITCH/>qos shaper 9-16 enable 1000
```

QoS Unicast

Description:

Set or show the unicast storm rate limiter.

Syntax:

QoS Storm Unicast [enable|disable] [<packet_rate>]

Parameters:

enable   : Enable unicast storm control

disable   : Disable unicast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable unicast storm rate limiter in 1kpps

```
SWITCH/>qos storm unicast enable 1k
```

QoS Multicast

Description:

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Multicast [enable|disable] [<packet_rate>]

Parameters:

enable   : Enable multicast storm control

disable   : Disable multicast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable multicast storm rate limiter in 1kpps

```
SWITCH/>qos storm multicast enable 1k
```

QoS Broadcast

Description:

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Broadcast [enable|disable] [<packet_rate>]

Parameters:

enable   : Enable broadcast storm control

disable   : Disable broadcast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable broadcast storm rate limiter in 1kpps

```
SWITCH/>qos storm broadcast enable 1k
```

6.8 802.1x Port Access Control Command

Dot1x Configuration

Description:

Show 802.1X configuration.

Syntax:

Dot1x Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show IEEE802.1x status of port1

```
SWITCH/>dot1x configuration 1

Mode           : Disabled

RADIUS Server  : 0.0.0.0

RADIUS Secret  :

Reauthentication: Disabled

Period         : 3600

Timeout        : 30

Age Period     : 300

Hold Time      : 10


Port    Admin State        Port State              Last Source       Last ID

------  -----------------  ----------------------  ----------------  -------

1       Authorized         802.1X Disabled          -                -
```

Dotx1 Mode

Description:

Set or show the 802.1X mode for the switch.

Syntax:

Dot1x Mode [enable|disable]

Parameters:

enable : Enable 802.1X

disable: Disable 802.1X

(default: Show 802.1X mode)

Default Setting:

Disable

Example:

Enable IEEE802.1x founction for port1

SWITCH/>dot1x mode enable

Dot1x Status

Description:

Set or show the 802.1X port state.

Syntax:

Dot1x State [<port_list>] [macbased|auto|authorized|unauthorized]

Parameters:

<port_list>: Port list or 'all', default: All ports

macbased   : Switch performs 802.1X authentication on behalf of the client

auto   : Port access requires 802.1X authentication

authorized   : Port access is allowed

unauthorized: Port access is not allowed

(default: Show 802.1X state)

Default Setting:

Authorized

Example:

Change IEEE802.1x mode in auto.

SWITCH/>dot1x state 1 auto

Dot1x Server

Description:

Set or show the RADIUS server IP address.

Syntax:

Dot1x Server [<ip_addr>]

Parameters:

ip_addr: RADIUS server IP address (a.b.c.d) (default: Show IP address)

Default Setting:

0.0.0.0

Example:

Set RADIUS server IP address for switch. RADIUS server IP address is 192.168.0.254.

SWITCH/>dot1x server 192.168.0.254

Dot1x Secret

Description:

Set or show the secret shared with the RADIUS server.

Syntax:

Dot1x Secret [<shared_secret>]

Parameters:

<shared_secret>: Secret shared with external RADIUS server. To set an empty secret, use two quotes (""). To use

spaces in secret, enquote the secret. Quotes in the secret are not allowed.

(default: Show shared secret)

Default Setting:

empty

Example:

Set authentication key "123abc@" in switch with the RADIUS server.

SWITCH/>dot1x secret 123abc@

Dot1x Authenticate

Description:

Refresh (restart) 802.1X authentication process.

Syntax:

Dot1x Authenticate [<port_list>] [now]

Parameters:

<port_list>: Port list or 'all', default: All ports

now   : Force reauthentication immediately

Dot1x Re-authentication

Description:

Set or show Reauthentication mode.

Syntax:

Dot1x Reauthentication [enable|disable]

Parameters:

enable : Enable reauthentication

disable: Disable reauthentication

(default: Show reauthentication mode)

Default Setting:

Disable

Example:

Enable re-authentication function

```
SWITCH/>dot1x reauthentication enable
```

Dot1x Period

Description:

Set or show the period between reauthentications.

Syntax:

Dot1x Period [<reauth_period>]

Parameters:

<reauth_period>: Period between reauthentications (1-3600 seconds)

(default: Show reauthentication period)

Default Setting:

3600

Example:

Set period re-authentication time in 3000 seconds

```
SWITCH/>dot1x period 3000
```

Dot1x Timeout

Description:

Set or show the time between EAPOL retransmissions.

Syntax:

Dot1x Timeout [<eapol_timeout>]

Parameters:

<eapol_timeout>: Time between EAPOL retransmissions (1-255 seconds)

(default: Show retransmission timeout)

Default Setting:

30

Example:

Set re-transmission time in 60 seconds

```
SWITCH/>dot1x timeout 60
```

Dot1x Statistics

Description:

Show 802.1X statistics.

Syntax:

Dot1x Statistics [<port_list>] [clear|eapol|radius]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear　　　　: Clear statistics

eapol　　　　 : Show EAPOL statistics

radius　　　　: Show RADIUS statistics

(default: Show all statistics)

Dot1x Clients

Description:

Set or show the maximum number of allowed clients for MAC-based ports.

Syntax:

Dot1x Clients [<port_list>] [all|<client_cnt>]

Parameters:

<port_list>　　　 : Port list or 'all', default: All ports

all|<client_cnt>: MAC-based authentication: Set maximum number of clients allowed on a port.

all　　　　　　 : Allow all new clients

<client_cnt>: A number >= 1

(default: Show current maximum)

Default Setting:

All

Dot1x Agetime

Description:

Time in seconds between check for activity on successfully authenticated MAC addresses.

Syntax:

Dot1x Agetime [<age_time>]

Parameters:

<age_time>: Time between checks for activity on a MAC address that succeeded authentication

(default: Show age time)

Default Setting:

300

Example:

Set age time in 100 seconds

```
SWITCH/>dot1x agetime 100
```

Dot1x Holdtime

Description:

Time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Syntax:

Dot1x Holdtime [<hold_time>]

Parameters:

<hold_time>: Hold time before MAC addresses that failed authentication expire

(default: Show hold time)

Default Setting:

10

Example:

Set hold time in 100 seconds

```
SWITCH/>dot1x holdtime 100
```

6.9 Access Control List Command

ACL Configuration

Description:

Show ACL Configuration.

Syntax:

ACL Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Default Setting:

300

Example:

Set age time in 100 seconds

```
SWITCH/>dot1x agetime 100
```

ACL Action

Description:

Set or show the ACL port default action.

Syntax:

ACL Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]

Parameters:

<port_list>   : Port list or 'all', default: All ports

permit   : Permit forwarding (default)

deny   : Deny forwarding

<rate_limiter>: Rate limiter number (1-15) or 'disable'

<port_copy>   : Port number for copy of frames or 'disable'

<logging>   : System logging of frames: log|log_disable

<shutdown>   : Shut down ingress port: shut|shut_disable

Default Setting:

Action: Permit

284

Rate Limiter: Disable

Port Copy: Disable

Loading: Disable

Shut down: Disable

Example:

????

```
SWITCH/>acl action 17-24 deny 1 24 log shut
```

ACL Policy

Description:

Set or show the ACL port policy.

Syntax:

ACL Policy [<port_list>] [<policy>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<policy>   : Policy number (1-8)

Default Setting:

1

Example:

Set policy ID 8 for port 17-24

```
SWITCH/>acl policy 17-24 8
```

ACL Rate

Description:

Set or show the ACL rate limiter.

Syntax:

ACL Rate [<rate_limiter_list>] [<packet_rate>]

Parameters:

<rate_limiter_list>: Rate limiter list (1-15), default: All rate limiters

<packet_rate>   : Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

1

Example:

???

SWITCH/>acl rate 15 1024k

ACL Add

Description:

Add or modify Access Control Entry (ACE).

If the ACE ID parameter <ace_id> is specified and an entry with this ACE ID already exists, the ACE will be modified.

Otherwise, a new ACE will be added. If the ACE ID is not specified, the next available ACE ID will be used.

If the next ACE ID parameter <ace_id_next> is specified, the ACE will be placed before this ACE in the list. If the next

ACE ID is not specified, the ACE will be placed last in the list.

If the Switch keyword is used, the rule applies to aSyntax:

ACL Add [<ace_id>] [<ace_id_next>] [switch | (port <port>) | (policy <policy>)] [<sid>] [<vid>] [<tag_prio>] [<dmac_type>]

[(etype [<etype>] [<smac>] [<dmac>]) | (arp   [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip   [<sip>]

[<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp   [<sip>] [<dip>]

[<sport>] [<dport>] [<ip_flags>]) | (tcp   [<sip>] [<dip>] [<sport>] [<dport>]Parameters:

<ace_id>   : ACE ID (1-1024), default: Next available ID

<ace_id_next> : Next ACE ID (1-1024), default: Add ACE last

switch   : Switch ACE keyword

port   : Port ACE keyword

<port>   : Port number

policy   : Policy ACE keyword

<policy>   : Policy number (1-8)

<sid>   : Switch ID (1-16) or 'any'

<vid>   : VLAN ID (1-4095) or 'any'

<tag_prio>   : VLAN tag priority (0-7) or 'any'

<dmac_type>   : DMAC type: any|unicast|multicast|broadcast

etype   : Ethernet Type keyword

<etype>   : Ethernet Type or 'any'

<smac>　　　　: Source MAC address (xx-xx-xx-xx-xx-xx) or 'any'

<dmac>　　　　 : Destination MAC address (xx-xx-xx-xx-xx-xx) or 'any'

arp　　　　: ARP keyword

<sip>　　　　: Source IP address (a.b.c.d/n) or 'any'

<dip>　　　　: Destination IP address (a.b.c.d/n) or 'any'

<arp_opcode>　 : ARP operation code: any|arp|rarp|other

<arp_flags>　 : ARP flags: request|smac|tmac|len|ip|ether [0|1|any]

ip　　　　: IP keyword

<protocol>　 : IP protocol number (0-255) or 'any'

<ip_flags>　 : IP flags: ttl|options|fragment [0|1|any]

icmp　　　 : ICMP keyword

<icmp_type>　 : ICMP type number (0-255) or 'any'

<icmp_code>　 : ICMP code number (0-255) or 'any'

udp　　　 : UDP keyword

<sport>　　 : Source UDP/TCP port range (0-65535) or 'any'

<dport>　　 : Destination UDP/TCP port range (0-65535) or 'any'

tcp　　　 : TCP keyword

<tcp_flags>　 : TCP flags: fin|syn|rst|psh|ack|urg [0|1|any]

permit　　 : Permit forwarding (default)

deny　　　 : Deny forwarding

<rate_limiter>: Rate limiter number (1-15) or 'disable'

<port_copy>　 : Port number for copy of frames or 'disable'

<logging>　　 : System logging of frames: log|log_disable

<shutdown>　 : Shut down ingress port: shut|shut_disable

ACL Delete

Description:

Delete ACE.

Syntax:

ACL Delete <ace_id>

Parameters:

<ace_id>: ACE ID (1-1024)

ACL Lookup

Description:

Show ACE, default: All ACEs.

Syntax:

ACL Lookup [<ace_id>]

Parameters:

<ace_id>: ACE ID (1-1024)

ACL Lookup

Description:

Clear all ACL counters.

Syntax:

ACL Clear

6.10 MAC Address Table Command

MAC Configuration

Description:

Show MAC address table configuration.

Syntax:

MAC Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show port1 Mac state

```
SWITCH/>mac configuration 1

MAC Age Time: 300


Switch 1:

---------


Port    Learning

------  ----------
1       Auto
```

Mac Add

Description:

Add MAC address table entry.

Syntax:

MAC Add <mac_addr> <port_list> [<vid>]

Parameters:

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)

<port_list>: Port list or 'all' or 'none'

<vid>   : VLAN ID (1-4095), default: 1

Example:

Add Mac address 00-30-4F-01-01-02 in port1 and vid1

```
SWITCH/>mac add 00-30-4f-01-01-02 1 1
```

MAC Delete

Description:

Delete MAC address entry.

Syntax:

MAC Delete <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

<vid>   : VLAN ID (1-4095), default: 1

Example:

Delete Mac address 00-30-4F-01-01-02 in vid1

```
SWITCH/>mac delete 00-30-4f-01-01-02 1
```

MAC Lookup

Description:

Lookup MAC address entry.

Syntax:

MAC Lookup <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

<vid>   : VLAN ID (1-4095), default: 1

Example:

Lookup state of Mac address 00-30-4F-01-01-02

```
SWITCH/>mac lookup 00-30-4f-01-01-02
```

MAC Age Time

Description:

Set or show the MAC address age timer.

Syntax:

MAC Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (10-1000000), default: Show age time

Default Setting:

300

Example:

Set agetime value in 30

```
SWITCH/>mac agetime 30
```

MAC Learning

Description:

Set or show the port learn mode.

Syntax:

MAC Learning [<port_list>] [auto|disable|secure]

Parameters:

<port_list>: Port list or 'all', default: All ports

auto   : Automatic learning

disable: Disable learning

secure : Secure learning

(default: Show learn mode)

Default Setting:

Auto

Example:

Set secure learning mode in port1

```
SWITCH/>mac learning 1 secure
```

MAC Dump

Description:

Show sorted list of MAC address entries.

Syntax:

MAC Dump [<mac_max>] [<mac_addr>] [<vid>]

Parameters:

<mac_max> : Maximum number of MAC addresses 1-8192, default: Show all addresses

<mac_addr>: First MAC address (xx-xx-xx-xx-xx-xx), default: MAC address zero

<vid> : First VLAN ID (1-4095), default: 1

Example:

Show all of MAC table

```
SWITCH/>mac dump
```

MAC Statistics

Description:

Show MAC address table statistics.

Syntax:

MAC Statistics [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Set all of MAC statistics

```
SWITCH/>mac statistics
```

MAC Flash

Description:

Flush all learned entries.

Syntax:

MAC Flush

6.11 LLDP Command

LLDP Configuration

Description:

Show LLDP configuration.

Syntax:

LLDP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

LLDP Mode

Description:

Set or show LLDP mode.

Syntax:

LLDP Mode [<port_list>]   [enable|disable|rx|tx]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable LLDP reception and transmission

disable: Disable LLDP

rx   : Enable LLDP reception only

tx   : Enable LLDP transmission only

(default: Show LLDP mode)

Default Setting:

Disable

Example:

Enable port1 LLDP function.

```
SWITCH/>lldp mode 1 enable
```

LLDP Optional TLV

Description:

Show / Set LLDP Optional TLVs.

Syntax:

LLDP Optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

port_descr   : Description of the port

sysm_name   : System name

sys_descr   : Description of the system

sys_capa   : System capabilities

mgmt_addr   : Master's IP address

(**default**: Show optional TLV's configuration)

enable   : Enables TLV

disable   : Disable TLV

(default: Show optional TLV's configuration)

Default Setting:

Description of the port: Enable

System name: Enable

Description of the system: Enable

System capabilities: Enable

Master's IP address: Enable

Example:

Disable description of the port for port1

```
SWITCH/>lldp optional_tlv 1 port_descr disable
```

LLDP Interval

Description:

Set or show LLDP Tx interval.

Syntax:

LLDP Interval [<interval>]

Parameters:

<interval>: LLDP transmission interval (5-32768)

Default Setting:

30

Example:

Set transmission interval in 10

```
SWITCH/>lldp interval 10
```

LLDP Hold

Description:

Set or show LLDP Tx hold value.

Syntax:

LLDP Hold [<hold>]

Parameters:

<hold>: LLDP hold value (2-10)

Default Setting:

3

Example:

Set LLDP hold value in 10

```
SWITCH/>lldp hold 10
```

LLDP Delay

Description:

Set or show LLDP Tx delay.

Syntax:

LLDP Delay [<delay>]

Parameters:

<delay>: LLDP transmission delay (1-8192)

Default Setting:

2

Example:

Set LLDP delay value in 1

```
SWITCH/>lldp delay 1
```

LLDP Reinit

Description:

Set or show LLDP reinit delay.

Syntax:

LLDP Reinit [<reinit>]

Parameters:

<reinit>: LLDP reinit delay (1-10)

Default Setting:

2

Example:

Set LLDP reinit delay value in 3

```
SWITCH/>lldp reinit 3
```

LLDP Information

Description:

Show LLDP neighbor device information.

Syntax:

LLDP Info [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

LLDP Statistics

Description:

Show LLDP Statistics.

Syntax:

LLDP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear   : Clear LLDP statistics

6.12 Stack Management Command

Stack List

Description:

Show the list of switches in stack.

Syntax:

Stack List [detailed|productinfo]

Parameters:

detailed: Show detailed information

Stack List

Description:

Set the master election priority.

Syntax:

Stack Master Priority <sid>|local <mst_elect_prio>

Parameters:

<sid>|local   : Switch ID (1-16) or local switch

<mst_elect_prio>: Master election priority: 1-4. 1 => Highest master probability

Example:

Set low priority for switch2

```
SWITCH/>stack master priority 2 4
```

Stack Master Reelect

Description:

Force master reelection (ignoring master time).

Syntax:

Stack Master Reelect

Stack Select

Description:

Set or show the selected switch ID.

Syntax:

Stack Select [<sid>|all]

Parameters:

<sid>: Switch ID (1-16), default: Show SID

Example:

Select switch2 to management switch2

```
SWITCH/>stack select 2
```

Stack SID Swap

Description:

Swap SID values used to identify two switches.

Syntax:

Stack SID Swap <sid> <sid>

Parameters:

<sid>: Switch ID (1-16)

Example:

Swap switch ID 1 and 2

```
SWITCH/>stack sid swap 2 1
```

Stack SID Delect

Description:

Delete SID assignment and associated configuration.

Syntax:

Stack SID Delete <sid>

Parameters:

<sid>: Switch ID (1-16)

Stack SID Asign

Description:

Assign SID and associated configuration to switch.

SID must be unassigned, switch must be present and switch must not already be assigned to a SID.

Syntax:

Stack SID Assign <sid> <mac_addr>

Parameters:

<sid>   : Switch ID (1-16)

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

Example:

Assign SID2 for switch that use MAC address 00-30-4f-24-04-76

SWITCH/>stack sid assign 2 00-30-4f-24-04-76

6.13 Power over Ethernet Command

PoE Configuration

Description:

Show PoE configuration.

Syntax:

PoE Configuration

Example:

```
SWITCH/>poe configuration

Port   Mode     Priority  Max.Power[W]   PowerAlloc[W]
----   -------  --------  --------------  -------------
1      Enabled  High      15.4            15.4
2      Enabled  High      15.4            15.4
3      Enabled  High      15.4            15.4
4      Enabled  High      15.4            15.4
5      Enabled  High      15.4            15.4
6      Enabled  High      15.4            15.4
7      Enabled  High      15.4            15.4
8      Enabled  High      15.4            15.4
9      Enabled  High      15.4            15.4
10     Enabled  High      15.4            15.4
11     Enabled  High      15.4            15.4
12     Enabled  High      15.4            15.4
13     Enabled  High      15.4            15.4
14     Enabled  High      15.4            15.4
15     Enabled  High      15.4            15.4
16     Enabled  High      15.4            15.4
17     Enabled  High      15.4            15.4
18     Enabled  High      15.4            15.4
19     Enabled  High      15.4            15.4
20     Enabled  High      15.4            15.4
21     Enabled  High      15.4            15.4
22     Enabled  High      15.4            15.4
23     Enabled  High      15.4            15.4
24     Enabled  High      15.4            15.4

Power Supply Max.
------------------
220 [W]

Power management mode
---------------------
Power management mode : automode
```

PoE Mode

Description:

Set or show PoE mode.

Syntax:

PoE Mode [<port_list>]   [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable   : Enables PoE

disable   : Disable PoE

(default: Show PoE's mode)

PoE Priority

Description:

Show / Set PoE Priority.

Syntax:

PoE Priority [<port_list>] [low|high|critical]

Parameters:

<port_list>: Port list or 'all', default: All ports

low   : Set priority to low

high   : Set priority to high

critival   : Set priority to critical

(default: Show PoE priority)

PoE Mgmt_mode

Description:

Show / Set PoE management mode.

Syntax:

PoE Mgmt_mode [mgt_class|mgt_alloc|mgt_auto|mgt_consumption|mgt_priority]

Parameters:

mgt_class : handle power allocation according to PD class

mgt_alloc :   power allocated according to values entered in power allocate

mgt_auto :   automatic mode , according to the sequence: class,allocation,consumption.

mgt_consumption : allocated according to PD actual need , with a maximum of 15.4 W per port

mgt_priority : max. port power determined by priority

(default: Show PoE power management mode)

Example:

```
SWITCH/> poe mgmt_mode

Power management mode
-----------------------------------
Power management mode : automode
```

PoE Maximum_Power

Description:

Set or show PoE maximum power per port (0-15.4, with one digit).

Syntax:

PoE Maximum_Power [<port_list>] [<port_power>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<port_power>: PoE maiximum power for the port (0-15.4)

PoE Alloc_Power

Description:

PoE Alloc_Power [<port_list>] [<alloc_power>].

Syntax:

PoE Mgmt_mode [mgt_class|mgt_alloc|mgt_auto|mgt_consumption|mgt_priority]

Parameters:

<port_list>   : Port list or 'all', default: All ports

<alloc_power>: PoE maiximum power allocated for the port (0-15.4)

PoE Power_Supply

Description:

Set or show the value of the power supply.

Syntax:

PoE Power_Supply [<supply_power>]

Parameters:

<supply_power>: PoE power for a power supply

PoE Status

Description:

Show PoE status.

Syntax:

PoE Status

Example:

```
SWITCH/> poe status

Port   Port Status          PD Class   Power Used [W]   Current Used [mA]
----   ------------------   --------   --------------   -------------------------
1      PoE ON               2          4.8              95
2      PoE OFF              0          0.0              0
3      PoE OFF              0          0.0              0
4      PoE OFF              0          0.0              0
5      PoE OFF              0          0.0              0
6      PoE OFF              0          0.0              0
7      PoE OFF              0          0.0              0
8      PoE OFF              0          0.0              0
9      PoE OFF              0          0.0              0
10     PoE OFF              0          0.0              0
11     PoE OFF              0          0.0              0
12     PoE OFF              0          0.0              0
13     PoE OFF              0          0.0              0
14     PoE OFF              0          0.0              0
15     PoE OFF              0          0.0              0
16     PoE OFF              0          0.0              0
17     PoE OFF              0          0.0              0
18     PoE OFF              0          0.0              0
19     PoE OFF              0          0.0              0
20     PoE OFF              0          0.0              0
21     PoE OFF              0          0.0              0
22     PoE OFF              0          0.0              0
23     PoE OFF              0          0.0              0
24     PoE OFF              0          0.0              0
Total                                  4.8              95

Current Power Consumption    4.8[W] (2%)
Total Power Reserved         7.268[W] (3%)
Temperature 1                37 (C) / 98 (F)
Temperature 2                43 (C) / 109 (F)
```

7. SWITCH OPERATION

7.1 Address Table

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

7.2 Learning

When one packet comes in from any port, the Switch will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

7.3 Forwarding & Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the Ethernet Switching will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

7.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The Ethernet Switch scans the destination address from the packet-header, searches the routing table pro-vided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. How-ever, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to signifi-cantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The Switch performs "Store and forward" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

7.5 Auto-Negotiation

The STP ports on the Switch have built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	100Base-TX port will set to:
10Mbps, no auto-negotiation	**10Mbps.**
10Mbps, with auto-negotiation	**10/20Mbps (10Base-T/Full-Duplex)**
100Mbps, no auto-negotiation	**100Mbps**
100Mbps, with auto-negotiation	**100/200Mbps (100Base-TX/Full-Duplex)**

8. POWER OVER ETHERNET OVERVIEW

What is PoE?

Based on the global standard IEEE 802.3af, PoE is a technology for wired Ethernet, the most widely installed local area network technology adopted today. PoE allows the electrical power necessary for the operation of each end-device to be carried by data cables rather than by separate power cords. New network applications, such as IP Cameras, VoIP Phones, and Wireless Networking, can help enterprises improve productivity. It minimizes wires that must be used to install the network for offering lower cost, and less power failures.

IEEE802.3af also called Data Terminal equipment (DTE) power via Media dependent interface (MDI) is an international standard to define the transmission for power over Ethernet. The 802.3af is delivering 48V power over RJ-45 wiring. Besides 802.3af also define two types of source equipment: Mid-Span and End-Span.

■ **Mid-Span**

Mid-Span device is placed between legacy switch and the powered device. Mid-Span is tap the unused wire pairs 4/5 and 7/8 to carry power, the other four is for data transmit.

■ **End-Span**

End-Span device is direct connecting with power device. End-Span could also tap the wire 1/2 and 3/6.

PoE System Architecture

The specification of PoE typically requires two devices: the **Powered Source Equipment (PSE)** and the **Powered Device (PD)**. The PSE is either an End-Span or a Mid-Span, while the PD is a PoE-enabled terminal, such as IP Phones, Wireless LAN, etc. Power can be delivered over data pairs or spare pairs of standard CAT-5 cabling.

How Power is Transferred Through the Cable

A standard CAT5 Ethernet cable has four twisted pairs, but only two of these are used for 10BASE-T and 100BASE-T. The specification allows two options for using these cables for power, shown in Figure 2 and Figure 3:

The spare pairs are used. Figure 2 shows the pair on pins 4 and 5 connected together and forming the positive supply, and the pair on pins 7 and 8 connected and forming the negative supply. (In fact, a late change to the spec allows either polarity to be used).
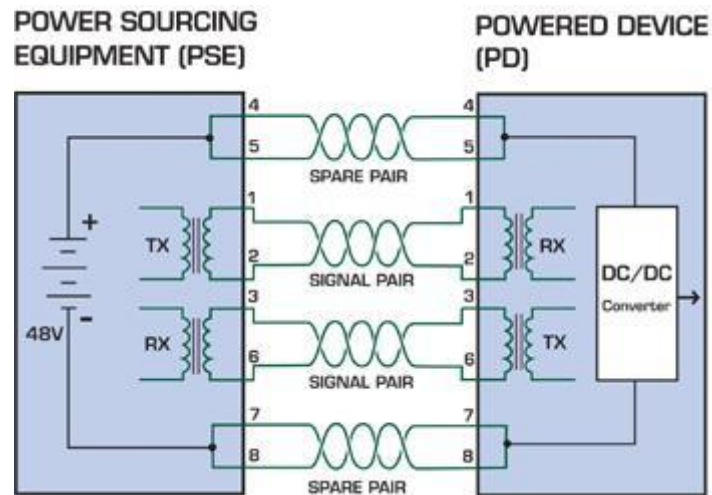
Figure 1 - Power Supplied over the Spare Pins

The data pairs are used. Since Ethernet pairs are transformer coupled at each end, it is possible to apply DC power to the center tap of the isolation transformer without upsetting the data transfer. In this mode of operation the pair on pins 3 and 6 and the pair on pins 1 and 2 can be of either polarity.
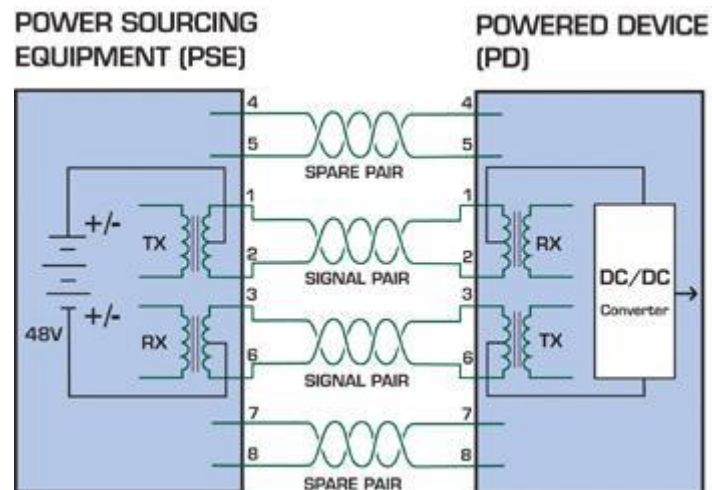
Figure 2 - Power Supplied over the Data Pins

When to install PoE?
Consider the following scenarios:

- • You're planning to install the latest VoIP Phone system to minimize cabling building costs when your company moves into new offices next month.

- • The company staff has been clamoring for a wireless access point in the picnic area behind the building so they can work on their laptops through lunch, but the cost of electrical power to the outside is not affordable.

- • Management asks for IP Surveillance Cameras and business access systems throughout the facility, but they would rather avoid another electrician's payment.

References:

IEEE Std 802.3af-2003 (Amendment to IEEE Std 802.3-2002, including IEEE Std 802.3ae-2002), 2003 Page(s):0_1-121

White Paper on Power over Ethernet (IEEE802.3af)

http://www.poweroverethernet.com/articles.php?article_id=52

Microsemi /PowerDsine

http://www.microsemi.com/PowerDsine/

Linear Tech

http://www.linear.com/

The PoE Provision Process

While adding PoE support to networked devices is relatively painless, it should be realized that power cannot simply be transferred over existing CAT-5 cables. Without proper preparation, doing so may result in damage to devices that are not designed to support provision of power over their network interfaces.

The PSE is the manager of the PoE process. In the beginning, only small voltage level is induced on the port's output, till a valid PD is detected during the Detection period. The PSE may choose to perform classification, to estimate the amount of power to be consumed by this PD. After a time-controlled start-up, the PSE begins supplying the 48 VDC level to the PD, till it is physically or electrically disconnected. Upon disconnection, voltage and power shut down.

Since the PSE is responsible for the PoE process timing, it is the one generating the probing signals prior to operating the PD and monitoring the various scenarios that may occur during operation.

All probing is done using voltage induction and current measurement in return.

Stages of powering up a PoE link

Stage	Action	Volts specified per 802.3af	Volts managed by chipset
Detection	Measure whether powered device has the correct signature resistance of 15–33 kΩ	2.7-10.0	1.8–10.0
Classification	Measure which power level class the resistor indicates	14.5-20.5	12.5–25.0
Startup	Where the powered device will startup	>42	>38
Normal operation	Supply power to device	36-57	25.0–60.0

Line Detection

Before power is applied, safety dictates that it must first be ensured that a valid PD is connected to the PSE's output. This process is referred to as "line detection", and involves the PSE seeking a specific, 25 KΩ signature resistor. Detection of this signature indicates that a valid PD is connected, and that provision of power to the device may commence.

The signature resistor lies in the PD's PoE front-end, isolated from the rest of the the PD's circuitries till detection is certified.

Classification

Once a PD is detected, the PSE may optionally perform classification, to determine the maximal power a PD is to consume. The PSE induces 15.5-20.5 VDC, limited to 100 mA, for a period of 10 to 75 ms responded by a certain current consumption by the PD, indicating its power class.

The PD is assigned to one of 5 classes: 0 (default class) indicates that full 15.4 watts should be provided, 1-3 indicate various required power levels and 4 is reserved for future use. PDs that do not support classification are assigned to class 0. Special care must be employed in the definition of class thresholds, as classification may be affected by cable losses.

Classifying a PD according to its power consumption may assist a PoE system in optimizing its power distribution. Such a system typically suffers from lack of power resources, so that efficient power management based on classification results may reduce total system costs.

Start-up

Once line detection and optional classification stages are completed, the PSE must switch from low voltage to its full voltage capacity (44-57 Volts) over a minimal amount of time (above 15 microseconds).

A gradual startup is required, as a sudden rise in voltage (reaching high frequencies) would introduce noise on the data lines.

Once provision of power is initiated, it is common for inrush current to be experienced at the PSE port, due to the PD's input capacitance. A PD must be designed to cease inrush current consumption (of over 350 mA) within 50 ms of power provision startup.

Operation

During normal operation, the PSE provides 44-57 VDC, able to support a minimum of 15.4 watts power.

*Power Overload*s

The IEEE 802.3af standard defines handling of overload conditions. In the event of an overload (a PD drawing a higher power level than the allowed 12.95 Watts), or an outright short circuit caused by a failure in cabling or in the PD, the PSE must shut down power within 50 to 75 milliseconds, while limiting current drain during this period to protect the cabling infrastructure. Immediate voltage drop is avoided to prevent shutdown due to random fluctuations.

Power Disconnection Scenarios

The IEEE 802.3af standard requires that devices powered over Ethernet be disconnected safely (i.e. power needs be shut down within a short period of time following disconnection of a PD from an active port).

When a PD is disconnected, there is a danger that it will be replaced by a non-PoE-ready device while power is still on. Imagine disconnecting a powered IP phone utilizing 48 VDC, then inadvertently plugging the powered Ethernet cable into a non-PoE notebook computer. What's sure to follow is not a pretty picture.

The standard defines two means of disconnection, DC Disconnect and AC Disconnect, both of which provide the same

functionality - the PSE shutdowns power to a disconnected port within 300 to 400ms. The upper boundary is a physical human limit for disconnecting one PD and reconnecting another.

DC Disconnect

DC Disconnect detection involves measurement of current. Naturally, a disconnected PD stops consuming current, which can be inspected by the PSE. The PSE must therefore disconnect power within 300 to 400 ms from the current flow stop. The lower time boundary is important to prevent shutdown due to random fluctuations.

AC Disconnect

This method is based on the fact that when a valid PD is connected to a port, the AC impedance measured on its terminals is significantly lower than in the case of an open port (disconnected PD).

AC Disconnect detection involves the induction of low AC signal in addition to the 48 VDC operating voltage. The returned AC signal amplitude is monitored by the PSE at the port terminals. During normal operation, the PD's relatively low impedance lowers the returned AC signal while a sudden disconnection of this PD will cause a surge to the full AC signal level and will indicate PD disconnection.

9. TROUBLE SHOOTING

This chapter contains information to help you solve problems. If the Ethernet Switch is not functioning properly, make sure the Ethernet Switch was set up according to instructions in this manual.

■ **The Link LED is not lit**

Solution:

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

■ **100Base-TX port link LED is lit, but the traffic is irregular**

Solution:

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

■ **Switch does not power up**

Solution:

1. AC power cord not inserted or faulty
2. Check 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

■ **Stacking not functioning**

Solution:

1. Check that modules are installed correctly

2. PLANET CB-STX50 or CB-STX200 cables not installed correctly (LEDs on front panel STX1 or STX2 do not light)

3. Check that the cables are inserted correctly

4. The stack cable is PLANET proprietary stack cable, the stack cable is cross-overed HDMI-like cable, the normal HDMI cable can't be used for the SGSW series.

■ **While IP Address be changed or forgotten admin password** –

To reset the IP address to the default IP Address "192.168.0.100" or reset the password to default value. Press the hardware **reset button** at the front panel about **10 seconds.** After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.
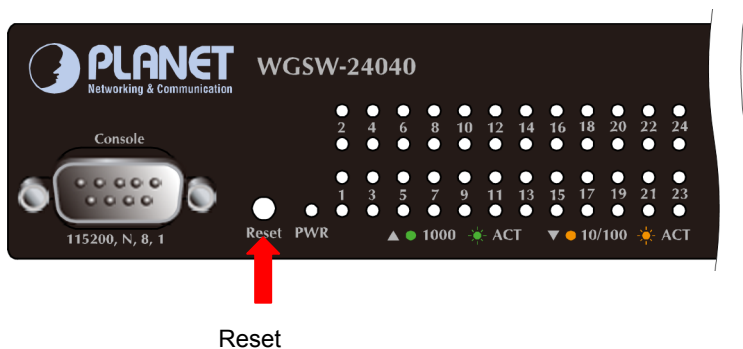
Reset

■ **No Power Forward**

Solution:

1. Make sure your PD device comply with IEEE 802.3af standard, the SGSW-24040P PoE switch only support the IEEE 802.3af compliant PD.

2. The POE switch uses the signal power pair to forward power, the data and the power is traverse the pin. Please, check the documentation for your PD device to make sure the power pair it uses. The following table is the signal power pair RJ-45 port pinout.

Pin	Signal / Name
1	RX+ / VCC -
2	RX- / VCC -
3	TX+ / VCC +
4	NC
5	NC
6	TX- / VCC +
7	NC
8	NC

APPENDEX A

A.1 Switch's RJ-45 Pin Assignments

1000Mbps, 1000Base T

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

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

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

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	MDI Media Dependant Interface	MDI-X Media Dependant Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

The standard cable, RJ-45 pin assignment
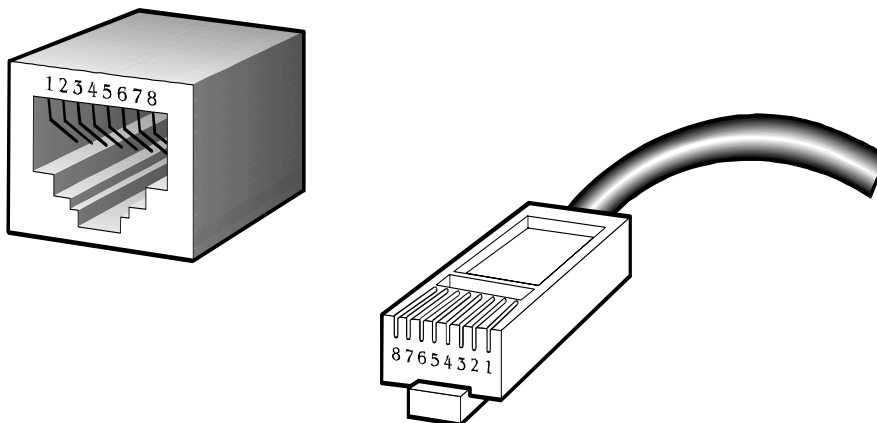
The standard RJ-45 receptacle/connector

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

	SIDE 1	SIDE2
Straight Cable		
SIDE 1	1 = White / Orange	1 = White / Orange
1 2 3 4 5 6 7 8	2 = Orange	2 = Orange
	3 = White / Green	3 = White / Green
	4 = Blue	4 = Blue
	5 = White / Blue	5 = White / Blue
	6 = Green	6 = Green
1 2 3 4 5 6 7 8	7 = White / Brown	7 = White / Brown
SIDE 2	8 = Brown	8 = Brown
	SIDE 1	SIDE2
Crossover Cable		
SIDE 1	1 = White / Orange	1 = White / Green
1 2 3 4 5 6 7 8	2 = Orange	2 = Green
	3 = White / Green	3 = White / Orange
	4 = Blue	4 = Blue
	5 = White / Blue	5 = White / Blue
	6 = Green	6 = Orange
1 2 3 4 5 6 7 8	7 = White / Brown	7 = White / Brown
SIDE 2	8 = Brown	8 = Brown

Figure A-1: Straight-Through and Crossover Cable

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

APPENDEX 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.

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.

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.

D

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.

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

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.

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, is used for network discovery, and works by having the units in the network exchanging information with their neighbors using LLDP frames.

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.

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.

N

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.

O

Optional TLVs.

A LLDP frame contains multiple TLVs

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

P

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.

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.

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.

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.

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.

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.

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.

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 obsoleted by RSTP.

Switch ID

Switch IDs (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

T

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.

ToS

ToS is an acronym for **T**ype **of** **S**ervice. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully

decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV (TLV is short for "Type Length Value").

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).

User Priority

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

V

VLAN

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

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

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

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

VLAN ID

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

EC Declaration of Conformity

For the following equipment:

*Type of Product: 24-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch
*Model Number: WGSW-24040 / WGSW-24040R / SGSW-24040 / SGSW-24040R

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

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (89/336/EEC).
For the evaluation regarding the EMC, the following standards were applied:

Emission	EN 55022	(1998/A1 + 2000/A2:2003 Class A)
Harmonic	EN 61000-3-2	(2006)
Flicker	EN 61000-3-3	(1995/A1: 2001/A2:2005)
Immunity	EN 55024	(1998/A1: 2001/A2:2003)
ESD	IEC 61000-4-2	(2001)
RS	IEC 61000-4-3	(2002)
EFT/ Burst	IEC 61000-4-4	(2004)
Surge	IEC 61000-4-5	(2001)
CS	IEC 61000-4-6	(2003) + A1 (2004)
Magnetic Field	IEC 61000-4-8	(2001)
Voltage Disp	IEC 61000-4-11	(2004)

Responsible for marking this declaration if the:

☒ **Manufacturer**   ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname   **Kent Kang**

Position / Title :   **Product Manager**

Taiwan   **29th Aug, 2008**   _____
Place   *Date*   *Legal Signature*

PLANET TECHNOLOGY CORPORATION

EC Declaration of Conformity

For the following equipment:

*Type of Product: 24 100/1000 SFP Slots with 8 Shared TP Managed Stackable Switch
*Model Number: SGSW-24240 / SGSW-24240R

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

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (89/336/EEC).
For the evaluation regarding the EMC, the following standards were applied:

Emission	EN 55022	(1998/A1 + 2000/A2:2003 Class A)
Harmonic	EN 61000-3-2	(2006)
Flicker	EN 61000-3-3	(1995/A1: 2001/A2:2005)
Immunity	EN 55024	(1998/A1: 2001/A2:2003)
ESD	IEC 61000-4-2	(2001)
RS	IEC 61000-4-3	(2002)
EFT/ Burst	IEC 61000-4-4	(2004)
Surge	IEC 61000-4-5	(2001)
CS	IEC 61000-4-6	(2003) + A1 (2004)
Magnetic Field	IEC 61000-4-8	(2001)
Voltage Disp	IEC 61000-4-11	(2004)

Responsible for marking this declaration if the:

☒ **Manufacturer**   ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname   **Kent Kang**

Position / Title :   **Product Manager**

Taiwan   **1ˢᵗ July, 2009**   _____
Place   *Date*   *Legal Signature*

PLANET TECHNOLOGY CORPORATION