PLANET
Networking & Communication

User's Manual

WGSW-28040

28-Port 10/100/1000Mbps with
4 Shared SFP
Managed Gigabit Switch

WGSW-28040P

24-Port 10/100/1000Mbps PoE
+ 4-Port Gigabit TP/SFP Combo
Managed Switch

Trademarks

Disclaimer

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

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

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

FCC Warning

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

CE Mark Warning

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

Energy Saving Note of the Device

This power required device does not support Standby mode operation.

For energy saving, please remove the power cable to disconnect the device from the power circuit.

Without removing power cable, the device will still consuming power from the power source. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

WEEE Warning

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

Revision

PLANET 28-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch User's Manual

FOR MODELS: WGSW-28040 / WGSW-28040P

REVISION: 1.2 (Sept.2011)

Part No: EM-WGSW-28040_28040P (2080-A93230-000)

TABLE OF CONETNTS

1. INTRODUTION

Thank you for purchasing PLANET Layer 2 Managed Switch, WGSW-28040 series. Terms of "**Managed Switch**" means the Switches mentioned titled in the cover page of this user's manual, i.e. WGSW-28040 and WGSW-28040P.

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

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

Cost-effective IPv6 Managed Gigabit Switch solution for SMB

Nowadays, lots of electronic products or mobile devices can browse the Internet, which means the need of IP Address increases. However, the current IPv4 network infrastructure is not capable enough to provide IP Address to each single users/Clients. The situation forces the ISP to build up the **IPv6 (Internet Protocol version 6)** network infrastructure speedily. To fulfill the demand, PLANET releases the **IPv6 management Gigabit Ethernet Switch**, WGSW-28040 series Managed Switch. It supports both IPv4 and IPv6 management functions. It can work with original network structure (IPv4) and also support the new network structure (IPv6) in the future. With easy and friendly management interfaces and plenty of management functions included, the WGSW-28040 series Managed Switch is the best choice for ISP to build the IPv6 FTTx edge service and for SMB to connect with IPv6 network.

High-Performance, Cost-effective Gigabit Networking Solution for SMB

The PLANET WGSW-28040 series is a Layer 2 Managed Gigabit Switch which can handle extremely large amounts of data in a secure topology linking to an Enterprise backbone or high capacity network server with 56Gbps switching fabric. The advanced features of QoS and network security included enable the WGSW-28040 series to offer effective data traffic control for SMB and Enterprises, such as VoIP, video streaming and multicast applications. It is ideal for the enterprise networks and the aggregation layer of IP metropolitan networks.

High Performance

The WGSW-28040 series provides 28 10/100/1000Mbps Gigabit Ethernet ports in which with 4 shared Gigabit SFP slots. It boasts high performance architecture of switch that is capable for providing the non-blocking switch fabric and wire-speed throughput as high as 56Gbps, which greatly simplifies the tasks of upgrading the LAN for catering to increasing bandwidth demands.

Robust Layer 2 Features

The WGSW-28040 series can be programmed for advanced switch management functions such as dynamic Port link aggregation, Q-in-Q VLAN, private VLAN, Multiple Spanning Tree protocol, Layer 2 QoS, bandwidth control and IGMP Snooping. The WGSW-28040 series provides 802.1Q Tagged VLAN, and the VLAN groups allowed will be maximally up to 255. Via aggregation of supporting ports, the WGSW-28040 series allows the operation of a high-speed trunk combining multiple ports. It enables maximum up to 8 groups of 8 ports for trunking and supports fail-over as well.

Excellent Traffic Control

The WGSW-28040 series is loaded with Port speed configuration, Port aggregation, VLAN, Spanning Tree protocol, QoS, bandwidth control and IGMP Snooping features to enhance services to business-class data, voice, security, and wireless solutions. The functionality includes QoS features, and bandwidth limiting that are particular useful for multi-tenant unit and multi-business unit applications. It also empowers the enterprises to take full advantages of the limited network resources and guarantees the best performance in VoIP and Video conferencing transmission.

Efficient Management

For efficient management, the WGSW-28040 series Managed Ethernet Switch is equipped with console, WEB and SNMP management interfaces. With the built-in Web-Based management interface, the WGSW-28040 series offers an easy-to-use, platform-independent management and configuration facility. The WGSW-28040 supports standard Simple Network Management Protocol (SNMP) and can be managed via any standard management software. For text-based management, the WGSW-28040 series can be accessed via Telnet and the console port.

Powerful Security

PLANET WGSW-28040 series offers comprehensive Layer 2 to Layer 4 Access Control List (ACL) for enforcing security to the edge. It can be used to restrict network access by denying packets based on source and destination IP address, TCP/UDP ports or defined typical network applications. Its protection mechanism also comprises of 802.1X port-based and MAC-based user and device authentication. With the private VLAN function, communication between edge ports can be prevented to ensure user privacy. The network administrators can now construct highly secured corporate networks with considerably less time and effort than before.

Power over Ethernet, Easy Cabling Installation

The PoE in-line power following the standard **IEEE 802.3af** makes the WGSW-28040P able to power on 24 PoE compliant devices at the distance up to 100 meters through the 4-pair Cat 5/5e UTP wire. With data and power over Ethernet from one unit, it can easily build a power central-controlled IP phone system, IP Camera system, or wireless AP group for the enterprises. The WGSW-28040P shall reduce cables deployment and eliminates the need for dedicated electrical outlets on

the wall, ceiling or any unreachable place. A wire carries both data and power lowering the installation costs, simplifying the installation effort and eliminating the need for electricians or extension cords.

Flexibility and Extension Solution

The four mini-GBIC slots built in the WGSW-28040 series are compatible with 1000Base-SX/LX and WDM SFP (Small Form Factor Pluggable) fiber-optic modules. The distance can be extended from 550 meters (Multi-Mode fiber) up to above 10/20/30/40/50/70/120 kilometers (Single-Mode fiber or WDM fiber). It is well suited for applications within the enterprise data centers and distributions.

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, **INSTALLATION**

The section explains the functions of the 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, **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-28040

- **28-Port 10/100/1000Base-T** Gigabit RJ-45 copper
- **4 1000Base-X** mini-GBIC/SFP slots, shared with Port-25 to Port-28
- **RS-232** DB9 console interface for Switch basic management and setup

WGSW-28040P

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

- **4 1000Base-X** mini-GBIC/SFP slots, shared with Port-25 to Port-28
- **RS-232** DB9 console interface for Switch basic management and setup

➢ **Layer 2 Features**

- Prevents packet loss with back pressure (Half-Duplex) and IEEE 802.3x PAUSE frame flow control (Full-Duplex)
- High performance of Store-and-Forward architecture and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
- Supports **VLAN**
  - IEEE 802.1Q Tagged VLAN
  - Up to 256 VLANs groups, out of 4094 VLAN IDs
  - Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
  - Private VLAN Edge (PVE / Port Isolation)
- Supports **Spanning Tree Protocol**
  - STP, IEEE 802.1D (Spanning Tree Protocol)
  - RSTP, IEEE 802.1w (Rapid Spanning Tree Protocol)
  - MSTP, IEEE 802.1s Multiple Spanning Tree Protocol, spanning tree by VLAN
- Supports **Link Aggregation**
  - IEEE 802.3ad Link Aggregation Control Protocol (LACP)
  - Cisco ether-channel (Static Trunk)
  - Maximum 8 trunk groups, up to 8 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**

- Ingress / Egress Rate Limit per port bandwidth control
- 8 priority queues on all switch ports
- Traffic classification:
  - Port-Based priority
  - IEEE 802.1p CoS
  - IP DSCP
- Strict priority and Weighted Round Robin (WRR) CoS policies
- DSCP remarking

- **Multicast**
  - Supports IGMP Snooping v1, v2 and v3
  - Querier mode support
  - IGMP Snooping v2 fast leave
  - Unknown Multicast drop

- **Security**
  - Storm Control support
    - Broadcast / Multicast / Unknown-Unicast / Unknown-Multicast
  - Authentication
    - IEEE 802.1X Port-Based network access authentication
    - Built-in RADIUS client to co-operate with the RADIUS servers
  - Access Control List
    - IP-Based ACL
    - MAC-Based ACL
  - MAC Security
    - Static MAC
    - Source / Destination MAC Filtering
    - Port Security for Source MAC address entries filtering

- **Management**
  - Switch Management Interfaces
    - Console / Telnet Command Line Interface
    - IPv4 and IPv6 Web switch management
    - SNMP v1, v2c switch management
    - SSH / SSL secure access
  - Four RMON groups (history, statistics, alarms, and events)
  - SNMP trap for interface Link Up and Link Down notification
  - SNTP (Simple Network Time Protocol)
  - Built-in Trivial File Transfer Protocol (TFTP) client
  - BOOTP and DHCP for IP address assignment
  - Firmware upload/download via HTTP / TFTP
  - Event message logging to remote Syslog server
  - Reset button for system reboot or reset to factory default

➢ **Power over Ethernet** (WGSW-28040P Only)

- Complies with IEEE 802.3af Power over Ethernet End-Span PSE
- Up to 24 ports for IEEE 802.3af / at 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
- Per port PoE function enable/disable

1.5 Product Specification

Product	WGSW-28040	WGSW-28040P
Hardware Specification		
Copper Ports	28 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports	
SFP/mini-GBIC Slots	4 1000Base-X SFP interfaces, shared with Port-25 to Port-28	
Switch Processing Scheme	Store-and-Forward	
Switch Fabric	56Gbps / non-blocking	
Throughput @ 64Kbytes	41.67Mpps	
MAC Address Table	16K entries	
Share Data Buffer	448K bytes	
Flow Control	IEEE 802.3x Pause Frame for Full-Duplex Back pressure for Half-Duplex	
Jumbo Frame	9216 Bytes	
LED	PWR, SYS, LNK/ACT, 1000	PWR, SYS, LNK/ACT, PoE In-Use, 1000, PWR Alert, FAN 1 & 2 Alert
Dimension (W x D x H)	440 x 200 x 44.5 mm, 1U height	440 x 300 x 44.5 mm, 1U height
Weight	2.7kg	3.9kg
Power Consumption	Max. 12 Watts / 40.92 BTU	Max. 202 Watts / 688.82 BTU
Power Requirement	AC 100~240V, 50/60Hz	
ESD Protection	6KV DC	
Power over Ethernet		
PoE Standard	-	IEEE 802.3af PoE / PSE
PoE Power Supply Type	-	End-Span
PoE Power Output	-	Per Port 48V DC. Max. 15.4 watts
Power Pin Assignment	-	1/2(+), 3/6(-)
PoE Power Budget	-	180 Watts

PoE Ability	**Number of PD @ 7Watts**	-	24
	Number of PD @ 15.4Watts	-	11
Layer 2 Function			
Basic Management Interfaces		Console, Telnet, IPv4 & IPv6 Web Browser, SNMPv1, v2c	
Security Management Interfaces		SSH, SSL	
Port Configuration		Port disable / enable Auto-Negotiation 10/100/1000Mbps full and half duplex mode selection Flow Control disable / enable Port Description	
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 Q-in-Q Up to 256 VLAN groups, out of 4094 VLAN IDs	
Link Aggregation		IEEE 802.3ad LACP / Static Trunk Supports 8 groups of 8-Port trunk support	
QoS		• 8-Level priority queue for switching • Traffic classification based, Strict priority and WRR - 802.1p priority - IP DSCP field	
IGMP Snooping		IGMP (v1/v2/v3) 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 2819 RMON MIB (Group 1) RFC 2737 Entity MIB RFC 3411 SNMP-MIB	
Standards Conformance			
Regulation Compliance		FCC Part 15 Class A, CE	

Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control IEEE 802.3ad Port trunk with LACP IEEE 802.1D Spanning tree protocol IEEE 802.1w Rapid spanning tree protocol IEEE 802.1s Multiple spanning tree protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.3af Power over Ethernet
Environment	
Operating	Temperature: 0 ~ 50 Degree C Relative Humidity: 20 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 70 Degree C Relative Humidity: 20 ~ 95% (non-condensing)

2. INSTALLATION

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

2.1 Hardware Description

2.1.1 Switch Front Panel

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

WGSW-28040 Front Panel

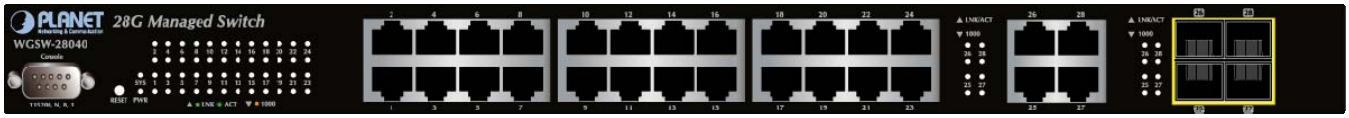


Figure 2-1 WGSW-28040 front panel

WGSW-28040P Front Panel

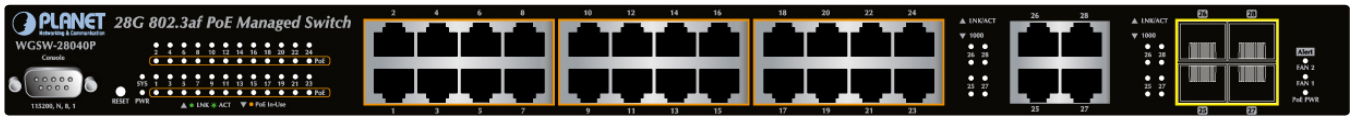


Figure 2-2 WGSW-28040P front panel

■ **Gigabit TP Interface**

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

■ **Gigabit SFP Slots**

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

■ **Console Port**

The console port is a DB9, RS-232 male serial 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 startup screen of the device.

■ **ResetButton**

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

2.1.2 LED Indications

The front panel LEDs indicates instant status of port links, data activity and system power; helps monitor and troubleshoot when needed. Figure 2-3 & Figure 2-4 shows the LED indications of these Managed Switch.

WGSW-28040 LED indication

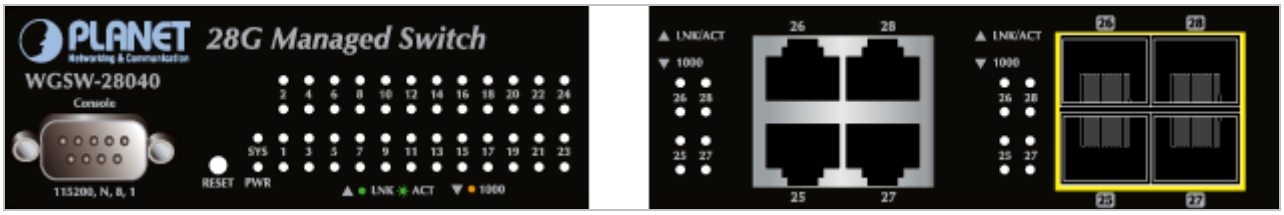


Figure 2-3 WGSW-28040 LED panel

■ **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate that the Switch has power.
SYS	**Green**	**Lights** to indicate the system is working.

■ **10/100/1000Base-T interfaces**

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

		Off:	If LNK/ACT LED light-> indicate that the port is operating at **10/100Mbps** If LNK/ACT LED Off -> indicate that the port is link down

■ **1000Base-SX/LX SFP interfaces (shared with Port-25 to Port-28)**

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

WGSW-28040P LED indication

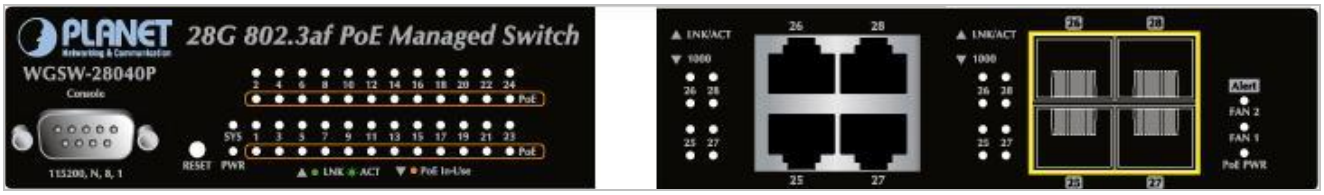


Figure 2-4 WGSW-28040P LED panel

■ **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate that the Switch has power.
SYS	**Green**	**Lights** to indicate the system is working.

■ **10/100/1000Base-T interfaces**

LED	Color	Function	
LNK/ACT	**Green**	**Lights**: **Blink:**	To indicate the link through that port is successfully established. To indicate that the switch is actively sending or receiving data over that port.
PoE In-Use	**Orange**	**Lights**: **Off:**	To indicate the port is providing 48VDC in-line power. To indicate the connected device is not a PoE Powered Device (PD)

■ **1000Base-SX/LX SFP interfaces (shared with Port-25 to Port-28)**

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

		Off:	If LNK/ACT LED light-> indicate that the port is operating at **100Mbps** If LNK/ACT LED Off -> indicate that the port is link down

■ **Alert**

LED	Color	Function
PoE PWR	**Green**	**Lights** to indicate that the power supply failure
FAN1	**Green**	**Lights** to indicate that the FAN1 failure
FAN2	**Green**	**Lights** to indicate that the FAN2 failure

2.1.3 Switch Rear Panel

The rear panel of the Managed Switch indicates an AC inlet power socket, which accepts input power from 100 to 240V AC, 50-60Hz. Figure 2-5 & Figure 2-6 shows the rear panel of these Managed Switches

WGSW-28040 Rear Panel

Figure 2-5 Rear panel of WGSW-28040

WGSW-28040P Rear Panel

Figure 2-6 Rear panel of WGSW-28040P

■ **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 100-240V AC 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.

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 2-7.

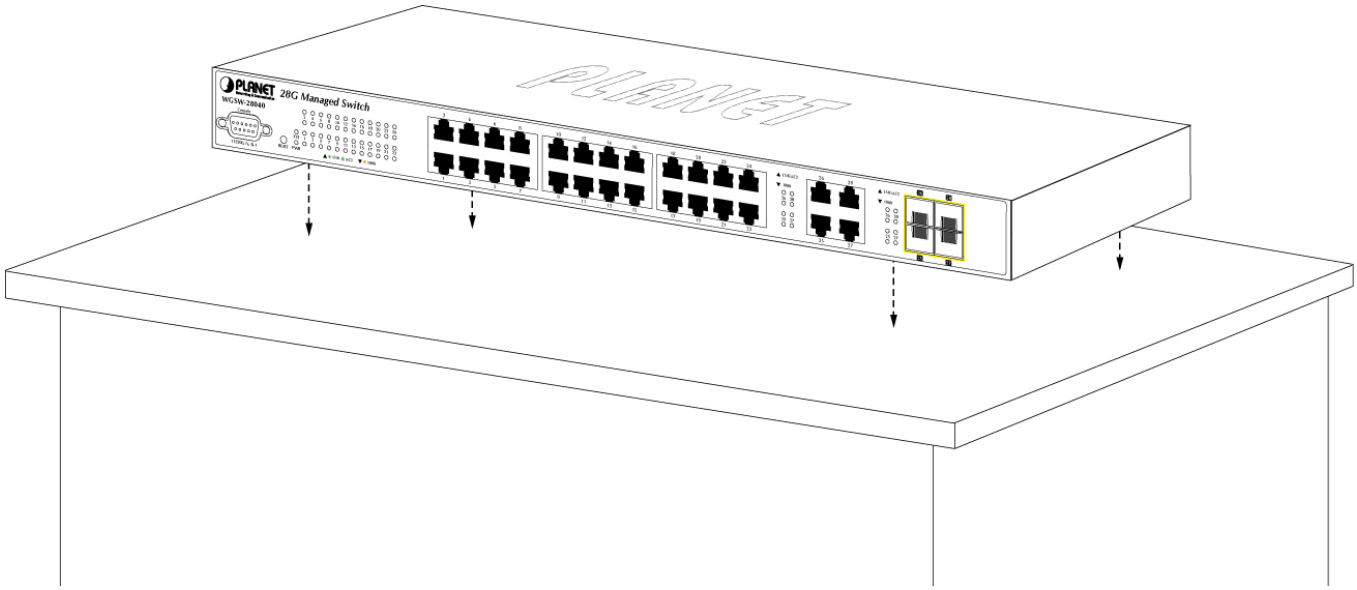


Figure 2-7 Place the Managed Switch on the desktop

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 2-8 shows how to attach brackets to one side of the Managed Switch.

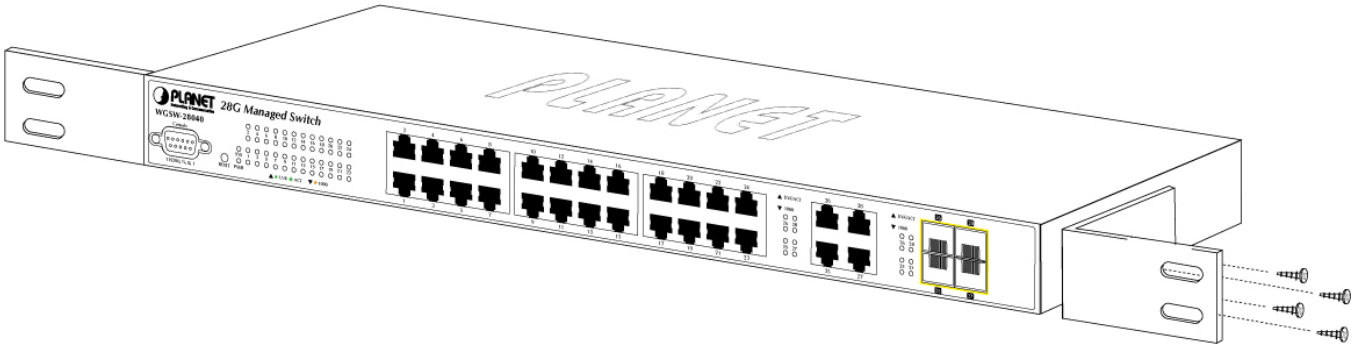


Figure 2-8 Attach brackets to the Managed Switch

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 2-9.

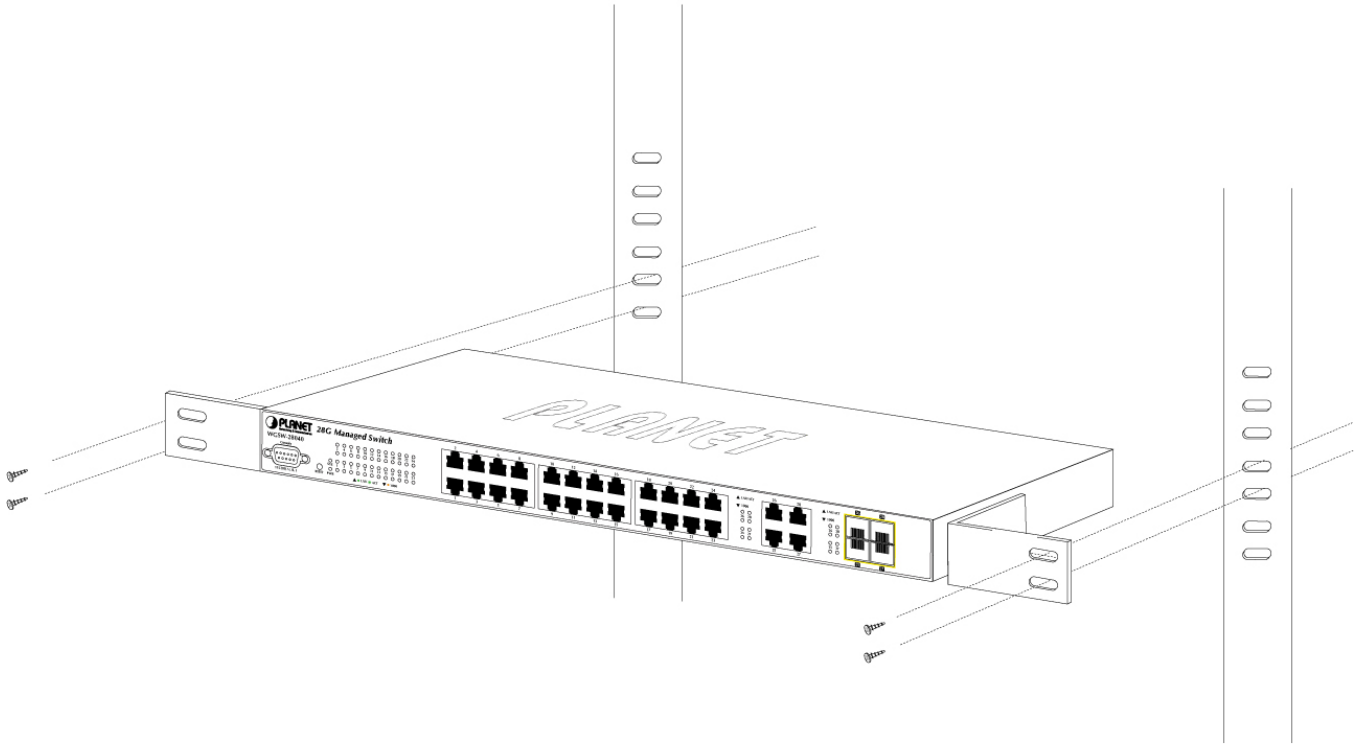


Figure 2-9 Mounting Managed Switch in a Rack

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 2-10 appears.

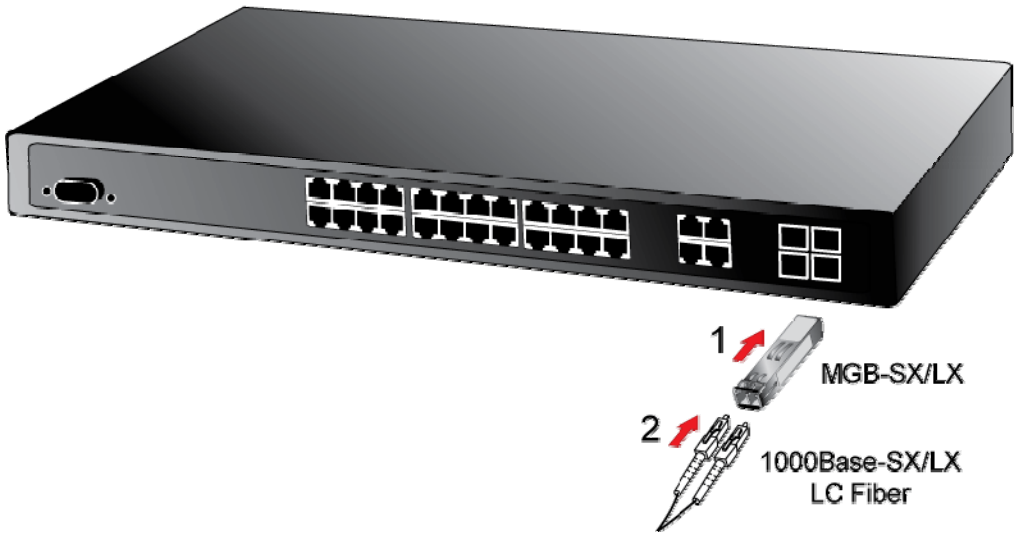


Figure 2-10 Plug-in the SFP transceiver

■ 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 or 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)

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.

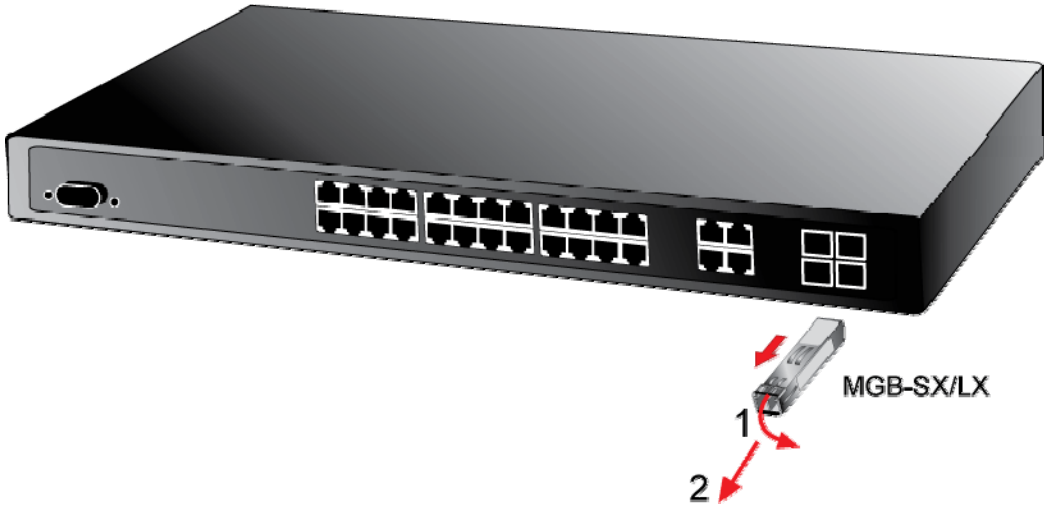


Figure 2-11 Pull out the SFP transceiver

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.

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 (DB9 / 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 **JAVA runtime environment** Plug-in

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

3.2 Management Access Overview

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

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

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

Method	Advantages	Disadvantages
Console	• No IP address or subnet needed • Text-based • Telnet functionality and 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**

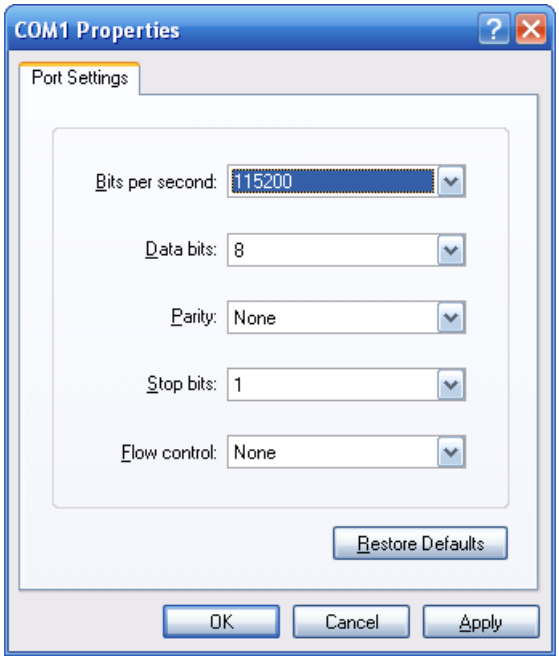


Figure 3-2 Terminal parameter settings

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.

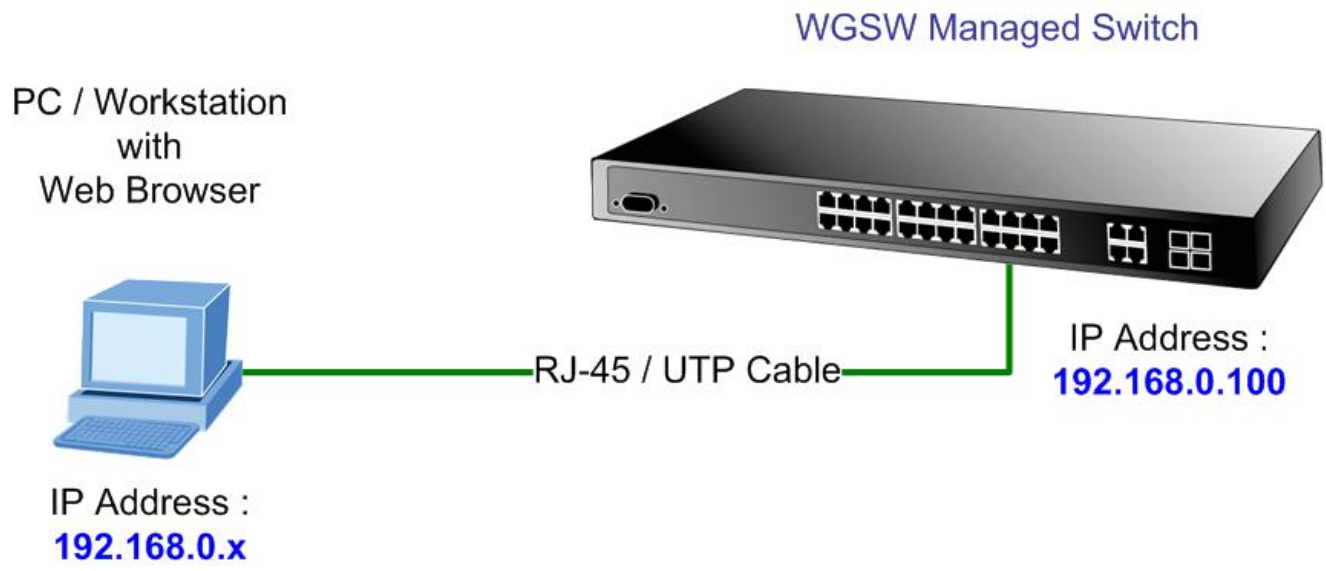


Figure 3-3 Web management

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

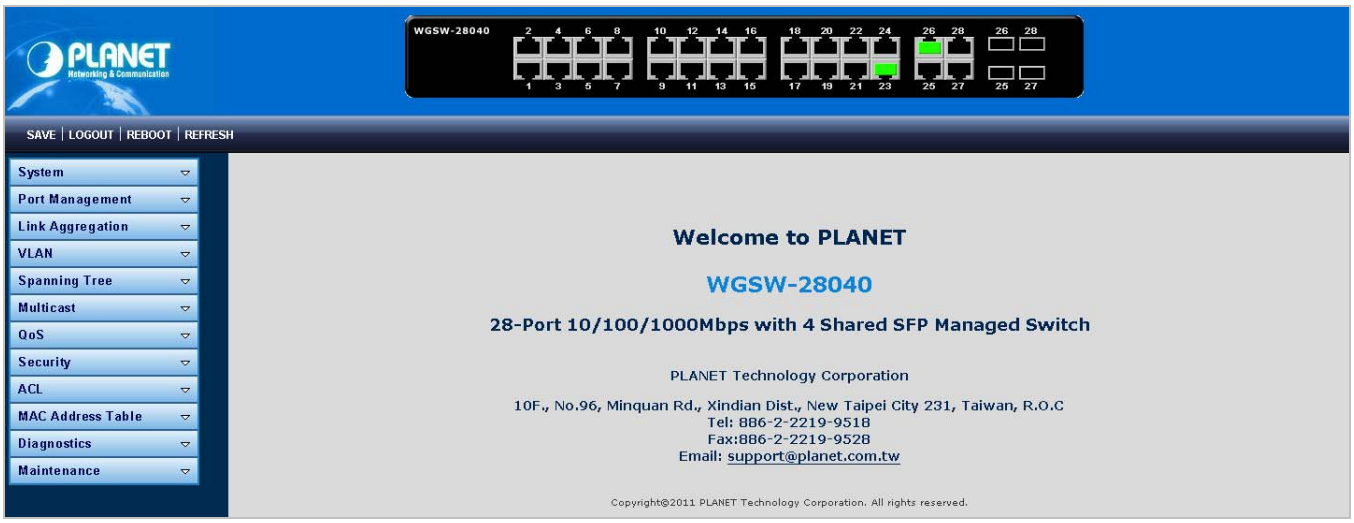


Figure 3-4 Web main screen of Managed Switch

3.5 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the Managed Switch, such as 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.

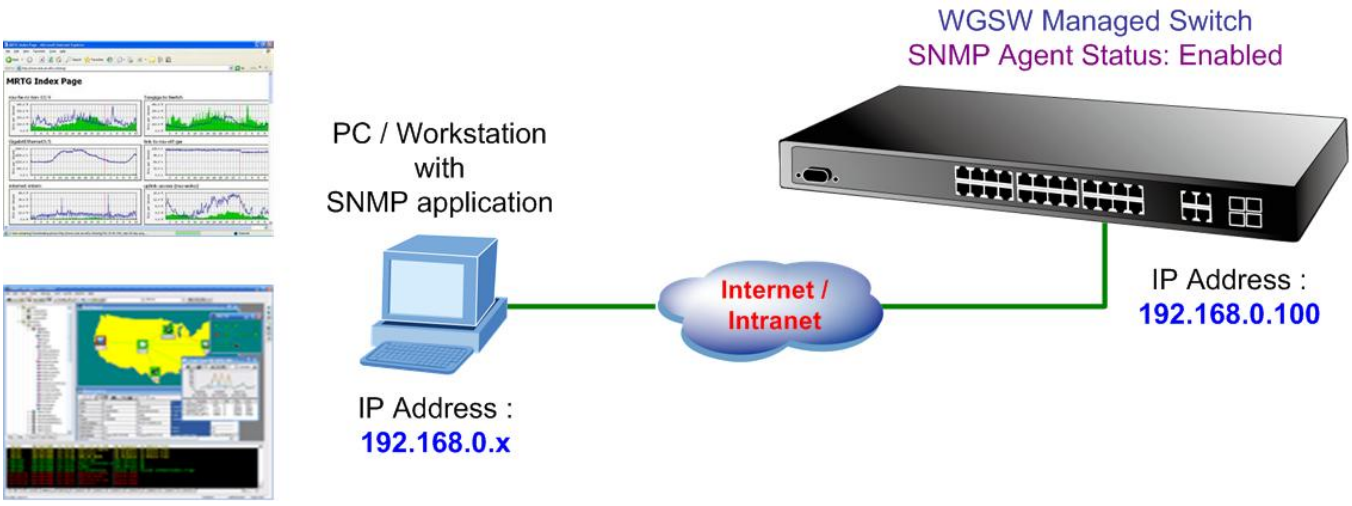


Figure 3-5 SNMP management

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 7.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

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

The Managed Switch can be configured through an Ethernet connection, 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 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.

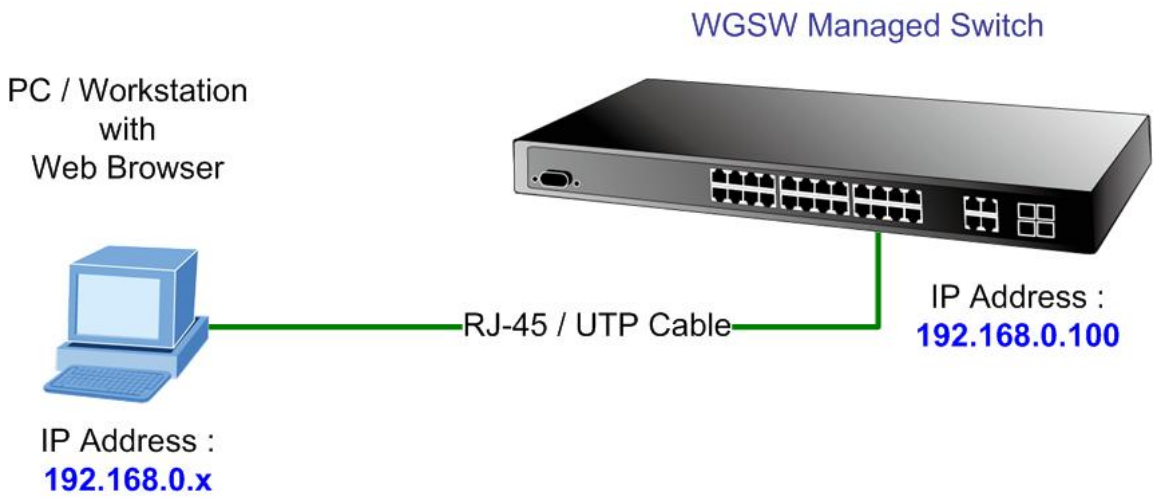


Figure 4-1-1 Web Management

■ **Logging on the switch**

1. Use Internet Explorer 7.0 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.

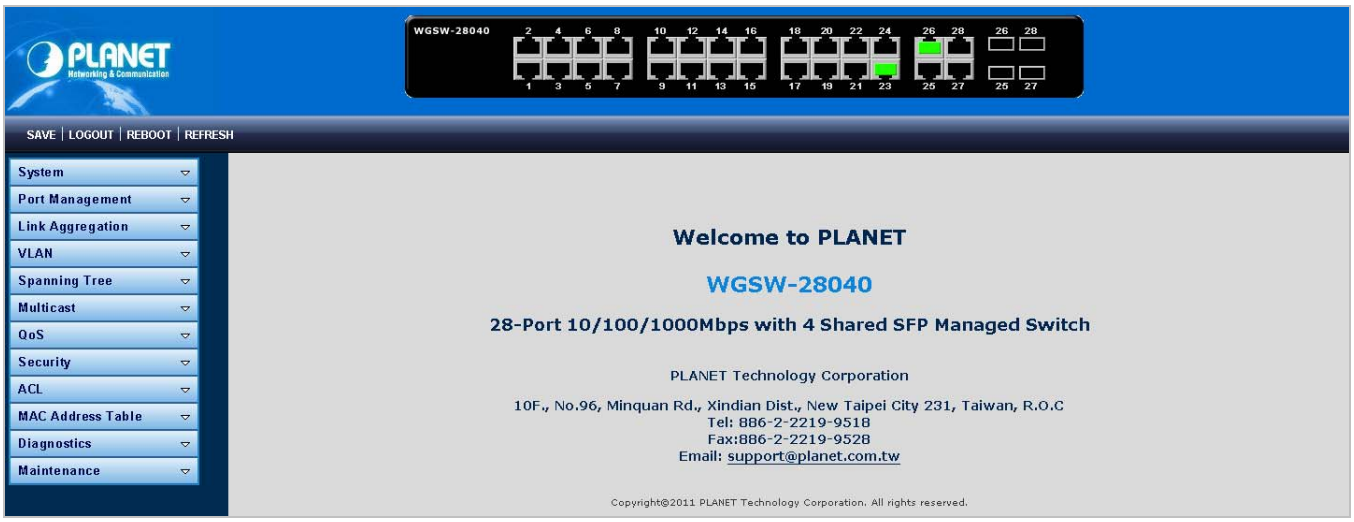


Figure 4-1-3 Default main page

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.

Note

1. It is recommended to use Internet Explore 7.0 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 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.

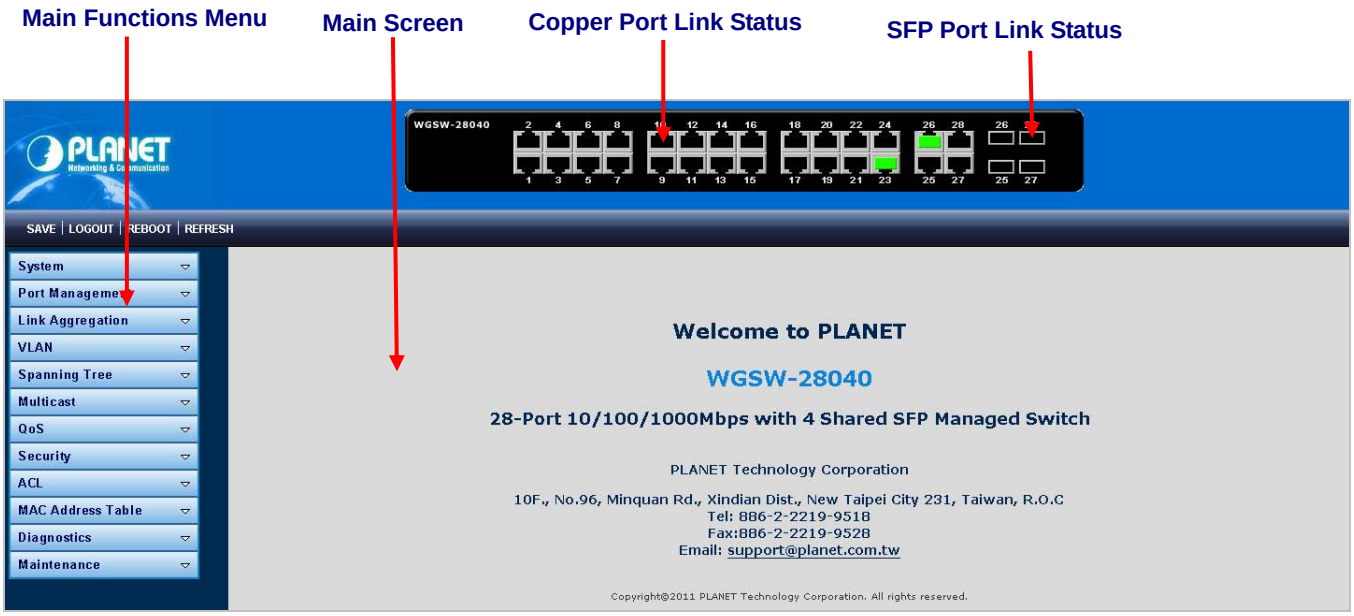


Figure 4-1-4 Main Page

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			

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.

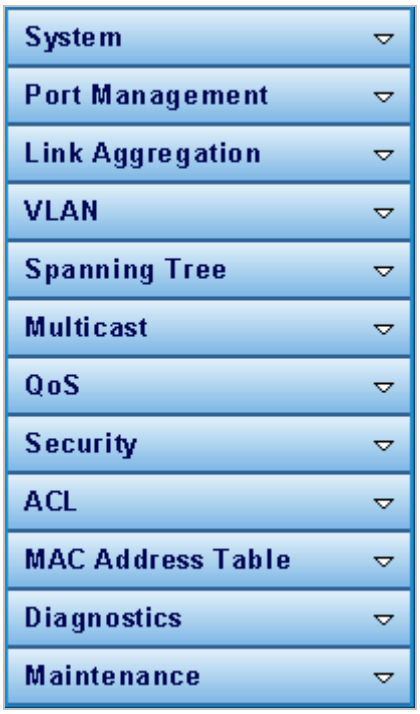


Figure 4-1-5 WGSW Managed Switch Main Functions Menu

Buttons

SAVE: Click to save changes or reset to default.

LOGOUT: Click to logout the Managed Switch.

REBOOT: Click to reboot the Managed Switch.

REFRESH: Click to refresh the page.

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** The switch system information is provided here.
- **IP Configuration** Configure the switch-managed IP information on this page.
- **IPv6 Configuration** Configure the switch-managed IPv6 information on this page.
- **User Configuration** Configure new user name & password on this page.
- **Enable Password** Change the current password on this page.
- **SNTP Configuration** Configure SNTP on this page.
- **Log Management** The switch log information is provided here.
- **SNMP Management** Configure SNMP on this page.

4.2.1 System Information

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

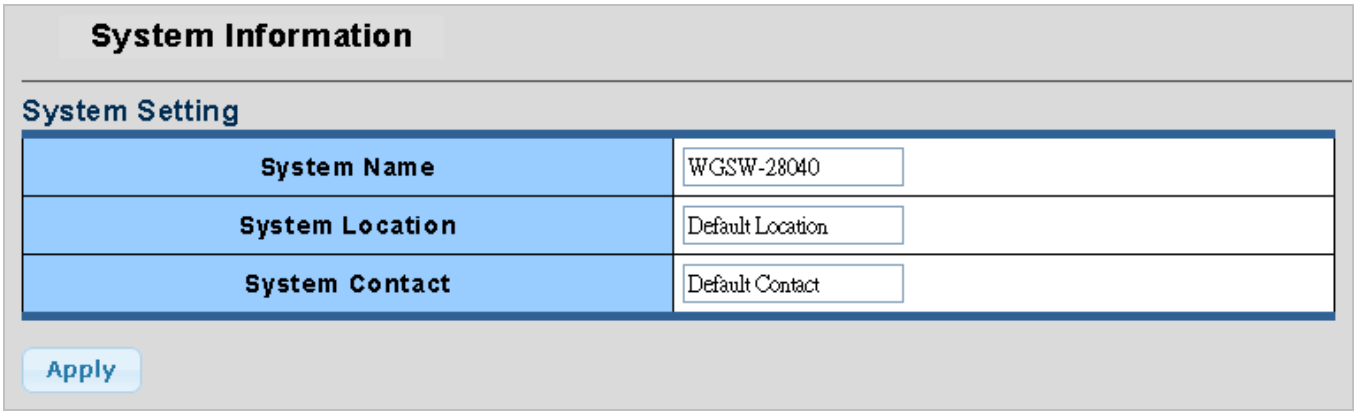


Figure 4-2-1 System Setting page screenshot

The page includes the following fields:

Object	Description
• System Name	The system name configured on this field.
• System Location	The system location configured on this field.
• System Contact	The system contact configured on this field.

Buttons

Apply: Click to apply changes.

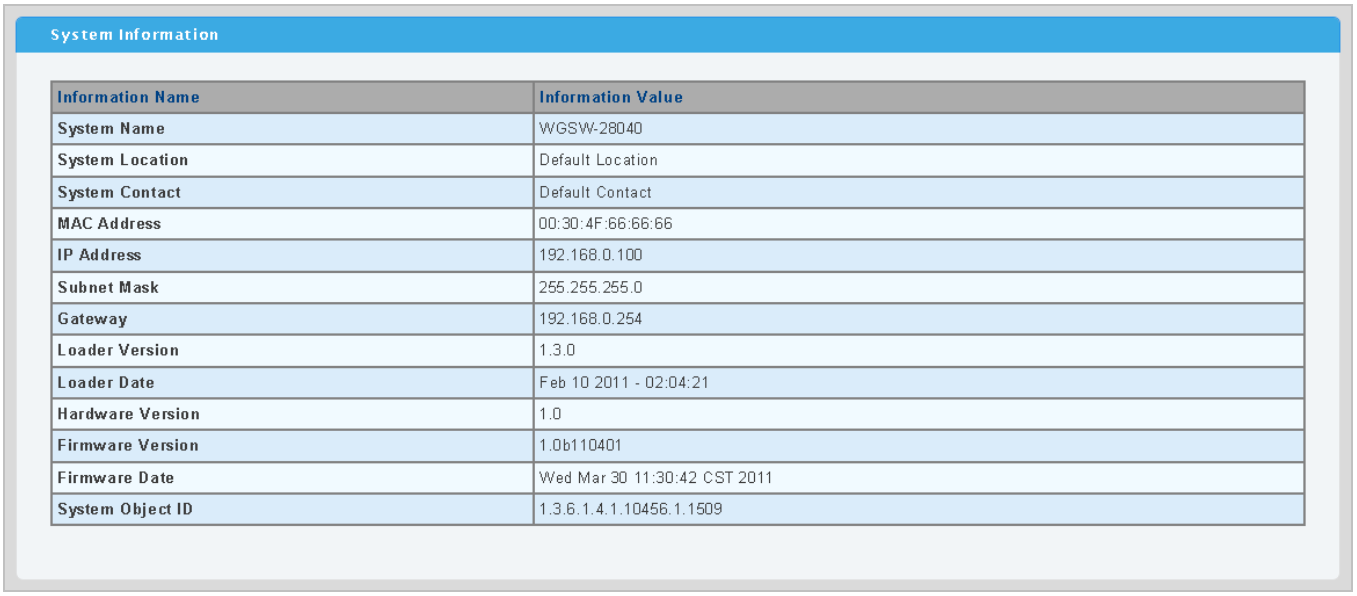


Figure 4-2-2 System Information page screenshot

The page includes the following fields:

Object	Description
• **System Name**	Display the current system name
• **System Location**	Display the current system location
• **System Contact**	Display the current system contact
• **MAC Address**	The MAC Address of this Managed Switch.
• **IP Address**	The IP Address of this Managed Switch.
• **Subnet Mask**	The subnet mask of this Managed Switch.
• **Gateway**	The gateway of this Managed Switch.
• **Loader Version**	The loader version of this Managed Switch.
• **Loader Date**	The loader date of this Managed Switch.
• **Hardware Version**	The hardware version of this Managed Switch..
• **Firmware Version**	The firmware version of this Managed Switch.
• **Firmware Date**	The firmware date of this Managed Switch.
• **System Object ID**	The system object ID of the Managed Switch.

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 4-2-3 & Figure 4-2-4 appears.

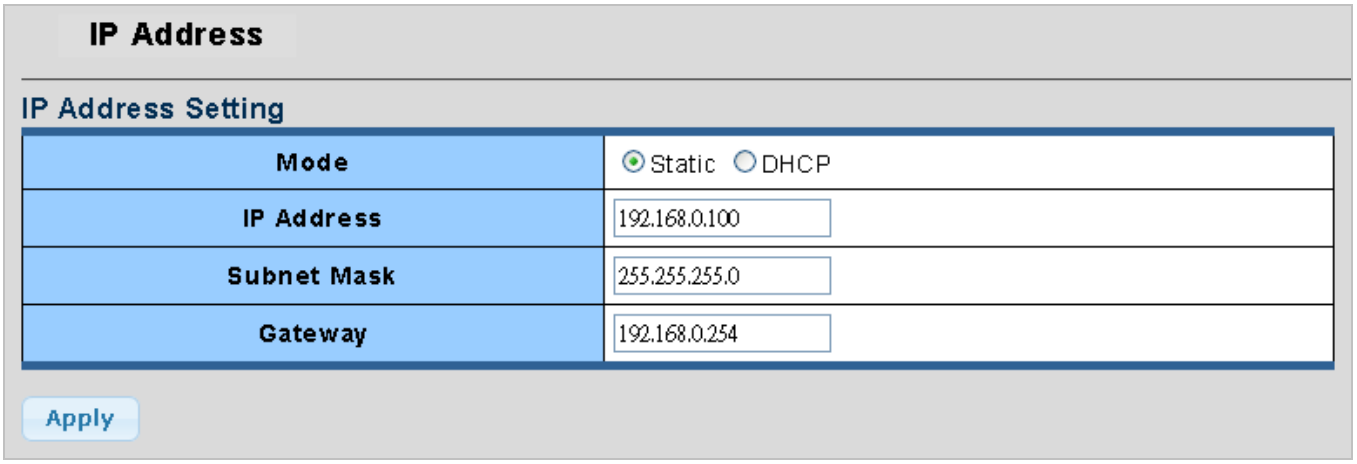


Figure 4-2-3 IP Address Setting page screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the IP address mode operation. Possible modes are: **Static**: Enable NTP mode operation. When enable NTP mode operation, the agent forward and to transfer NTP messages between the clients and the server when they are not on the same subnet domain. **DHCP**: Enable DHCP client mode operation. 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.
• **Subnet Mask**	Provide the subnet mask of this switch dotted decimal notation.
• **Gateway**	Provide the IP address of the router in dotted decimal notation.

Buttons

Apply: Click to apply changes.

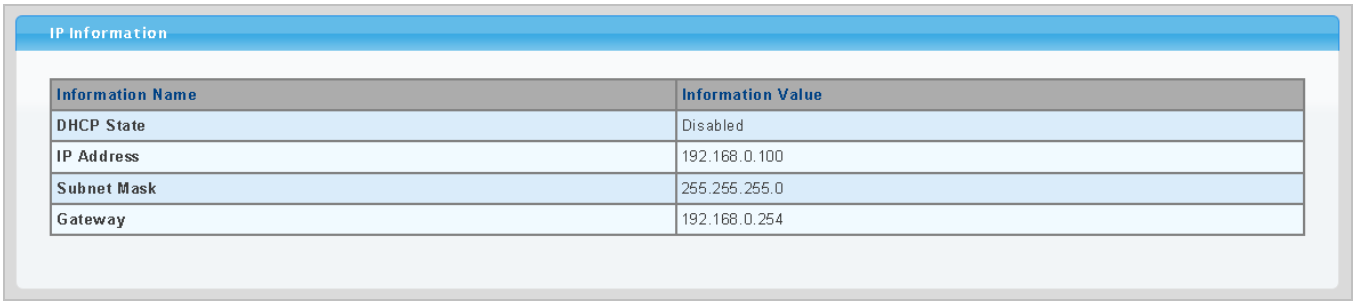


Figure 4-2-4 IP Information page screenshot

The page includes the following fields:

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

4.2.3 IPv6 Configuration

The IPv6 Configuration includes the Auto Configuration, IPv6 Address and Gateway. The Configured column is used to view or change the IPv6 configuration. Fill up the Auto Configuration, IPv6 Address and Gateway for the device. The screen in Figure 4-2-5 & Figure 4-2-6 appears.

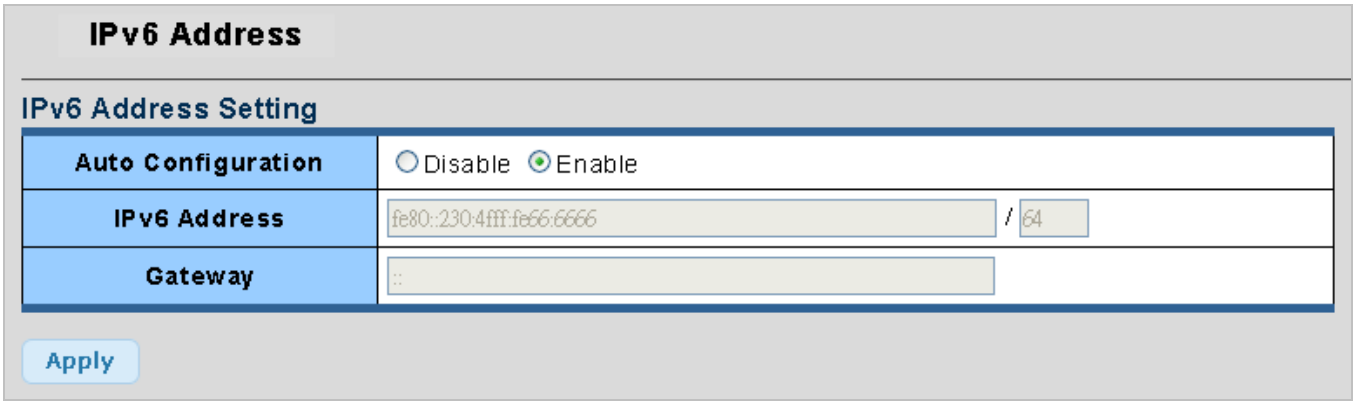


Figure 4-2-5 IPv6 Address Setting page screenshot

The page includes the following fields:

Object	Description
• **Auto Configuration**	Enable IPv6 auto-configuration by checking this box. If fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.
• **IPv6 Address**	Provide the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'. Provide the IPv6 Prefix of this switch. The allowed range is 1 through 128.
• **Gateway**	Provide the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'.

Buttons

Apply: Click to apply changes.

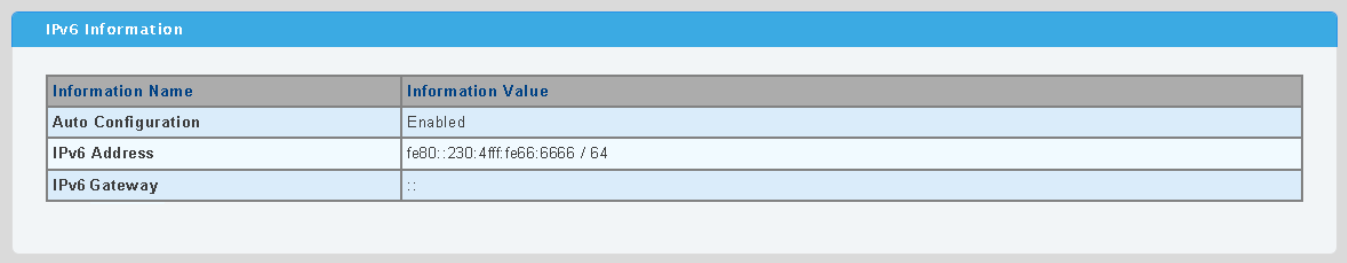


Figure 4-2-6 IPv6 Information page screenshot

The page includes the following fields:

Object	Description
• **Auto Configuration**	Display the current auto configuration state.
• **IPv6 Address**	Display the current IPv6 address
• **IPv6 Gateway**	Display the current gateway

4.2.4 User Configuration

This page provides an overview of the current users and privilege type. Currently the only way to login as another user on the web server is to close and reopen the browser. After setup completed, please press "**Apply**" button to take effect. Please login web interface with new user name and password, the screen in Figure 4-2-7 & Figure 4-2-8 appears.

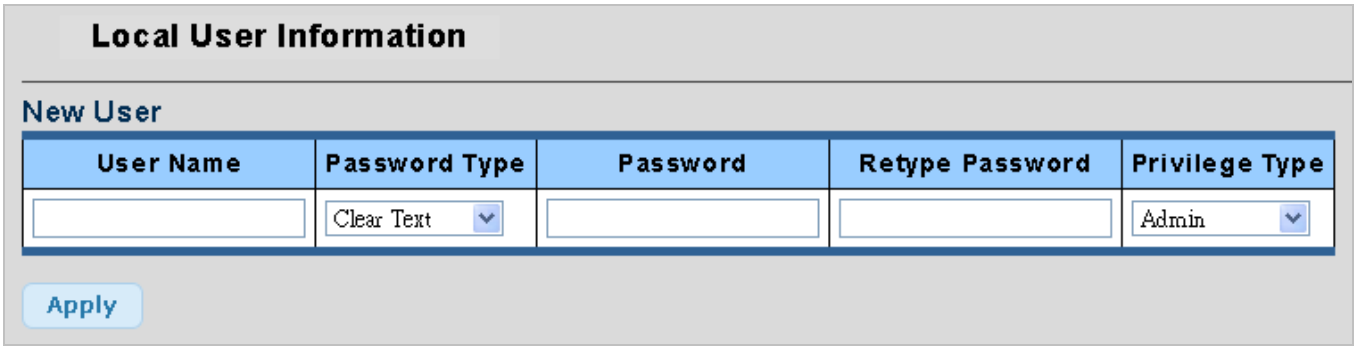


Figure 4-2-7 Local User Information page screenshot

The page includes the following fields:

Object	Description
• **Username**	The name identifying the user.
• **Password Type**	The password type for the user.
• **Password**	Enter the user's new password here.
• **Retype Password**	Please enter the user's new password here again to confirm.
• **Privilege Type**	The privilgeg type for the user.

Buttons

Apply: Click to apply changes.

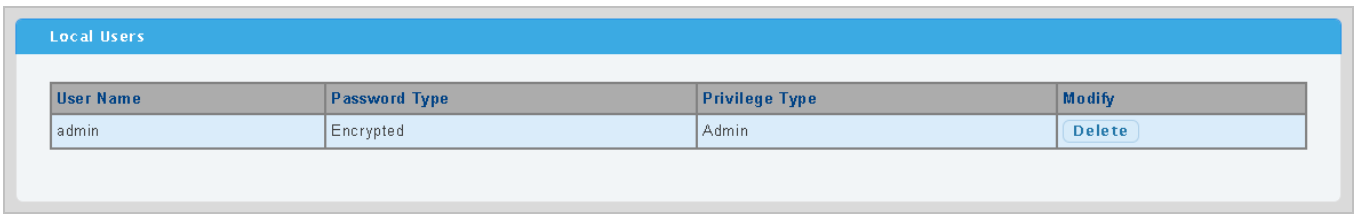


Figure 4-2-8 Local User page screenshot

The page includes the following fields:

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

4.2.5 Enable Password

This page provides to configure new password, the screen in Figure 4-2-9 appears.

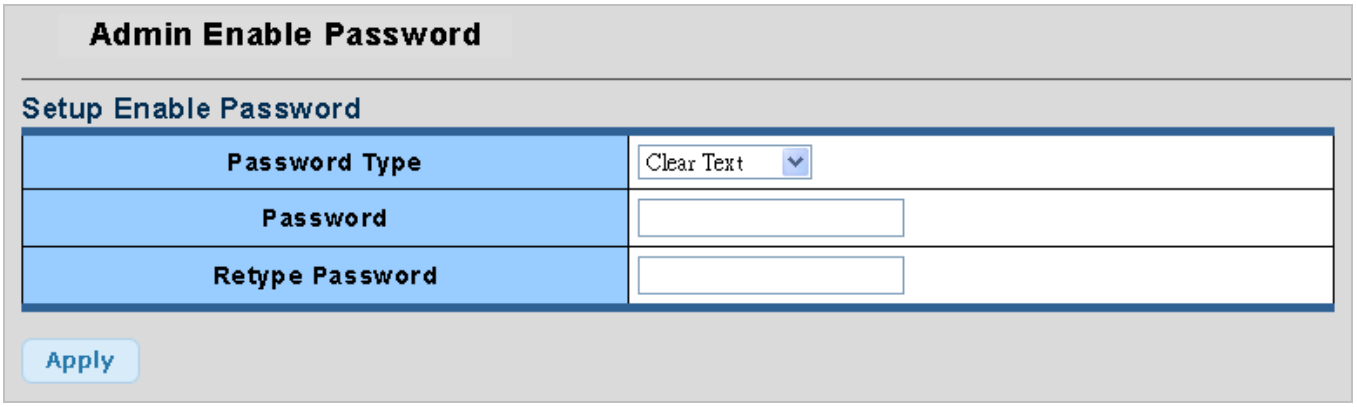


Figure 4-2-9 Admin Enable Password page screenshot

The page includes the following fields:

Object	Description
• **Password Type**	The password type for the user.
• **Password**	Enter the user's new password here.
• **Retype Password**	Please enter the user's new password here again to confirm.

Buttons

Apply: Click to apply changes.

4.2.6 SNTP Configuration

Configure SNTP on this page.

SNTP is an acronym for **Simple Network Time Protocol**, a network protocol for synchronizing the clocks of computer systems. You can specify SNTP Servers and set GMT Time zone. The SNTP Configuration screen in Figure 4-2-10 & Figure 4-2-11 appears.

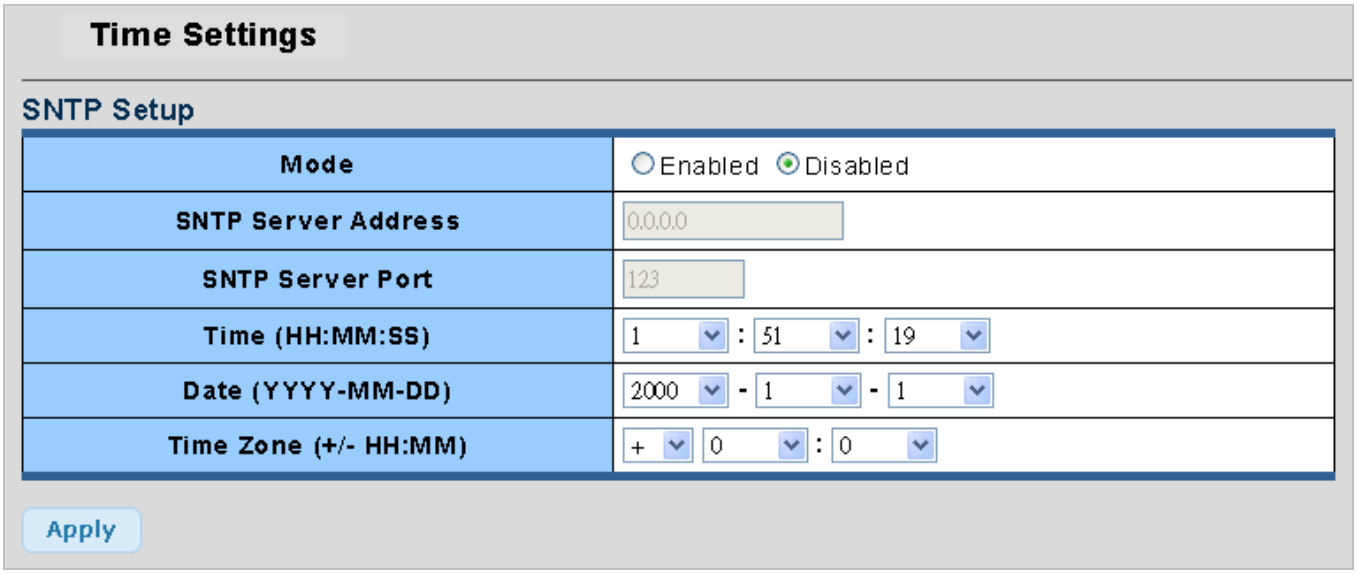


Figure 4-2-10 SNTP Setup page screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the SNTP mode operation. Possible modes are: **Enabled**: Enable SNTP mode operation. When enable SNTP mode operation, the agent forward and to transfer SNTP messages between the clients and the server when they are not on the same subnet domain. **Disabled**: Disable SNTP mode operation.
• **SNTP Server Address**	Type the IP address or domain name of the SNTP server.
• **SNTP Server Port**	Type the port number of the SNTP.
• **Time (HH:MM:SS)**	Click this option to set time manually.
• **Date (YYYY-MM-DD)**	Click this option to set date manually.
• **Time Zone (+/- HH:MM)**	Allow select the time zone according to current location of switch.

Buttons

Apply: Click to apply changes.

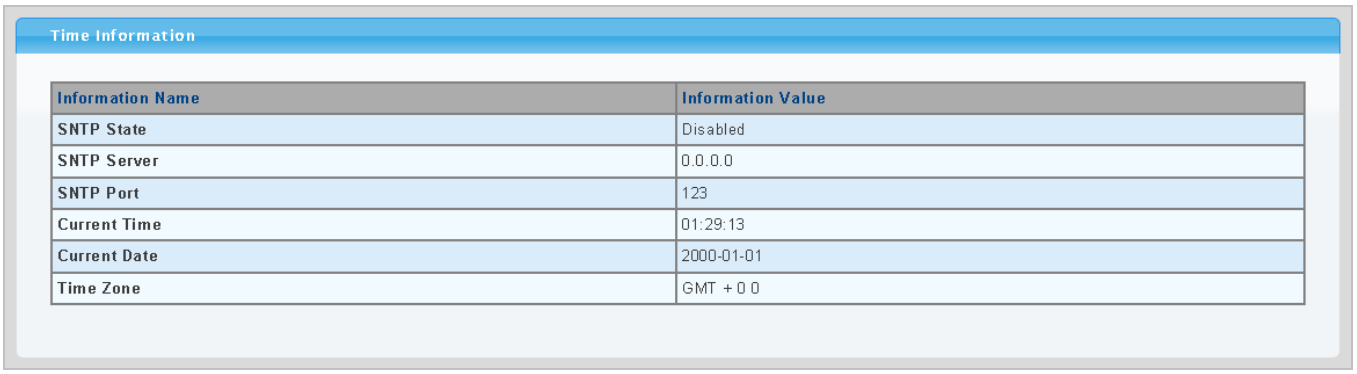


Figure 4-2-11 Time Information page screenshot

The page includes the following fields:

Object	Description
• **SNTP State**	Display the current SNTP state.
• **SNTP Server**	Display the current SNTP server.
• **SNTP Port**	Display the current SNTP port.
• **Current Time**	Display the current time.
• **Current Date**	Display the current date.
• **Time Zone**	Display the current time zone.

4.2.7 Log Management

The switch log management is provided here.

4.2.7.1 Local Log

The switch system local log information is provided here. The local Log screen in Figure 4-2-12 & Figure 4-2-13 appears.

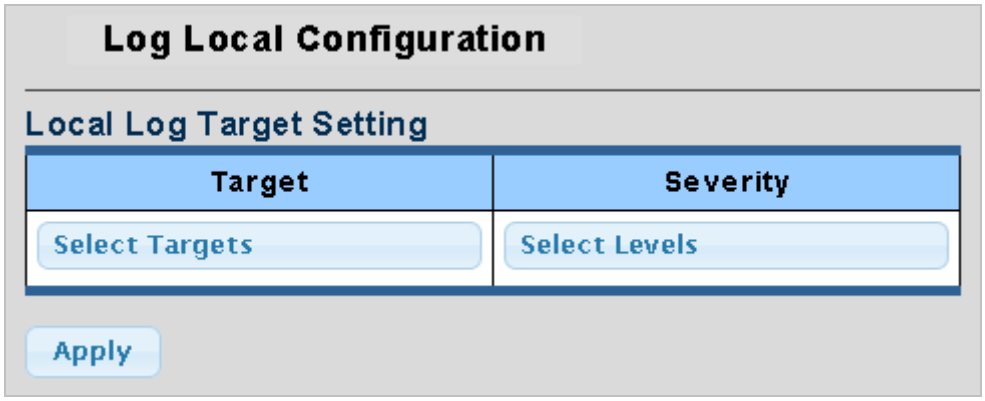


Figure 4-2-12 Local Log Target Setting page screenshot

The page includes the following fields:

Object	Description
• **Target**	The target of the local log entry. The following target types are supported: **RAM**: Target the RAM of the local log. **Flash**: Target the Flash of the local log.
• **Severity**	The severuty of the local log entry. The following severity types are supported: **emerg**: Emergency level of the system unsable for local log. **alert**: Alert level of the immediate action needed for local log. **crit**: Critical level of the critical conditions for local log. **error**: Error level of the error conditions for local log. **warning**: Warning level of the warning conditions for local log. **notice**: Notice level of the normal but significant conditions for local log. **info**: Informational level of the informational messages for local log. **debug**: Debug level of the debugging messages for local log.

Buttons

Apply: Click to apply changes.

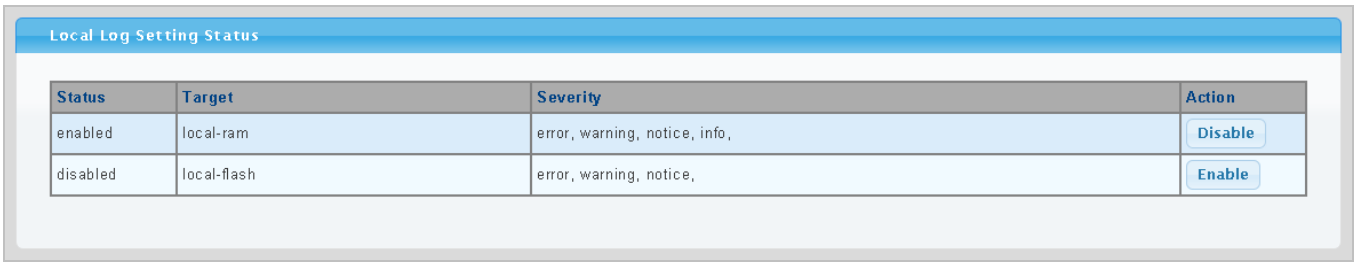


Figure 4-2-13 Local Log Setting Status page screenshot

The page includes the following fields:

Object	Description
• **Status**	Display the current local log state
• **Target**	Display the current local log target
• **Severity**	Display the current local log severity
• **Action**	Indicates the local log mode operation. Possible modes are: **Enabled**: Enable local log mode operation. When enable local log mode operation, the log and messages will be recorded in the switch. **Disabled**: Disable local log mode operation.

4.2.7.2 Remote Syslog

Configure remote syslog on this page. The Remote Syslog screen in Figure 4-2-14 & Figure 4-2-15 appears.

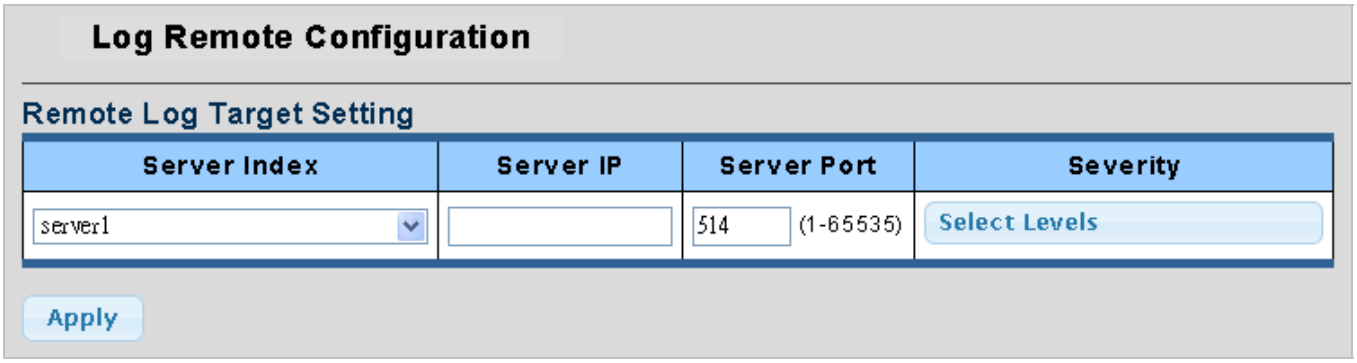


Figure 4-2-14 Remote Log Target page screenshot

The page includes the following fields:

Object	Description
• **Server Index**	Select remote syslog server number for this drop down list.
• **Server IP**	Provide the remote syslog IP address of this switch.
• **Server Port**	Provide the port nimber of remote syslog server.
• **Severity**	The severity of the local log entry. The following severity types are supported: **emerg**: Emergency level of the system unsable for local log. **alert**: Alert level of the immediate action needed for local log. **crit**: Critical level of the critical conditions for local log. **error**: Error level of the error conditions for local log. **warning**: Warning level of the warning conditions for local log. **notice**: Notice level of the normal but significant conditions for local log. **info**: Informational level of the informational messages for local log. **debug**: Debug level of the debugging messages for local log.

Buttons

Apply: Click to apply changes.

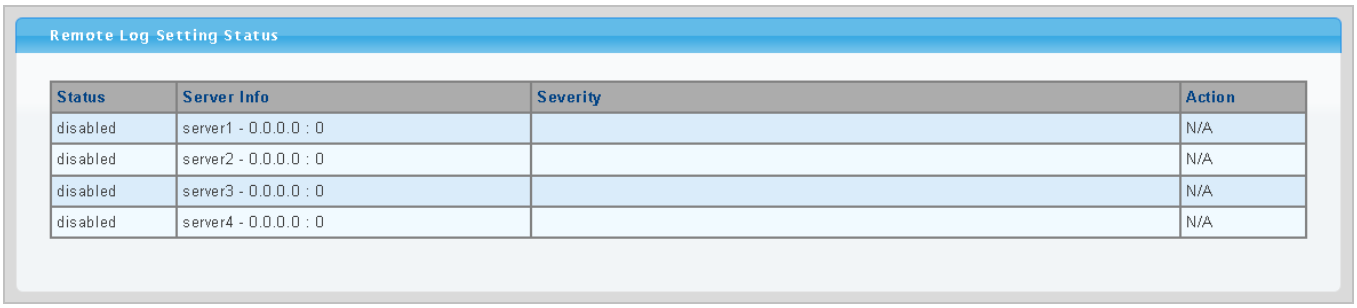


Figure 4-2-15 Remote Log Setting Status page screenshot

The page includes the following fields:

Object	Description
• **Status**	Display the current remote syslog state
• **Server Info**	Display the current remote syslog server information
• **Severity**	Display the current remote syslog severity
• **Action**	Indicates the remote syslog server mode operation. Possible modes are: **Enabled**: Enable emote syslog server mode operation. When enable remote syslog server mode operation, the log and messages will be recorded to the remote syslog server. **Disabled**: Disable remote syslog server mode operation.

4.2.7.3 Log View

The switch log view is provided here. The Log View screen in Figure 4-2-16, Figure 4-2-17 & Figure 4-2-18 appears.

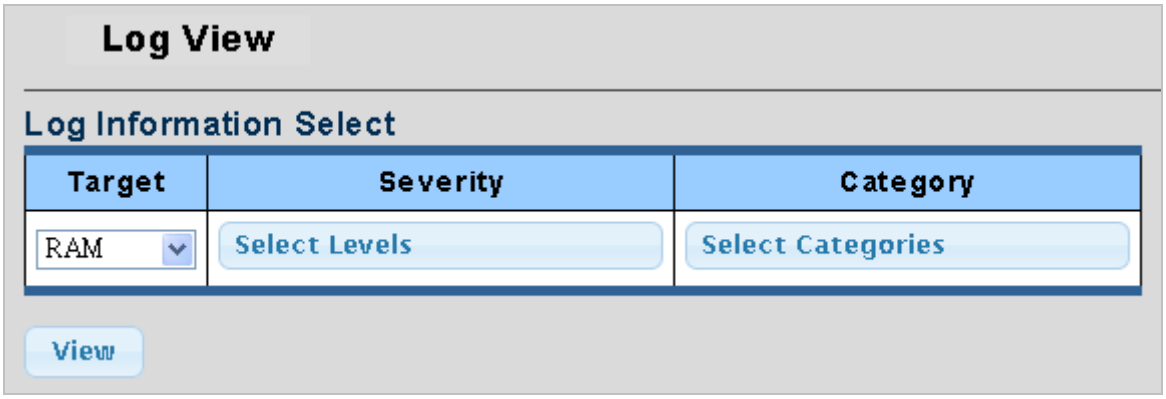


Figure 4-2-16 Log Information Select page screenshot

The page includes the following fields:

Object	Description
• **Target**	The target of the log view entry. The following target types are supported: **RAM**: Target the RAM of the log view . **Flash**: Target the Flash of the log view.
• **Severity**	The severity of the log view entry. The following severity types are supported: **emerg**: Emergency level of the system unsable for log view. **alert**: Alert level of the immediate action needed for log view. **crit**: Critical level of the critical conditions for log view. **error**: Error level of the error conditions for log view. **warning**: Warning level of the warning conditions for log view. **notice**: Notice level of the normal but significant conditions for log view. **info**: Informational level of the informational messages for log view. **debug**: Debug level of the debugging messages for log view.
• **Category**	The category of the log view that are including: ACL, Common, DAI, DEF_ENGINE, DoS, Dot1X, EEE, IGMP, L2, LACP, LLDP, Log, Mirror, PoE, Port, QoS, QinQ , Rate, SNMP, STP, SVLAN, Switch, System, TFTP, Trunk, UDLD, VLAN, LOOP_PROT

Buttons

View: Click to view log.

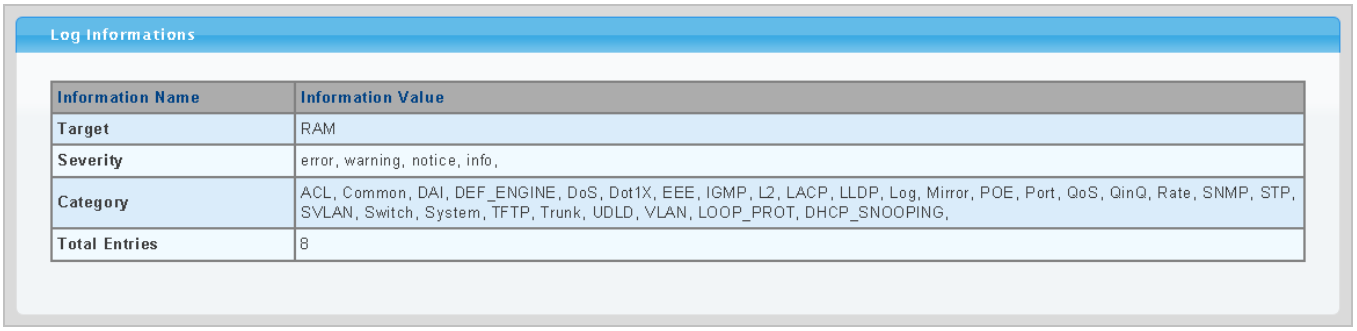


Figure 4-2-17 Log Information page screenshot

The page includes the following fields:

Object	Description
• **Target**	Display the current log target.
• **Severity**	Display the current log severity.
• **Category**	Display the current log category
• **Total Entries**	Display the current log entries

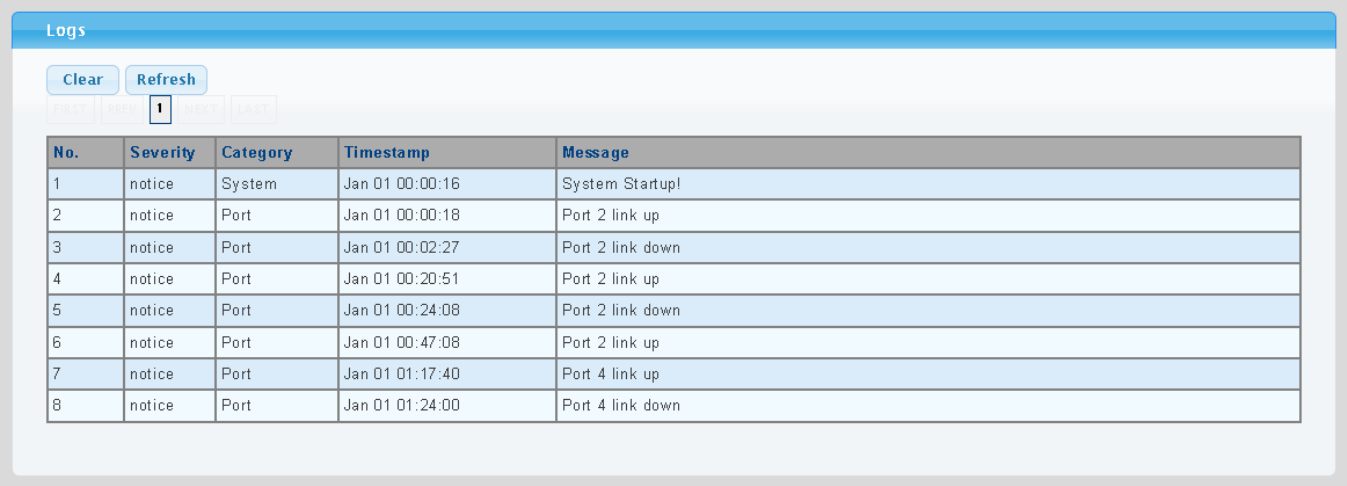


Figure 4-2-18 Logs page screenshot

The page includes the following fields:

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

Buttons

Clear: Click to clear the log.

Refresh: Click to refresh the log.

4.2.8 SNMP Management

4.2.8.1 SNMP Overview

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

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

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

SNMP Operations

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

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

SNMP community

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

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

4.2.8.2 System Information

The switch system information is provided here. The System Information Configuration screen in Figure 4-2-19 & Figure 4-2-20 appears.

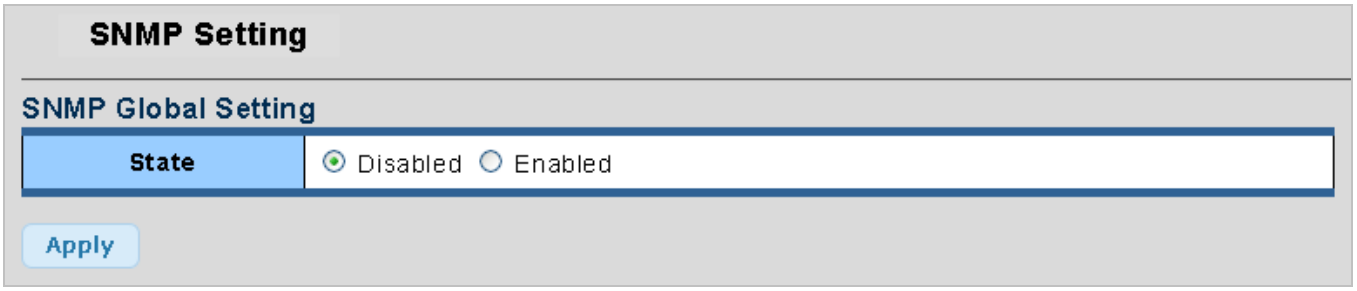


Figure 4-2-19 SNMP Global Setting page screenshot

The page includes the following fields:

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

Buttons

Apply: Click to apply changes.

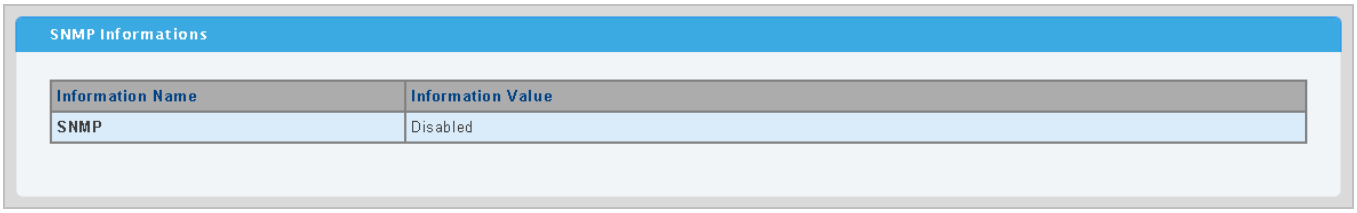


Figure 4-2-20 SNMP Informations page screenshot

The page includes the following fields:

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

4.2.8.3 Community

Configure SNMP Community on this page. The SNMP Community screen in Figure 4-2-21 & Figure 4-2-22 appears.

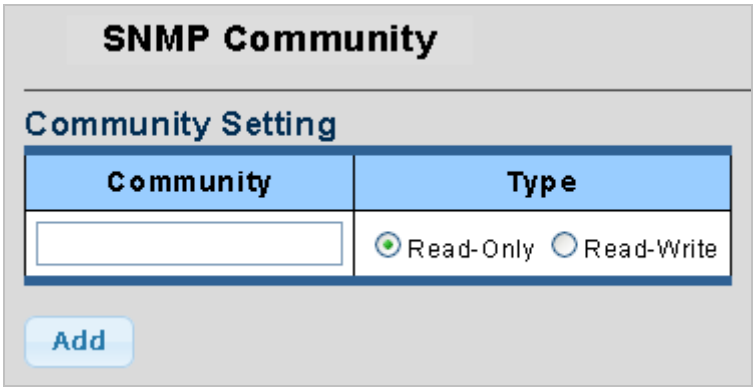


Figure 4-2-21 Community Setting page screenshot

The page includes the following fields:

Object	Description
• **Community**	Indicates the community read/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.
• **Type**	Indicates the SNMP community type operation. Possible types are: **Read-Only**: Set access string type in read-only mode. **Read-Write**: Set access string type in read-write mode.

Buttons

Apply: Click to apply changes.

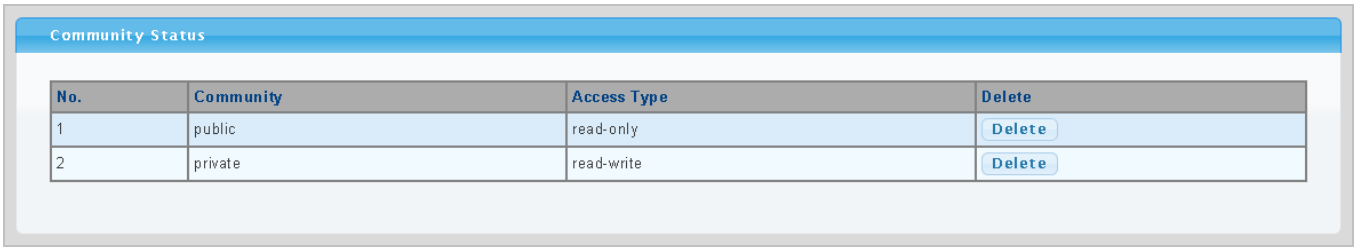


Figure 4-2-22 Community Status page screenshot

The page includes the following fields:

Object	Description
• **No.**	This is the number for community entry.
• **Community**	Display the current community type.
• **Access Type**	Display the current access type.
• **Delete**	Click to delete the community entry.

4.2.8.4 Trap

Configure SNMP trap on this page. The SNMP Trap Configuration screen in Figure 4-2-23 & Figure 4-2-24 appears.

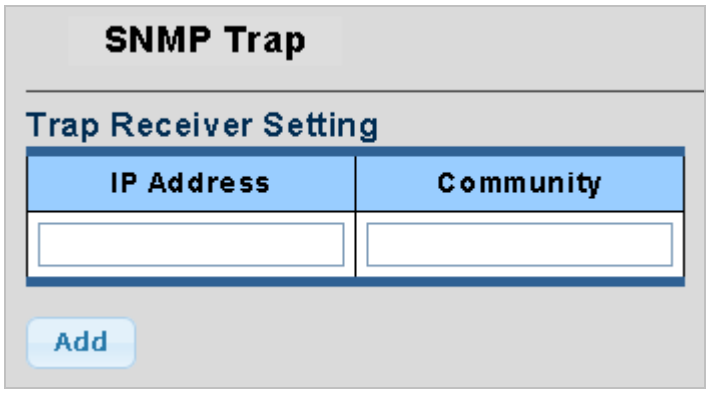


Figure 4-2-23 Trap Receiver Setting page screenshot

The page includes the following fields:

Object	Description
• **IP Address**	Indicates the SNMP trap destination address.
• **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.

Buttons

Apply: Click to apply changes.

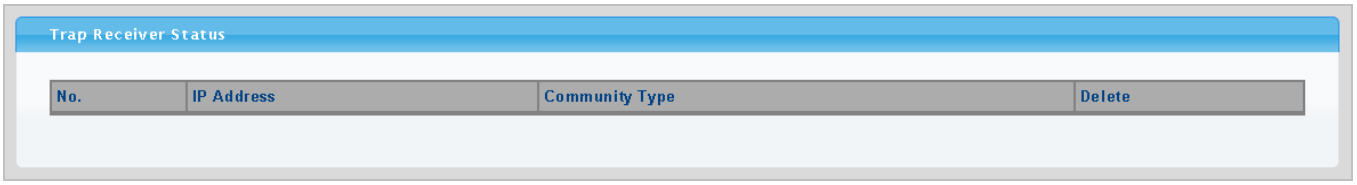


Figure 4-2-24 Trap Receiver Status page screenshot

The page includes the following fields:

Object	Description
• **No.**	This is the number for SNMP trap server entry.
• **IP Address**	Display the current SNMP trap destination address.
• **Community Type**	Display the current community type.
• **Delete**	Click to delete the SNMP trap server entry.

4.3 Port Management

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

■ **Port Configuration**	Configures port configuration settings
■ **Port Statistics** ■ **Port Counters**	Lists Ethernet and RMON port statistics
■ **Port Error Disabled**	Disable port error status
■ **Port Mirroring**	Sets the source and target ports for mirroring
■ **Jumbo Frame**	Set the jumbo frame on the switch
■ **Protected Ports**	Configuration protected ports settings
■ **Bandwidth Control**	Configures bandwidth control settings

4.3.1 Port Configuration

This page displays current port configurations and status. 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 4-3-1 & Figure 4-3-2 appears.

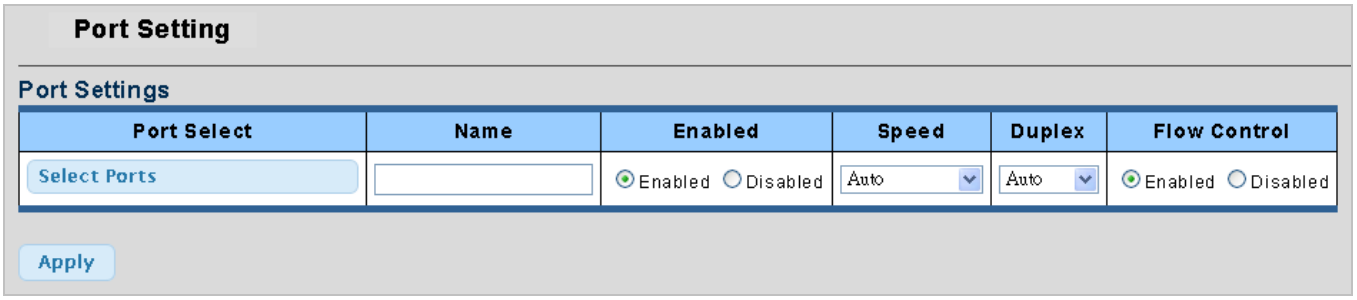


Figure 4-3-1 Port Settings page screenshot

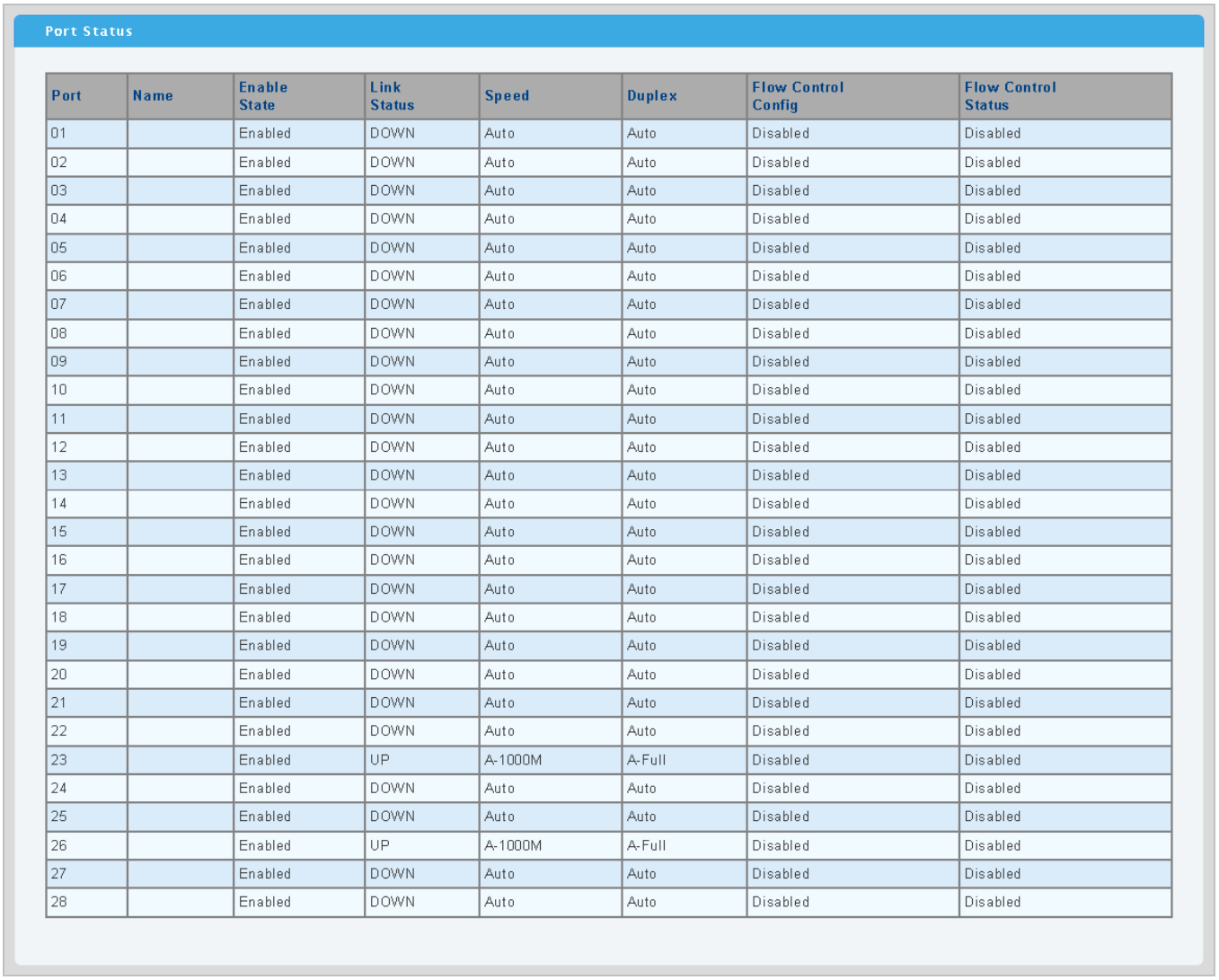
The page includes the following fields:

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

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

Buttons

Apply: Click to apply changes.



Port Status

Port	Name	Enable State	Link Status	Speed	Duplex	Flow Control Config	Flow Control Status
01		Enabled	DOWN	Auto	Auto	Disabled	Disabled
02		Enabled	DOWN	Auto	Auto	Disabled	Disabled
03		Enabled	DOWN	Auto	Auto	Disabled	Disabled
04		Enabled	DOWN	Auto	Auto	Disabled	Disabled
05		Enabled	DOWN	Auto	Auto	Disabled	Disabled
06		Enabled	DOWN	Auto	Auto	Disabled	Disabled
07		Enabled	DOWN	Auto	Auto	Disabled	Disabled
08		Enabled	DOWN	Auto	Auto	Disabled	Disabled
09		Enabled	DOWN	Auto	Auto	Disabled	Disabled
10		Enabled	DOWN	Auto	Auto	Disabled	Disabled
11		Enabled	DOWN	Auto	Auto	Disabled	Disabled
12		Enabled	DOWN	Auto	Auto	Disabled	Disabled
13		Enabled	DOWN	Auto	Auto	Disabled	Disabled
14		Enabled	DOWN	Auto	Auto	Disabled	Disabled
15		Enabled	DOWN	Auto	Auto	Disabled	Disabled
16		Enabled	DOWN	Auto	Auto	Disabled	Disabled
17		Enabled	DOWN	Auto	Auto	Disabled	Disabled
18		Enabled	DOWN	Auto	Auto	Disabled	Disabled
19		Enabled	DOWN	Auto	Auto	Disabled	Disabled
20		Enabled	DOWN	Auto	Auto	Disabled	Disabled
21		Enabled	DOWN	Auto	Auto	Disabled	Disabled
22		Enabled	DOWN	Auto	Auto	Disabled	Disabled
23		Enabled	UP	A-1000M	A-Full	Disabled	Disabled
24		Enabled	DOWN	Auto	Auto	Disabled	Disabled
25		Enabled	DOWN	Auto	Auto	Disabled	Disabled
26		Enabled	UP	A-1000M	A-Full	Disabled	Disabled
27		Enabled	DOWN	Auto	Auto	Disabled	Disabled
28		Enabled	DOWN	Auto	Auto	Disabled	Disabled

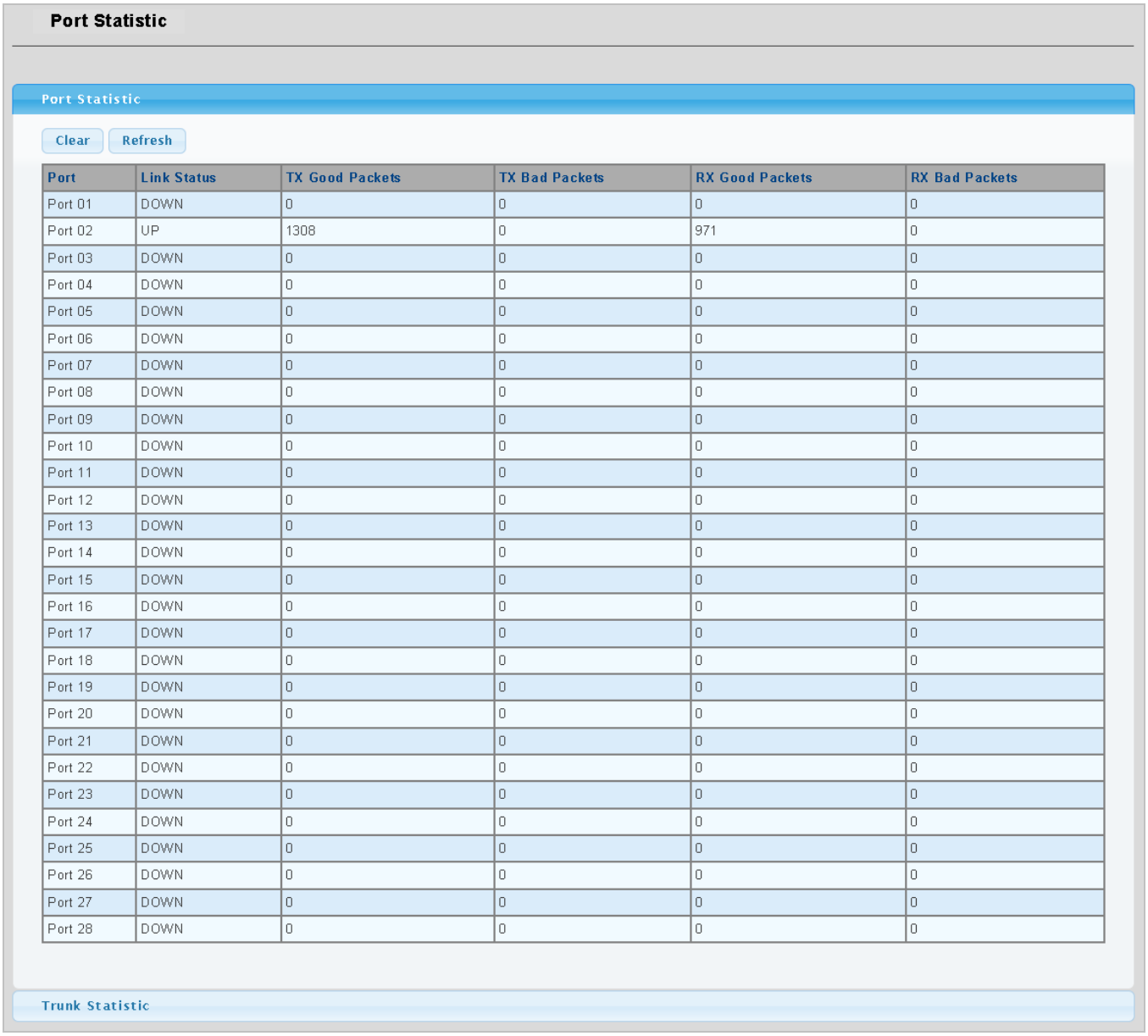
Figure 4-3-2 Port Status page screenshot

The page includes the following fields:

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

4.3.2 Port Statistics

This page provides an overview of traffic and trunk statistics for all switch ports. The Port Statistics screen in Figure 4-3-3 & Figure 4-3-4 appears.



Port	Link Status	TX Good Packets	TX Bad Packets	RX Good Packets	RX Bad Packets
Port 01	DOWN	0	0	0	0
Port 02	UP	1308	0	971	0
Port 03	DOWN	0	0	0	0
Port 04	DOWN	0	0	0	0
Port 05	DOWN	0	0	0	0
Port 06	DOWN	0	0	0	0
Port 07	DOWN	0	0	0	0
Port 08	DOWN	0	0	0	0
Port 09	DOWN	0	0	0	0
Port 10	DOWN	0	0	0	0
Port 11	DOWN	0	0	0	0
Port 12	DOWN	0	0	0	0
Port 13	DOWN	0	0	0	0
Port 14	DOWN	0	0	0	0
Port 15	DOWN	0	0	0	0
Port 16	DOWN	0	0	0	0
Port 17	DOWN	0	0	0	0
Port 18	DOWN	0	0	0	0
Port 19	DOWN	0	0	0	0
Port 20	DOWN	0	0	0	0
Port 21	DOWN	0	0	0	0
Port 22	DOWN	0	0	0	0
Port 23	DOWN	0	0	0	0
Port 24	DOWN	0	0	0	0
Port 25	DOWN	0	0	0	0
Port 26	DOWN	0	0	0	0
Port 27	DOWN	0	0	0	0
Port 28	DOWN	0	0	0	0

Figure 4-3-3 Port Statistic page screenshot

The displayed counters are:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Link Status**	Display the current link status of the port.
• **Tx Good Packets**	The number of transmitted good packets per port.

• **Tx Bad Packets**	The number of frames transmitted in error and the number of incomplete transmissions per port.
• **Rx Good Packets**	The number of received good packets per port.
• **Rx Bad Packets**	The number of frames received in error and the number of incomplete transmissions per port.

Buttons

Clear: Clears the counters for all ports.

Refresh: Click to refresh the page immediately.

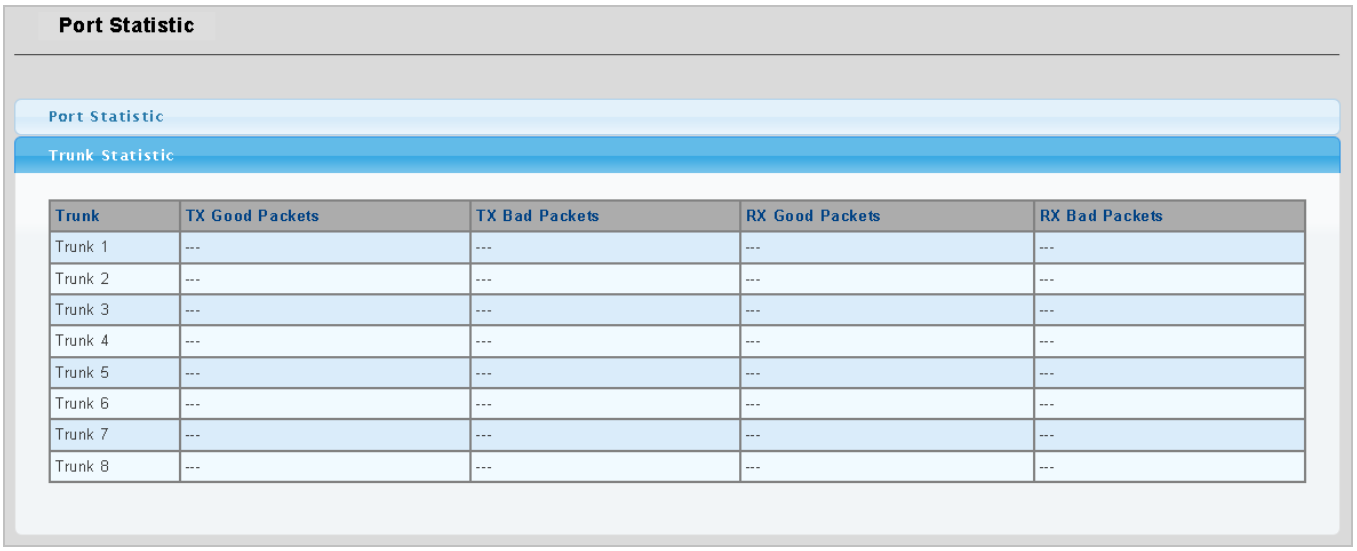


Figure 4-3-4 Trunk Statistic page screenshot

The displayed counters are:

Object	Description
• **Trunk**	This is the number for trunk entry.
• **Tx Good Packets**	The number of transmitted good packets per trunk.
• **Tx Bad Packets**	The number of frames transmitted in error and the number of incomplete transmissions per trunk.
• **Rx Good Packets**	The number of received good packets per trunk.
• **Rx Bad Packets**	The number of frames received in error and the number of incomplete transmissions per trunk.

4.3.3 Port Counters

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 Port Counters screen in Figure 4-3-5 & Figure 4-3-6 appears.

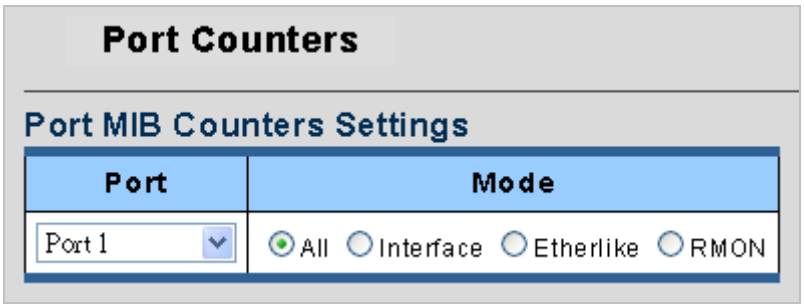


Figure 4-3-5 Port Counters Settings page screenshot

The displayed counters are:

Object	Description
• **Port**	Select port number for this drop down list.
• **Mode**	Select port counters mode.

Port1 mib Counters

IF mib Counter Name	mib Counter Value
ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	0
ifOutUcastPkts	0
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0
ifInBroadcastPkts	0
ifOutMulticastPkts	0
ifOutBroadcastPkts	0

Ether-Like mib Counter Name	mib Counter Value
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpcodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

Rmon mib Counter Name	mib Counter Value
etherStatsDropEvents	0
etherStatsOctets	0
etherStatsPkts	0
etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0
etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0
IngressLackPktBufDrop	0

Figure 4-3-6 Counters page screenshot

Interface Counters:

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

Ethernet-Link Counters:

Object	Description
• **Alignment Errors**	The number of alignment errors (missynchronized data packets).
• **FCS Errors**	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include

	frames received with frame-too-long or frame-too-short error.
• **Single Collision Frames**	The number of successfully transmitted frames for which transmission isinhibited by exactly one collision.
• **Multiple Collision Frames**	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
• **Deferred Transmissions**	A count of frames for which the first transmission attempt on a particularinterface is delayed because the medium was busy.
• **Late Collision**	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
• **Excessive Collision**	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
• **Frame Too Longs**	A count of frames received on a particular interface that exceed the maximum permitted frame size.
• **Symbol Errors**	The number of received and transmitted symbol errors.
• **Control In Unknow Opcodes**	The number of received control unknown opcodes
• **In Pause Frames**	The number of received pause frames
• **Out Pause Frames**	The number of transmitted pause frames

RMON Counters:

Object	Description
• **Drop Events**	The total number of events in which packets were dropped due to lack of resources.
• **Octets**	The total number of octets received and transmitted on the interface, including framing characters.
• **Packets**	The total number of packets received and transmitted on the interface.
• **Broadcast Packets**	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
• **Multicast Packets**	The total number of good frames received that were directed to this multicast address.
• **CRC / Alignment Errors**	The number of CRC/alignment errors (FCS or alignment errors).
• **Undersize Packets**	The total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed.
• **Oversize Packets**	The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed.

• **Fragments**	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
• **Jabbers**	The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
• **Collisions**	The best estimate of the total number of collisions on this Ethernet segment.
• **64 Bytes Frames**	The total number of frames (including bad packets) received andtransmitted that were 64 octets in length (excluding framing bits but including FCS octets).
• **65-127 Byte Frames** **128-255 Byte Frames** **256-511 Byte Frames** **512-1023 Byte Frames** **1024-1518 Byte Frames**	The total number of frames (including bad packets) received andtransmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
• **Lack Packets Buffer Drop**	The number of Lack Packets Buffer Drop

4.3.4 Port Error Disabled

This page provides disable that transitions a port into error disable and the recovery options. The Port Error Disable screen in Figure 4-3-7 appears.

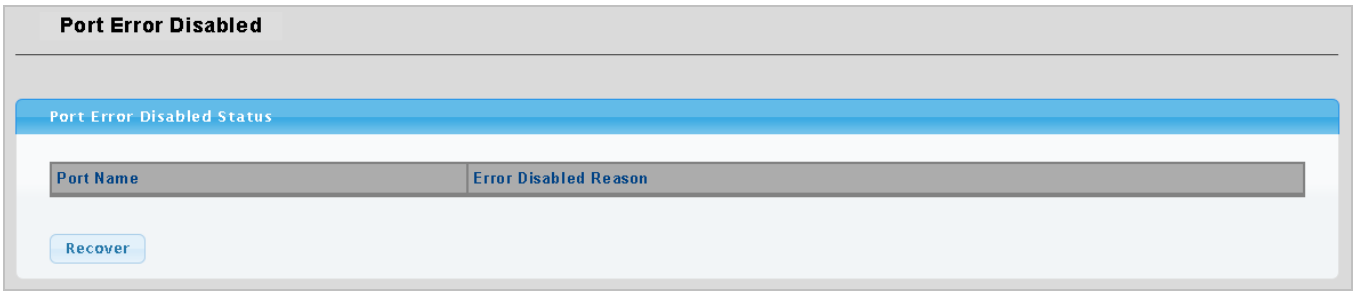


Figure 4-3-7 Port Error Disable page screenshot

The displayed counters are:

Object	Description
• **Port Name**	Display the port for error disable.
• **Error Disable Reason**	Display the error disabled reason of the port.

Buttons

Recover: Click to recover port error status.

4.3.5 Port Mirroring

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

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

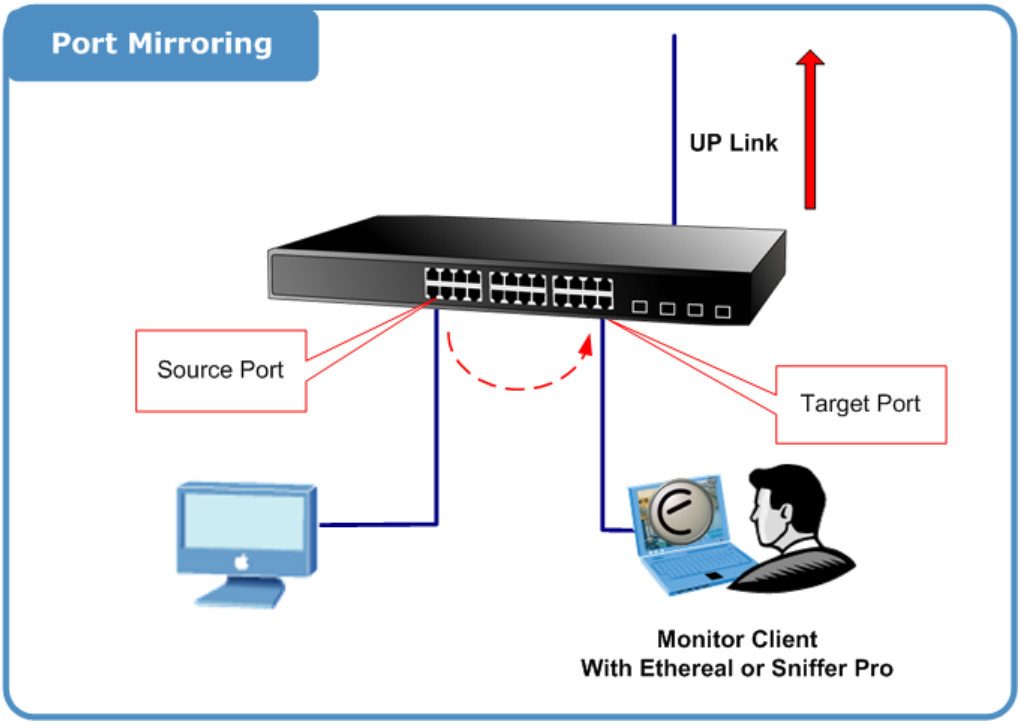


Figure 4-3-8 Port Mirror application

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

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

Mirror Port Configuration

The Port Mirror Configuration screen in Figure 4-3-9 & Figure 4-3-10 appears.

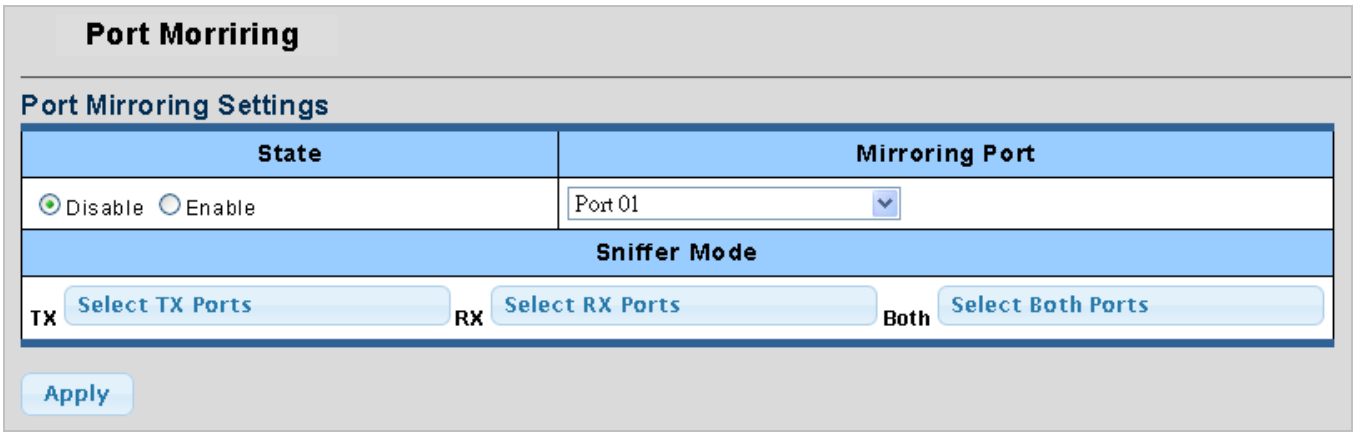


Figure 4-3-9 Port Mirroring Settings page screenshot

The page includes the following fields:

Object	Description
• **State**	Frames from ports that have either source or destination mirroring enabled are mirrored to this port. Disabled disables mirroring.
• **Mirroring Port**	Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port.
• **Sniffer Mode**	Select mirror mode and target port. • **Rx** (receive) • **Tx** (transmit) • **Both** (receive and transmit)

Buttons

Apply: Click to apply changes.

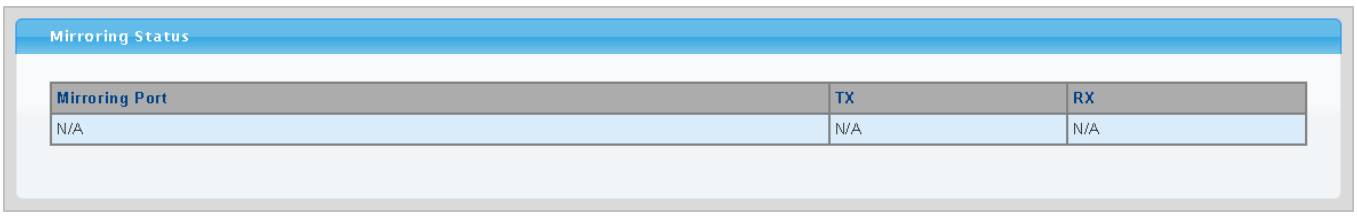


Figure 4-3-10 Mirroring Status page screenshot

The page includes the following fields:

Object	Description
• **Mirroring Port**	This is the mirroring port entry.

• **TX**	Display the current TX status.
• **RX**	Display the current RX status.

4.3.6 Jumbo Frame

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

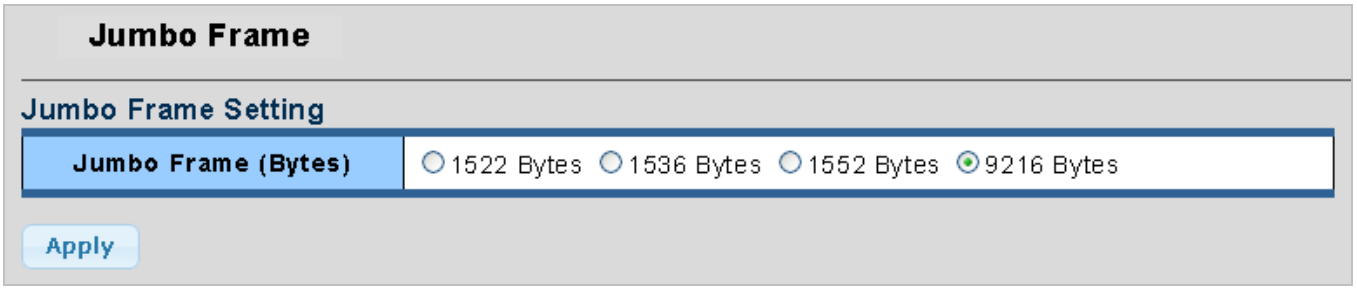


Figure 4-3-11 Jumbo Frame Setting page screenshot

The page includes the following fields:

Object	Description
• **Jumbo Frame (Bytes)**	Select any available maximum frame size for the switch. Possible frame size are: **1522 Bytes** **1539 Bytes** **1552 Bytes** **9216 Bytes**

Buttons

Apply: Click to apply changes.

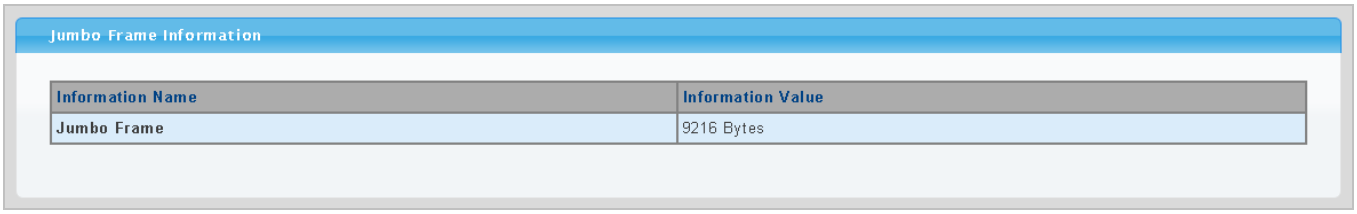


Figure 4-3-12 Jumbo Frame Information page screenshot

The page includes the following fields:

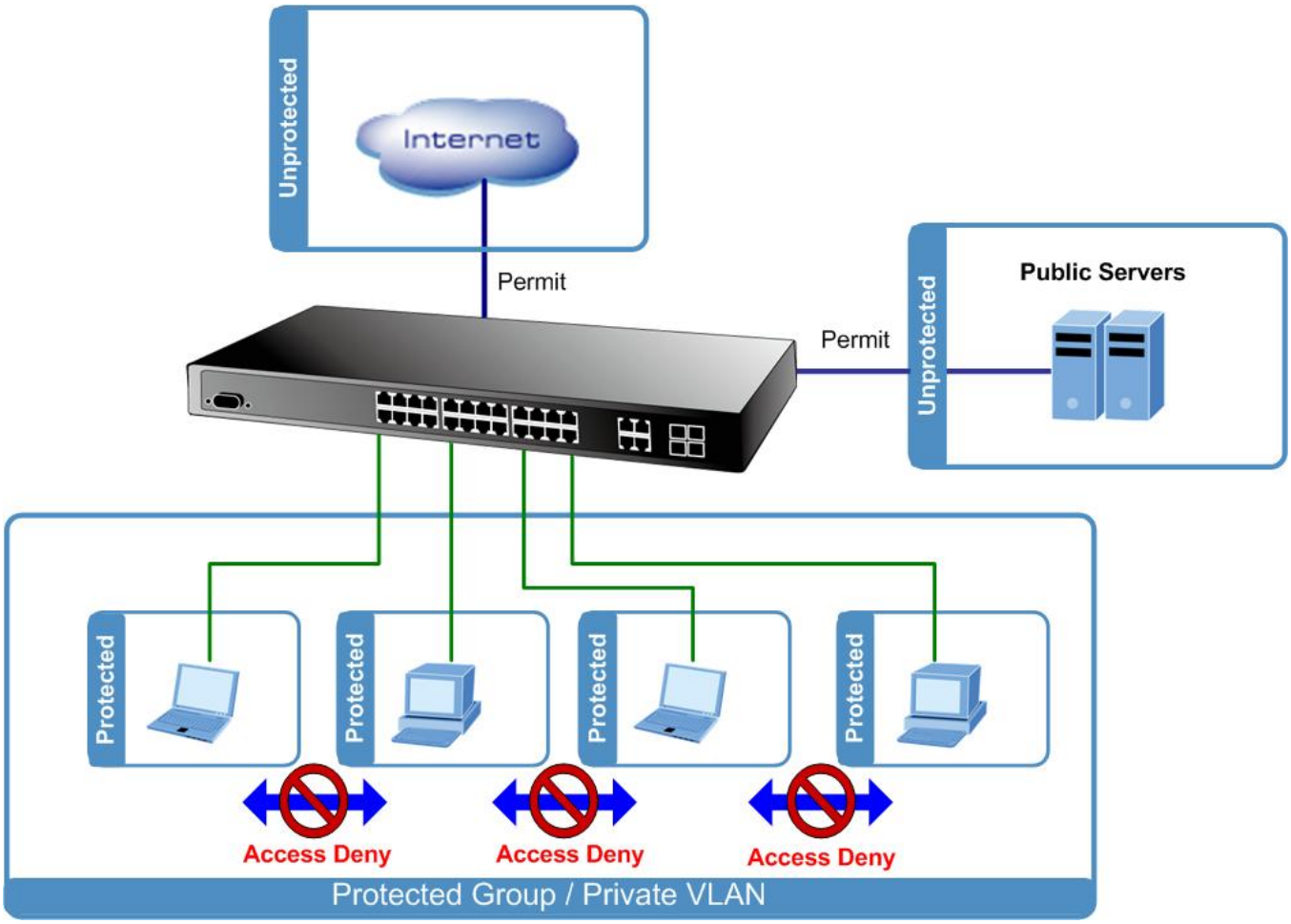
Object	Description
• **Jumbo**	Display the current maximum frame size.

4.3.7 Protected Ports

Overview

When a switch port is configured to be a member of protected group (also called Private VLAN), communication between protected ports within that group can be prevented. Two application examples are provided in this section:

- Customers connected to an ISP can be members of the protected group, 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 protected port group to be applied, the Managed switch must first be configured for standard VLAN operation. Ports in a protected port group fall into one of these two groups:

- **Promiscuous (Unprotected) 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 (Protected) ports**
  - — Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN
  - — Ports which can receive traffic from only promiscuous ports in the private VLAN

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. The Port Isolation Configuration screen in Figure 4-3-13 & Figure 4-3-14 appears.

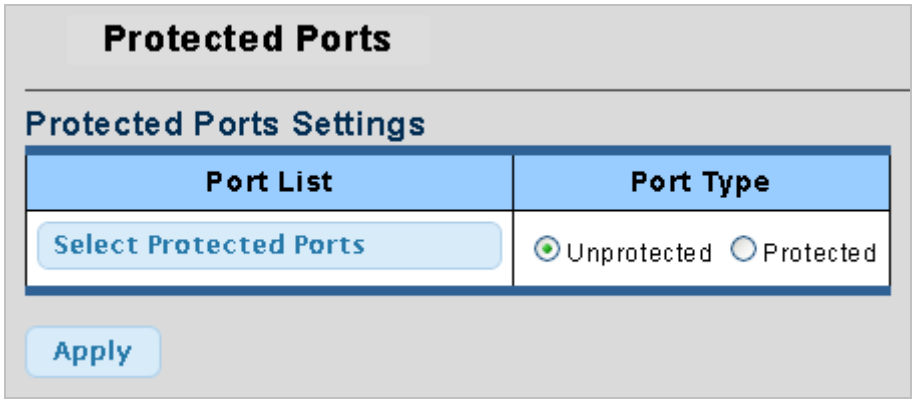


Figure 4-3-13 Protected Ports Settings page screenshot

The page includes the following fields:

Object	Description
• **Port List**	Select port number for this drop down list.
• **Port Type**	Displays protected port types. - **Protected**: 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. - **Unprotected**: A promiscuous port can communicate with all the interfaces within a private VLAN. This is the default setting.

Buttons

Apply: Click to apply changes.

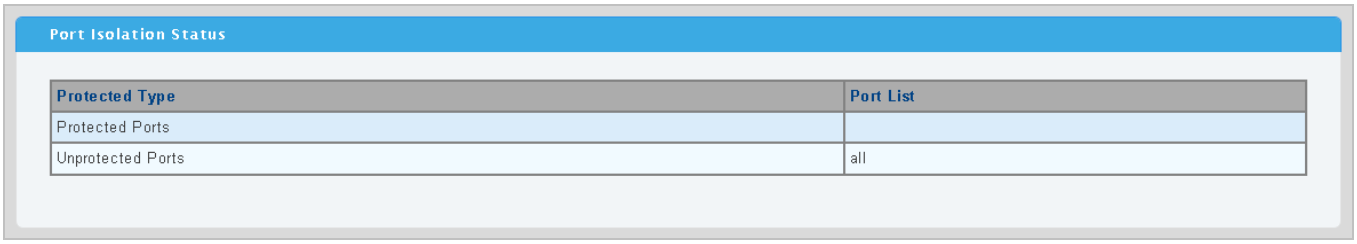


Figure 4-3-14 Port Isolation Status page screenshot

The page includes the following fields:

Object	Description
• **Protected Type**	Display the current protected type.
• **Port List**	Display the current port list.

4.3.8 Bandwidth Control

Configure the switch port rate limit for the switch port on this page. The settings relate to the currently selected stack unit, as reflected by the page header.

4.3.8.1 Preamble Setting

This page provides to select the ingress and egress preamble. The Bandwidth Control Peramble Setting screen in Figure 4-3-15 & Figure 4-3-16 appears.

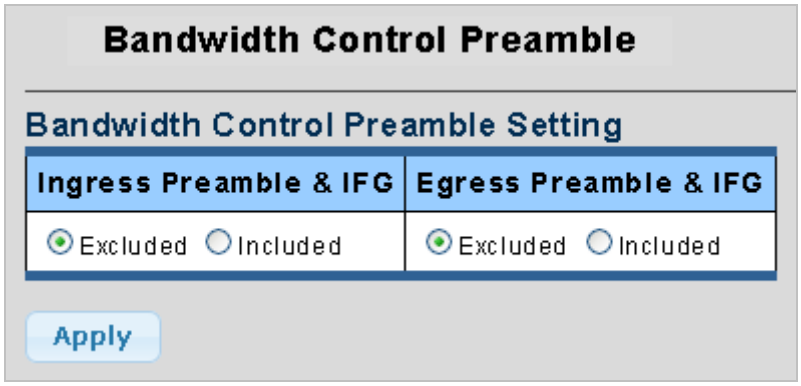


Figure 4-3-15 Bandwidth Control Peramble Setting page screenshot

Buttons

Apply: Click to apply changes.

The page includes the following fields:

Object	Description
• **Ingress Preamble & IFG**	Select Ingress preamble & IFG mode.
• **Egress Preamble & IFG**	Select egress preamble & IFG mode.

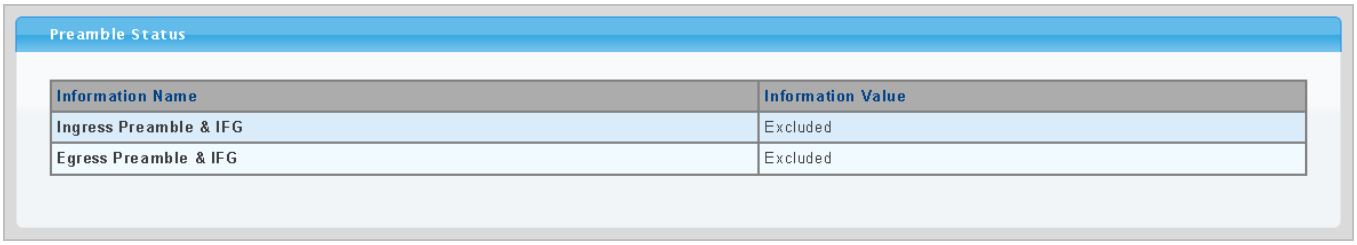


Figure 4-3-16 Preamble Status page screenshot

The page includes the following fields:

Object	Description
• **Information Name**	Display the current information name.
• **Information Value**	Display the current information value.

4.3.8.2 Port Rate Setting

This page provides to configuration port rate parameter. The Bandwidth Control Port Rate screen in Figure 4-3-17 & Figure 4-3-18 appears.

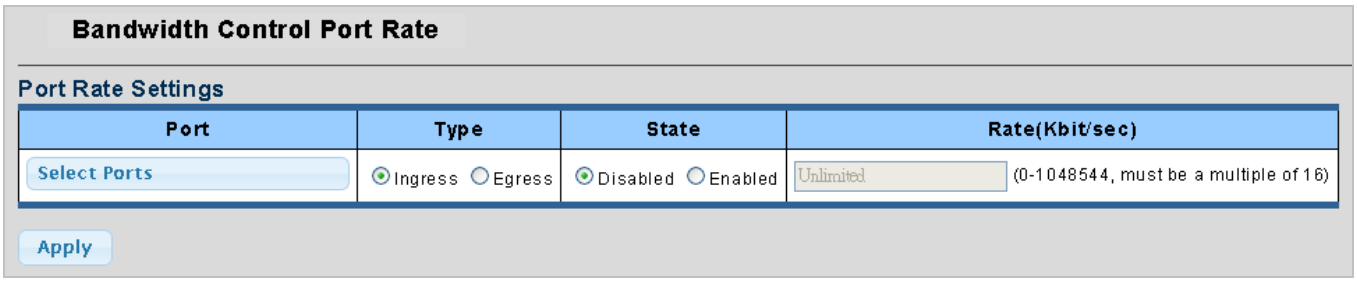


Figure 4-3-17 Port Rate Settings page screenshot

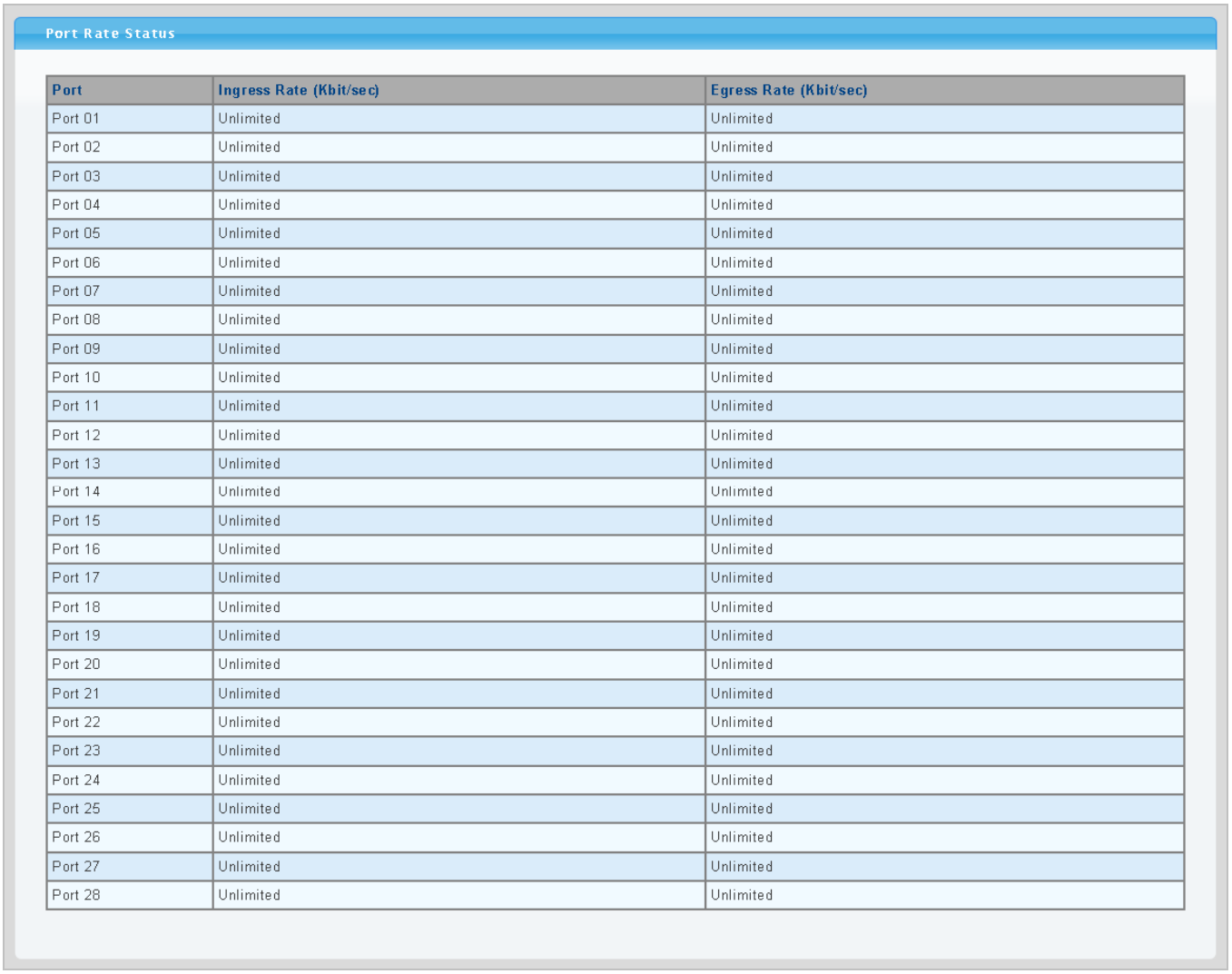
Buttons

Apply: Click to apply changes.

The page includes the following fields:

Object	Description
• **Port**	Select port number for this drop down list.
• **Type**	Allow ingress or egress type for port rate. **Ingress**: traffic control for incoming. **Egress**: traffic control for outgoing.
• **State**	Enable or disable the port rate policer. The default value is "Disabled".

• **Rate (Kbit/sec)**	Configure the rate for the port policer. The default value is "unlimited". Valid values are in the range 0 to 1048544.



Port Rate Status

Port	Ingress Rate (Kbit/sec)	Egress Rate (Kbit/sec)
Port 01	Unlimited	Unlimited
Port 02	Unlimited	Unlimited
Port 03	Unlimited	Unlimited
Port 04	Unlimited	Unlimited
Port 05	Unlimited	Unlimited
Port 06	Unlimited	Unlimited
Port 07	Unlimited	Unlimited
Port 08	Unlimited	Unlimited
Port 09	Unlimited	Unlimited
Port 10	Unlimited	Unlimited
Port 11	Unlimited	Unlimited
Port 12	Unlimited	Unlimited
Port 13	Unlimited	Unlimited
Port 14	Unlimited	Unlimited
Port 15	Unlimited	Unlimited
Port 16	Unlimited	Unlimited
Port 17	Unlimited	Unlimited
Port 18	Unlimited	Unlimited
Port 19	Unlimited	Unlimited
Port 20	Unlimited	Unlimited
Port 21	Unlimited	Unlimited
Port 22	Unlimited	Unlimited
Port 23	Unlimited	Unlimited
Port 24	Unlimited	Unlimited
Port 25	Unlimited	Unlimited
Port 26	Unlimited	Unlimited
Port 27	Unlimited	Unlimited
Port 28	Unlimited	Unlimited

Figure 4-3-18 Port Rate Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Ingress Rate (Kbit/sec)**	Display the current ingress rate.
• **Egress Rate (Kbit/sec)**	Display the current egress rate.

4.4 Link Aggregation

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

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

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

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

The device supports the following Aggregation links :

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

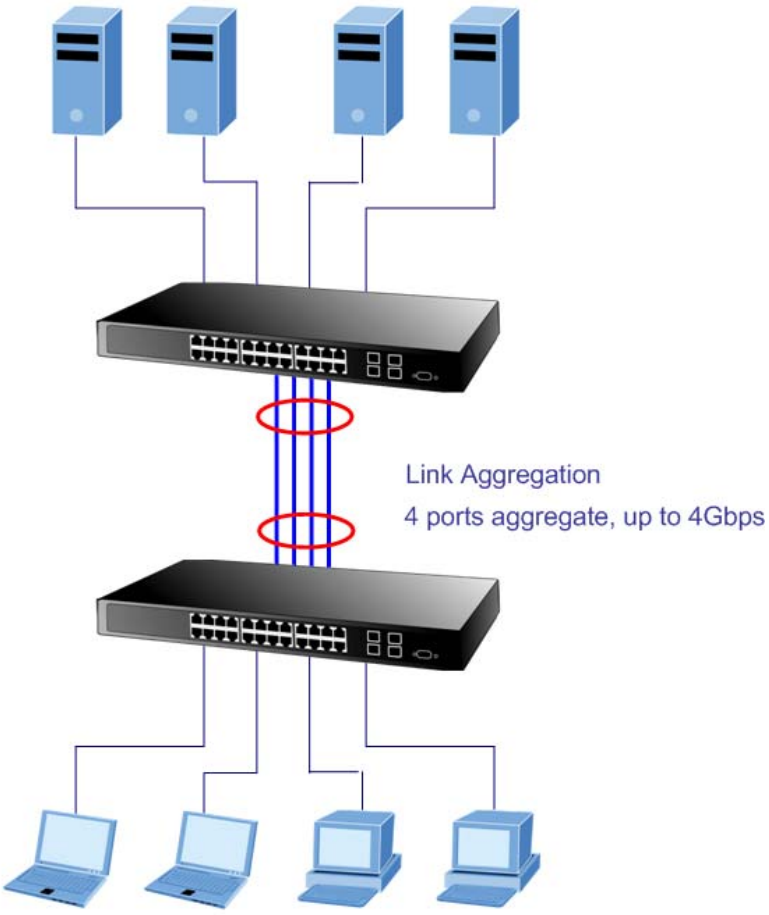


Figure 4-4-1 Link Aggregation

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

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 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 8 ports to be aggregated at the same time. The Managed Switch support Gigabit Ethernet ports (up to 6 groups). If the group is defined as a LACP static link aggregationing group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregationing group, then the number of ports must be the same as the group member ports.

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

Trunk Group	Configures Trunk group configuration settings
LACP Configuration	Configures LACP configuration settings

4.4.1 Trunk Group

This page is used to configure the turnk group. The Trunk Group Configuration screen in Figure 4-4-2 & Figure 4-4-3 appears.

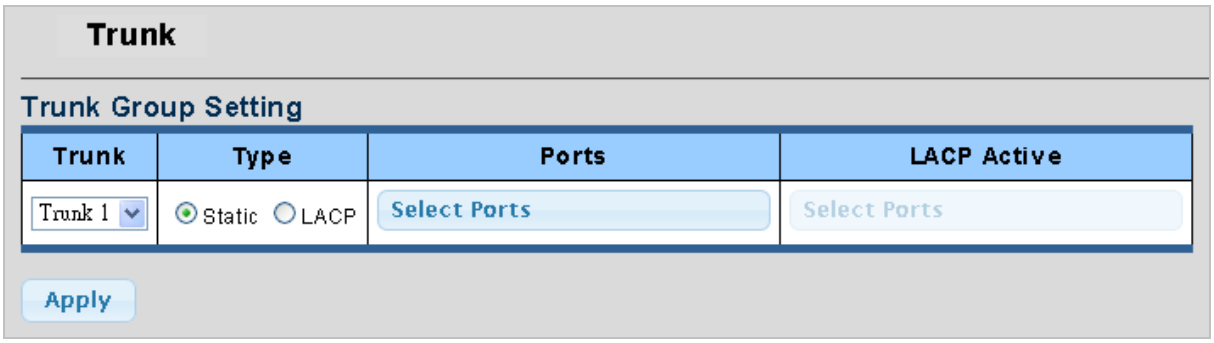


Figure 4-4-2 Trunk Group Setting page screenshot

The page includes the following fields:

Object	Description
• **Trunk**	Select trunk number for this drop down list.
• **Type**	Indicates the trunk type. This field is only valid for stackable switches. **Static**: Force aggregared selected ports to be a trunk group. **LACP**: LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.
• **Ports**	Select port number for this drop down list to esatablish Link Aggregation.
• **LACP Active**	Indicates 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).

Buttons

Apply: Click to apply changes.

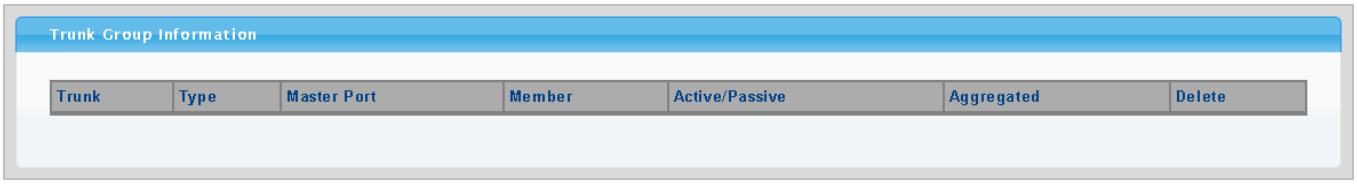


Figure 4-4-3 Trunk Group Information page screenshot

The page includes the following fields:

Object	Description
• **Trunk**	Display the current trunk entry.
• **Type**	Display the current trunk type.
• **Master Port**	Display the current master port.
• **Member**	Display the current member of link aggregation.
• **Active/Passive**	Display the current trunk role.
• **Aggregated**	Display the current aggregated status.
• **Delete**	Click to delete the trunk group entry.

4.4.2 LACP Configuration

This page is used to configure the LACP Configruation. The LACP Configuration screen in Figure 4-4-4 & Figure 4-4-5 appears.

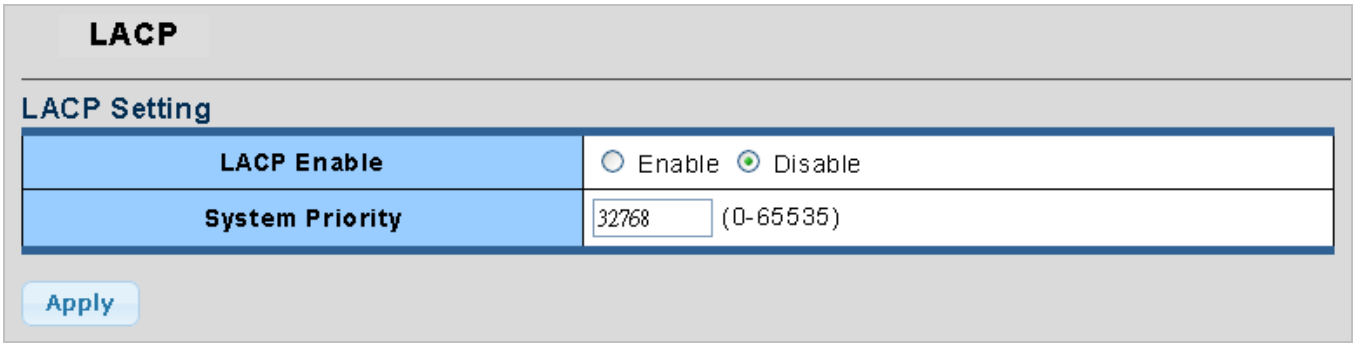


Figure 4-4-4 LACP Setting page screenshot

The page includes the following fields:

Object	Description
• **LACP Enable**	Enable or disable the LACP function. The default value is "Disabled".
• **System Priority**	A value which is used to identify the active LACP. The Managed Switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.

Buttons

Apply: Click to apply changes.

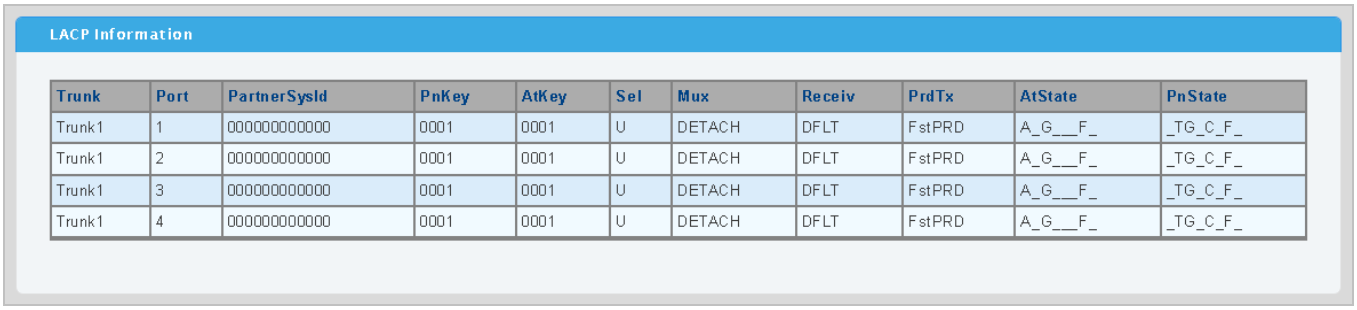


Figure 4-4-5 LACP Information page screenshot

The page includes the following fields:

Object	Description
• **Trunk**	Display the current trunk ID.
• **Port**	Display the current port number.
• **PartnerSysId**	The system ID of link partner. This field would be updated when the port receives LACP PDU from link partner.
• **PnKey**	Port key of partner. This field would be updated when the port receives LACP PDU from link partner.
• **AtKey**	Port key of actor. The key is designed to be the same as trunk ID.
• **Sel**	LACP selection logic status of the port. "S" means selected, "U" means unselected, and "D" means standby.
• **Mux**	LACP mux state machine status of the port. "DETACH" means the port is in detach state, "WAIT" means waiting state, "ATTACH" means attach state, "CLLCT" means collecting state, "DSTRBT" means distributing state.
• **Receiv**	LACP receive state machine status of the port. "INIT" means the port is in initialize state, "PORTds" means port disabled state, "EXPR" means expired state, "LACPds" means LACP disabled state, "DFLT" means defaulted state, "CRRNT" means current state.
• **PrdTx**	LACP periodic transmission state machine status of the port. "no PRD" means the port is in no periodic state, "FstPRD" means fast periodic state, "SlwPRD" means slow periodic state, "PrdTX" means periodic TX state.
• **AtState**	The actor state field of LACP PDU description. The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired". The contents could be true or false. If the contents are false, the web shows "_"; if the contents are true, the web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.
• **PnState**	The partner state field of LACP PDU description. The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired". The contents could be true or false. If the contents are false, the web shows "_"; if the contents are true, the web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.

4.5 VLAN

4.5.1 VLAN Overview

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

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

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

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
2. The 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:

- **VLAN Swithcing** Configures VLAN Swithcing settings
- **VLAN Port Configuation** Configuration VLAN Port Configuration settings
- **QinQ** Enables 802.1Q (QinQ) Tunneling

4.5.2 IEEE 802.1Q VLAN

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

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

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

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
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices

IEEE 802.1Q Standard

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

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

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

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

Some relevant terms:

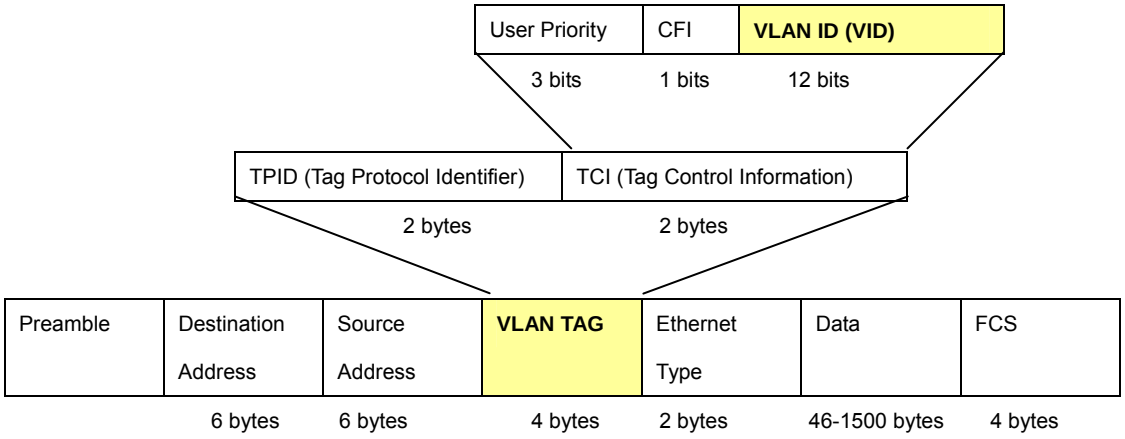
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN Tags

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

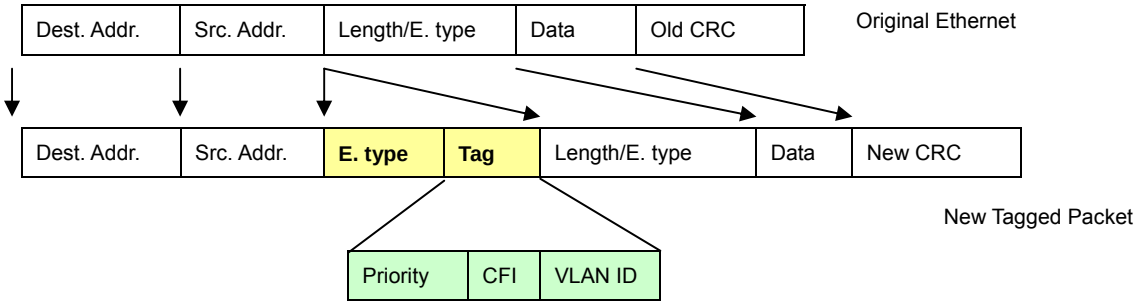
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



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

Adding an IEEE802.1Q Tag



■ Port VLAN ID

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

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

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of

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

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

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

Default VLANs

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

Assigning Ports to VLANs

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

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

VLAN Classification

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

Port Overlapping

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

Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users

assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

4.5.3 VLAN Switching

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.

Understand nomenclature of the Switch

IEEE 802.1Q Tagged and Untagged

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

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

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

Table 4-5-1 Ingress/Egress port with VLAN VID Tag/Untag table

The VLAN Switching screen in Figure 4-5-1 & Figure 4-5-2 appears.

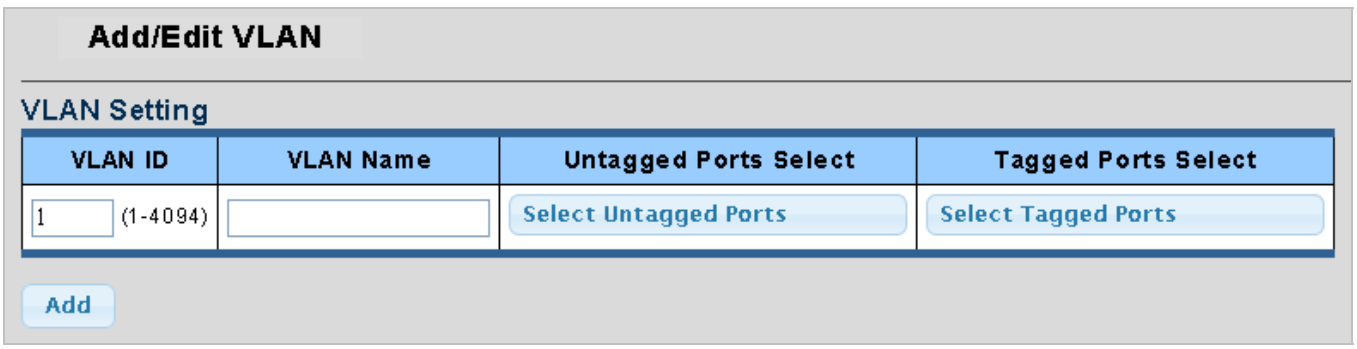


Figure 4-5-1 VLAN Setting page screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Indicates the ID of this particular VLAN.
• **VLAN Name**	Indicates the name of this particular VLAN.
• **Untagged Ports Select**	Select port number for this drop down list to transmit outgoing frames without VLAN-Tagged.
• **Tagged Ports Select**	Select port number for this drop down list to transmit outgoing frames with VLAN-Tagged.

Buttons

Add: Click to add new VLAN.

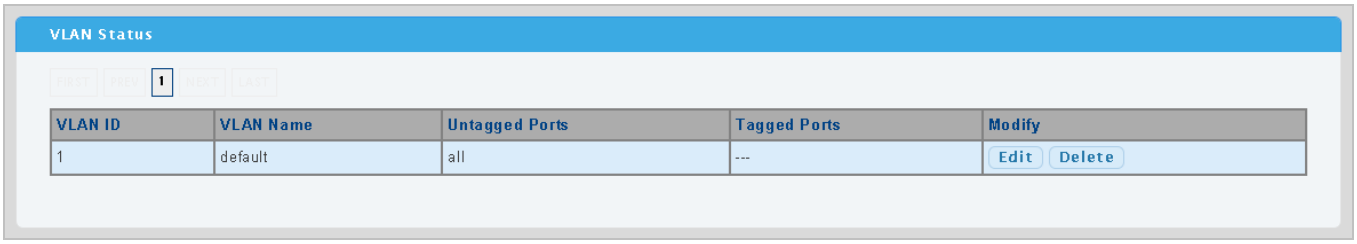


Figure 4-5-2 VLAN Status page screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Display the current VLAN ID entry.
• **VLAN Name**	Display the current VLAN name.
• **Untagged Ports**	Display the current untagged ports.
• **Tagged Ports**	Display the current tagged ports.
• **Modify**	Click to edit or delete the VLAN configuration.

4.5.4 VLAN Port Configuration

This page provides to configuration VLAN Port Configuration parameter. The VLAN Port Configuration screen in Figure 4-5-3 & Figure 4-5-4 appears.

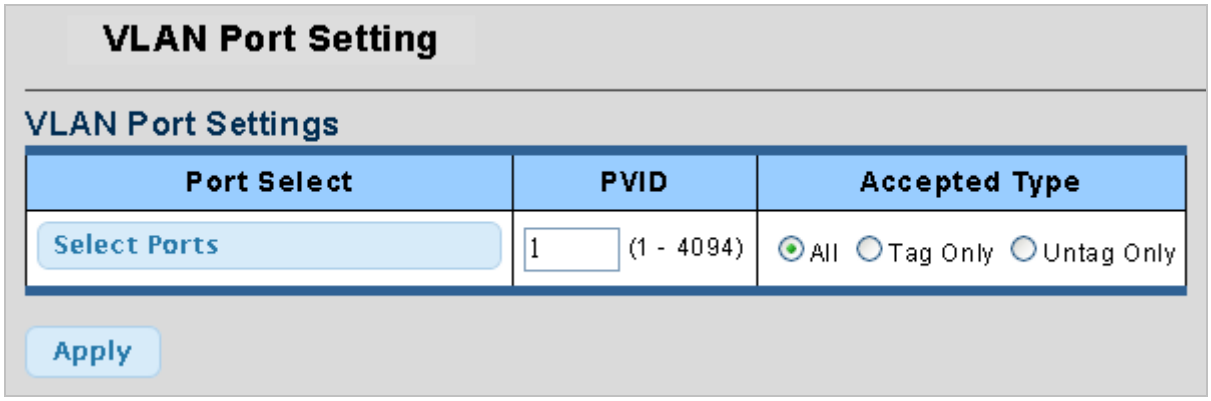


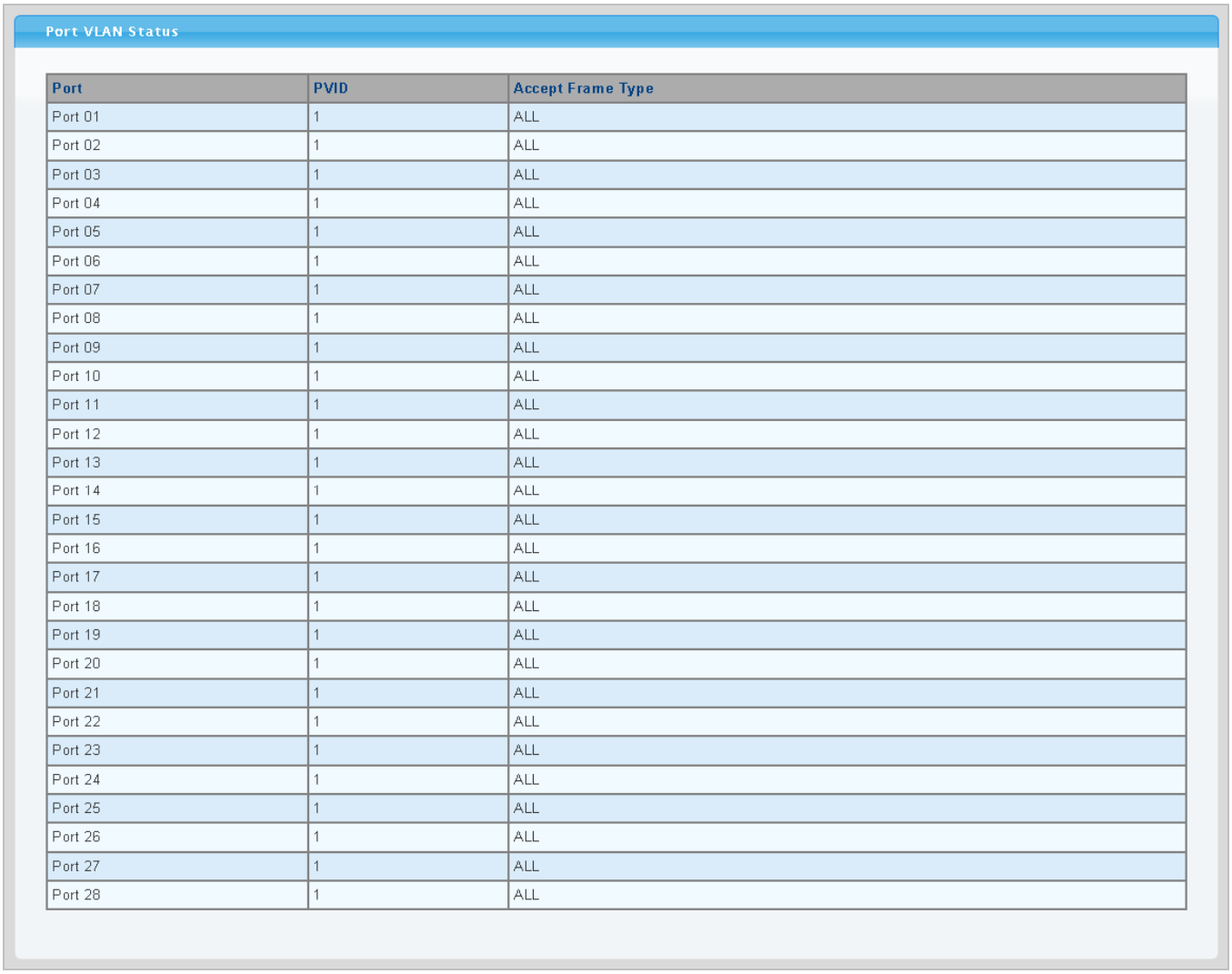
Figure 4-5-3 VLAN Port Settings page screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number for this drop down list to assign PVID and accepted type.
• **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.
• **Accepted Type**	Determines whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.

Buttons

Apply: Click to apply changes.



Port VLAN Status

Port	PVID	Accept Frame Type
Port 01	1	ALL
Port 02	1	ALL
Port 03	1	ALL
Port 04	1	ALL
Port 05	1	ALL
Port 06	1	ALL
Port 07	1	ALL
Port 08	1	ALL
Port 09	1	ALL
Port 10	1	ALL
Port 11	1	ALL
Port 12	1	ALL
Port 13	1	ALL
Port 14	1	ALL
Port 15	1	ALL
Port 16	1	ALL
Port 17	1	ALL
Port 18	1	ALL
Port 19	1	ALL
Port 20	1	ALL
Port 21	1	ALL
Port 22	1	ALL
Port 23	1	ALL
Port 24	1	ALL
Port 25	1	ALL
Port 26	1	ALL
Port 27	1	ALL
Port 28	1	ALL

Figure 4-5-4 Port VLAN Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **PVID**	Display the current PVID.
• **Accept Frame Type**	Displays the current accept frame type.

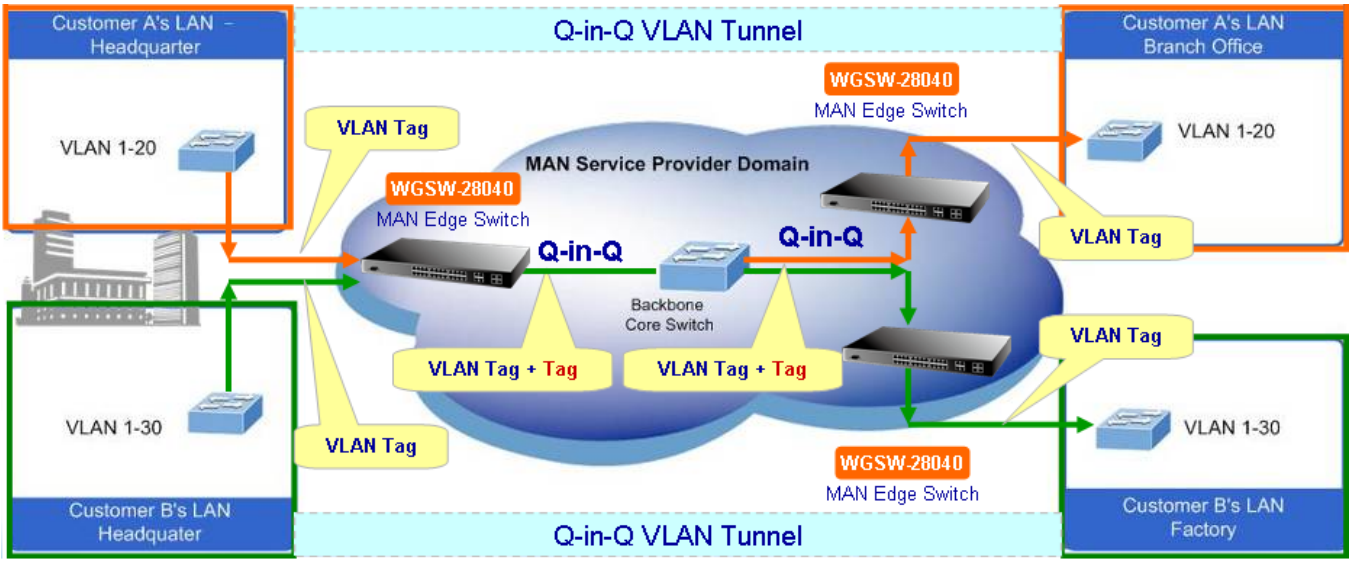
4.5.5 QinQ

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.

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.

4.5.5.1 SVLAN Setting

The SVLAN Setting screen in Figure 4-5-5 & Figure 4-5-6 appears.

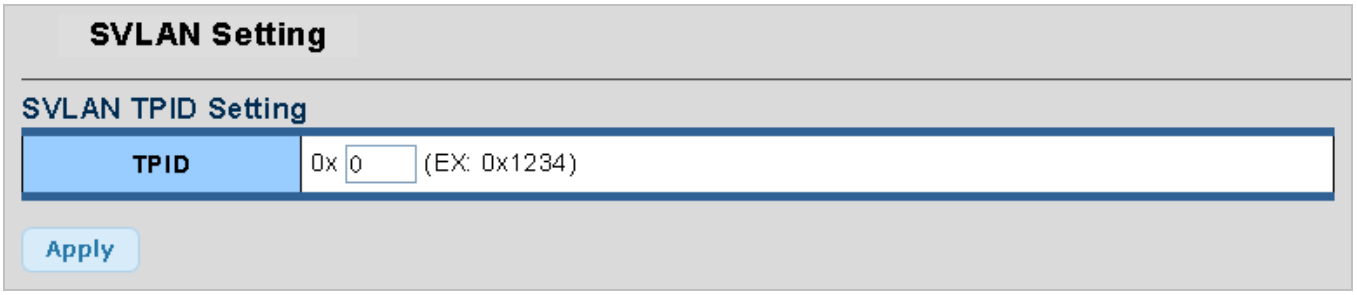


Figure 4-5-5 SVLAN TPID Settings page screenshot

The page includes the following fields:

Object	Description
• **TPID**	The **Tag Protocol Identifier (TPID)** specifies the ethertype of incoming packets on a tunnel access port. • **802.1Q Tag: 8100** • **vMAN Tag: 88A8**

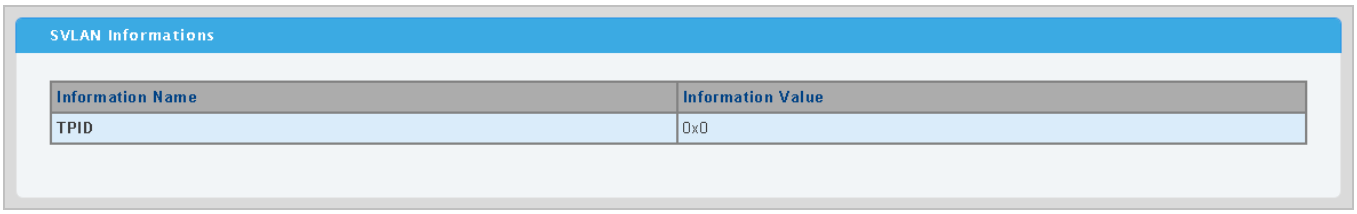


Figure 4-5-6 SVLAN Informations page screenshot

The page includes the following fields:

Object	Description
• **TPID**	Display the current TPID.

4.5.5.2 SVLAN Member Setting

The SVLAN Member Setting screen in Figure 4-5-7 & Figure 4-5-8 appears.

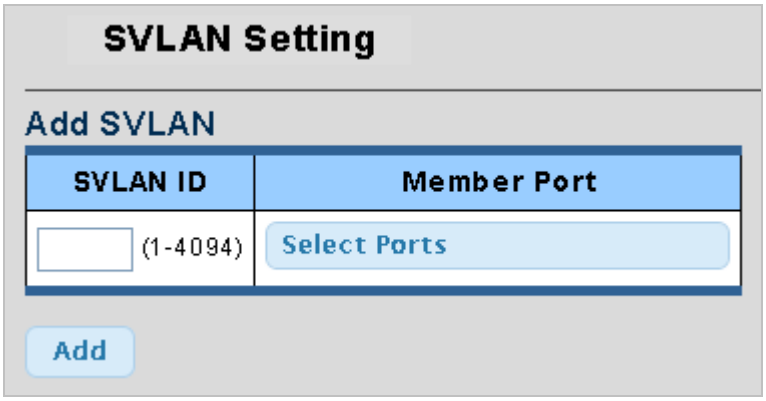


Figure 4-5-7 Add SVLAN page screenshot

The page includes the following fields:

Object	Description
• **SVLAN ID**	Allow assign SVLAN ID for selected port. The range for the SVLAN ID is 1-4094.
• **Member Port**	Select port number for this drop down list to assign SVLAN ID.

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

Buttons

Add: Click to add new SVLAN.

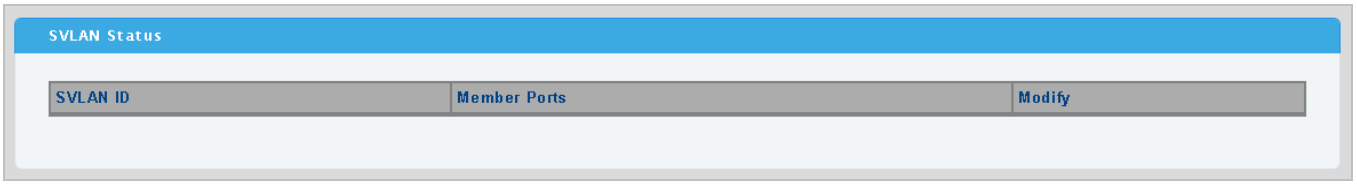


Figure 4-5-8 SVLAN Status page screenshot

The page includes the following fields:

Object	Description
• **SVLAN ID**	Display the current SVLAN ID entry.
• **Member Port**	Display the current member port.
• **Modify**	Click to edit or delete the SVLAN ID.

4.5.5.3 SVLAN PVID Settings

The SVLAN PVID Settings screen in Figure 4-5-9 & Figure 4-5-10 appears.

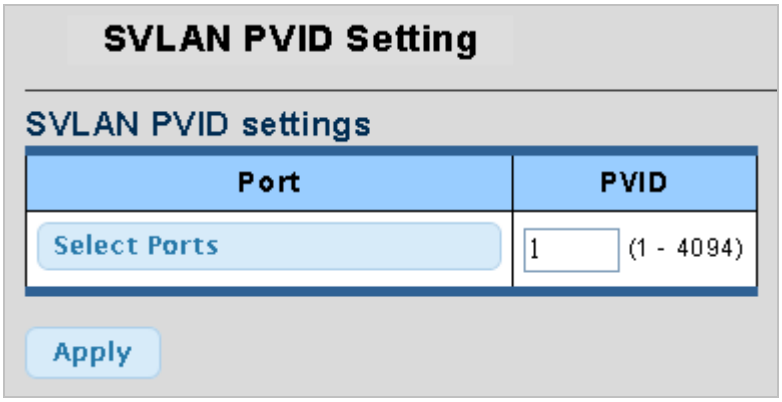


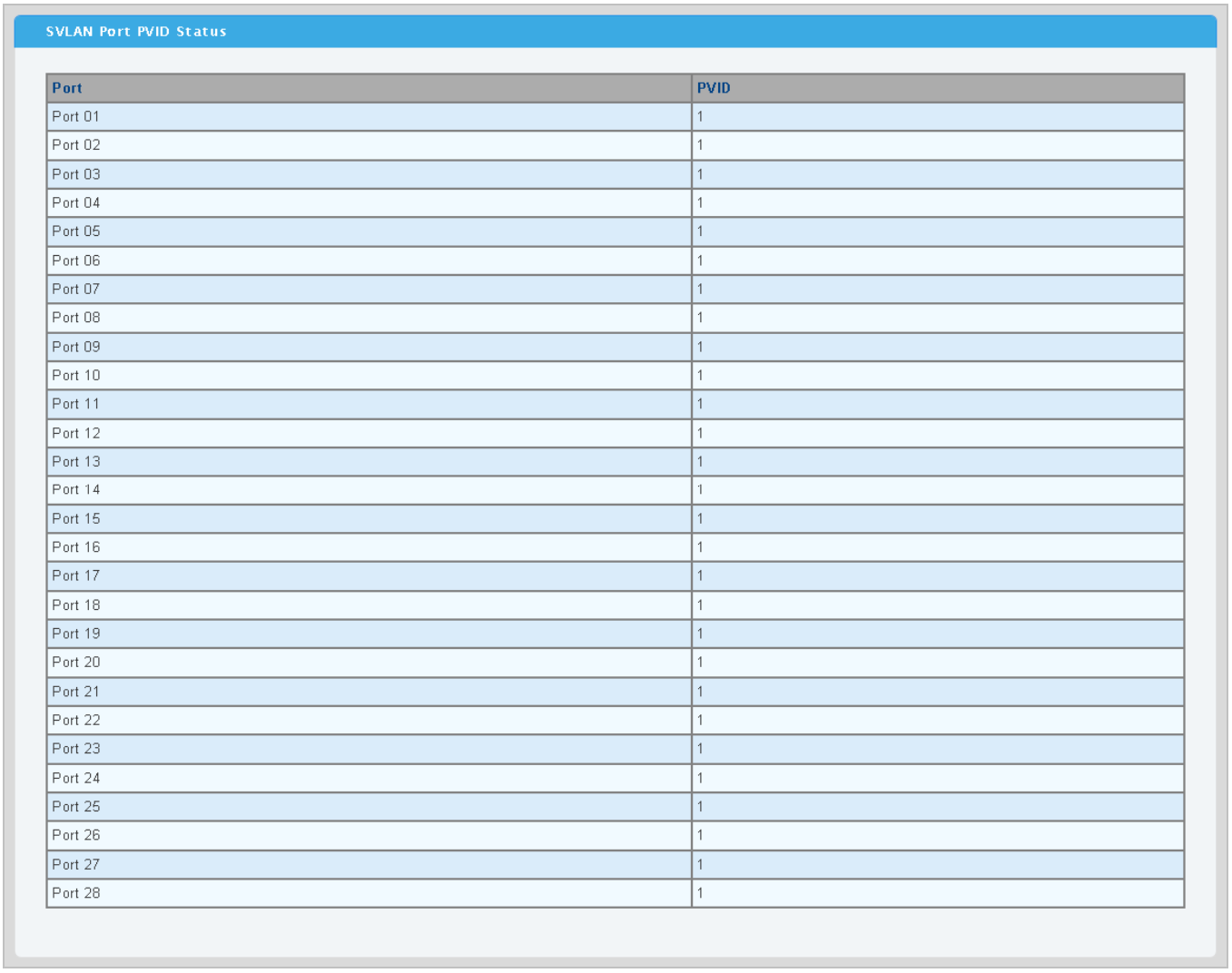
Figure 4-5-9 SVLAN PVID Setting page screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number for this drop down list to assign TPID.
• **PVID**	Allow assign PVID for selected port. The range for the PVID is 1-4094.

Buttons

Apply: Click to apply changes.



SVLAN Port PVID Status

Port	PVID
Port 01	1
Port 02	1
Port 03	1
Port 04	1
Port 05	1
Port 06	1
Port 07	1
Port 08	1
Port 09	1
Port 10	1
Port 11	1
Port 12	1
Port 13	1
Port 14	1
Port 15	1
Port 16	1
Port 17	1
Port 18	1
Port 19	1
Port 20	1
Port 21	1
Port 22	1
Port 23	1
Port 24	1
Port 25	1
Port 26	1
Port 27	1
Port 28	1

Figure 4-5-10 SVLAN Port PVID Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **PVID**	Display the current PVID.

4.5.5.4 SVLAN Service Port

The SVLAN Service Port screen in Figure 4-5-11 & Figure 4-5-12 appears.

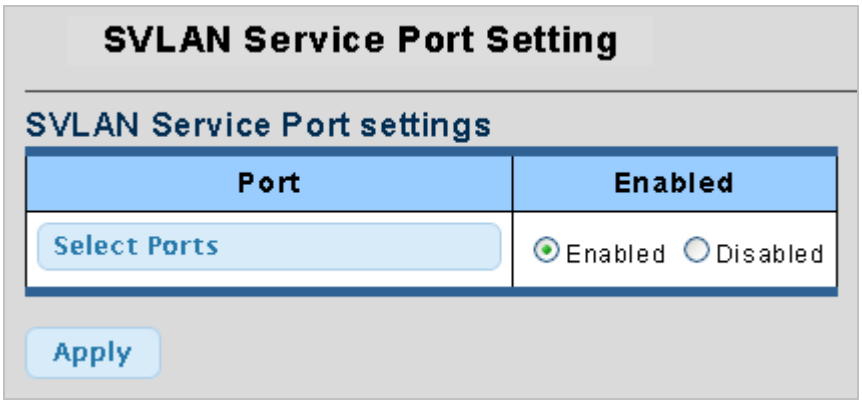


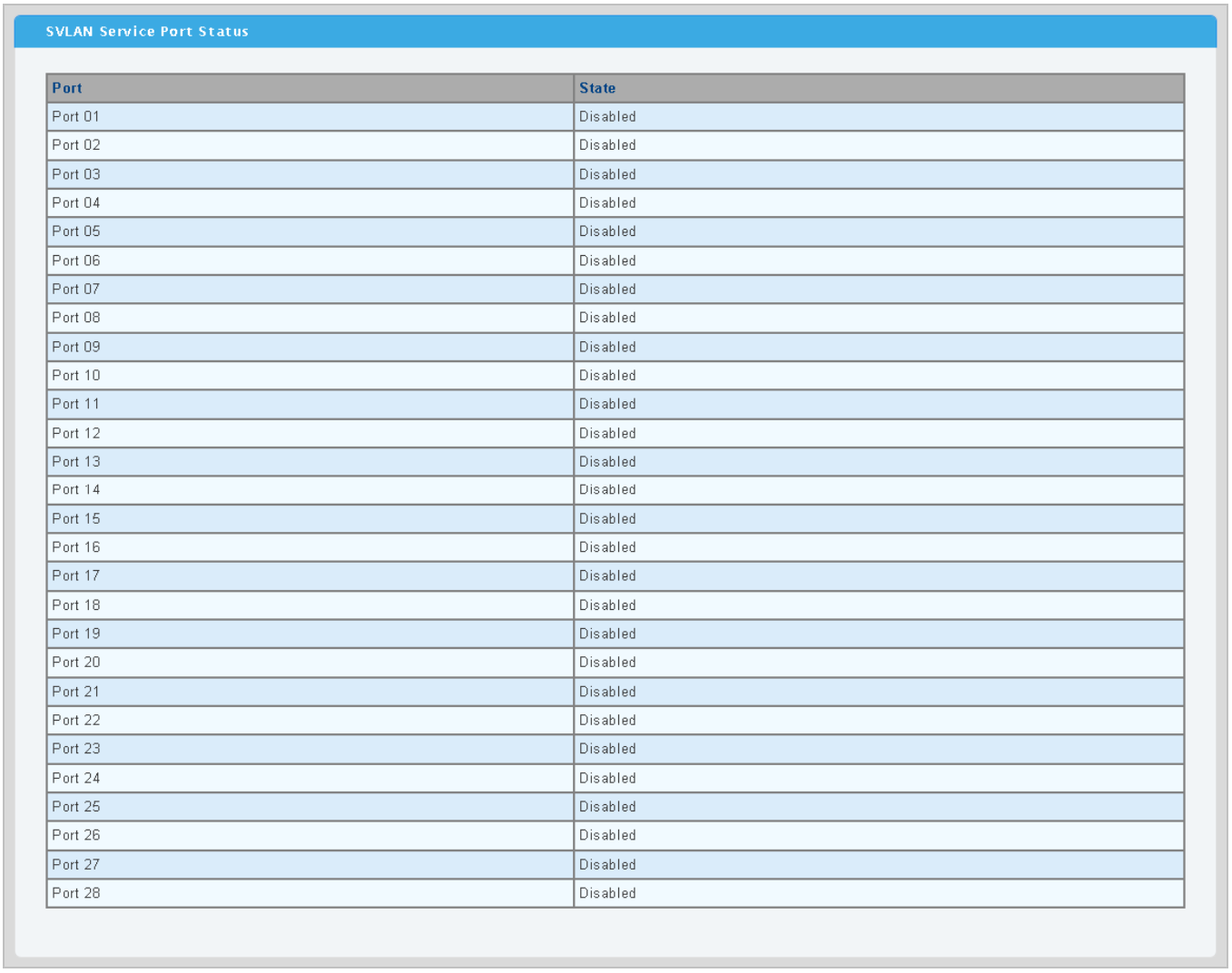
Figure 4-5-11 SVLAN Service Port page screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port number for this drop down list to assign service port.
• **Enabled**	Enable or disable the SVLAN service port.

Buttons

Apply: Click to apply changes.



SVLAN Service Port Status

Port	State
Port 01	Disabled
Port 02	Disabled
Port 03	Disabled
Port 04	Disabled
Port 05	Disabled
Port 06	Disabled
Port 07	Disabled
Port 08	Disabled
Port 09	Disabled
Port 10	Disabled
Port 11	Disabled
Port 12	Disabled
Port 13	Disabled
Port 14	Disabled
Port 15	Disabled
Port 16	Disabled
Port 17	Disabled
Port 18	Disabled
Port 19	Disabled
Port 20	Disabled
Port 21	Disabled
Port 22	Disabled
Port 23	Disabled
Port 24	Disabled
Port 25	Disabled
Port 26	Disabled
Port 27	Disabled
Port 28	Disabled

Figure 4-5-12 SVLAN Service Port Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **State**	Display the current SVLAN Service Port state.

4.5.6 VLAN setting example:

- Separate VLAN

- 802.1Q VLAN Trunk

- Port Isolate (Protected Port)

4.5.6.1 Two separate 802.1Q VLAN

The diagram shows how the Managed Switch handle Tagged and Untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separated VLAN. Each VLAN isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. The screen in Figure 4-5-13 appears and Table 4-5-2 describes the port configuration of the Managed Switches.

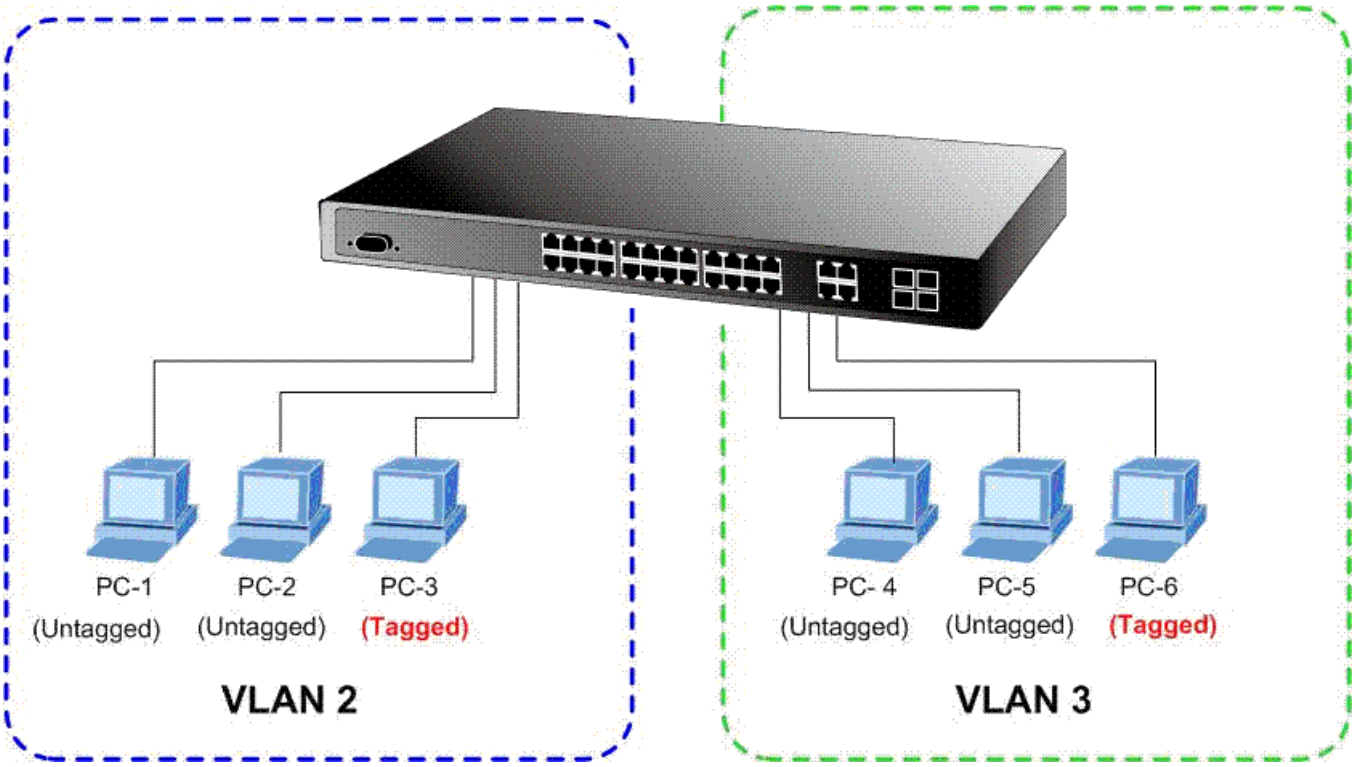


Figure 4-5-13 two separate VLAN diagram

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

Table 4-5-2 VLAN and Port Configuration

The scenario described as follow:

- **Untagged packet entering VLAN 2**

1. While **[PC-1]** transmit an **untagged** packet enters **Port-1**, the Managed Switch will tag it with a **VLAN Tag=2**. **[PC-2]** and **[PC-3]** will received the packet through **Port-2** and **Port-3**.
2. [PC-4],[PC-5] and [PC-6] received no packet.
3. While the packet leaves **Port-2**, it will be stripped away it tag becoming an **untagged** packet.
4. While the packet leaves **Port-3**, it will keep as a **tagged** packet with **VLAN Tag=2**.

- **Tagged packet entering VLAN 2**

5. While **[PC-3]** transmit a **tagged** packet with **VLAN Tag=2** enters **Port-3**, **[PC-1]** and **[PC-2]** will received the packet through **Port-1** and **Port-2**.
6. While the packet leaves **Port-1** and **Port-2**, it will be stripped away it tag becoming an **untagged** packet.

- **Untagged packet entering VLAN 3**

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

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

Setup steps

1. Create VLAN 2 Group

Add VLAN Group 2 with VID=2

Untagged Port : Port-1 & Port-2

Tagged Port : Port-3

2. Create VLAN 3 Group

Add VLAN Group 3 with VID=3

Untagged Port : Port-4 & Port-5

Tagged Port : Port-6

3. Remove VLAN Member for VLAN 1:

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

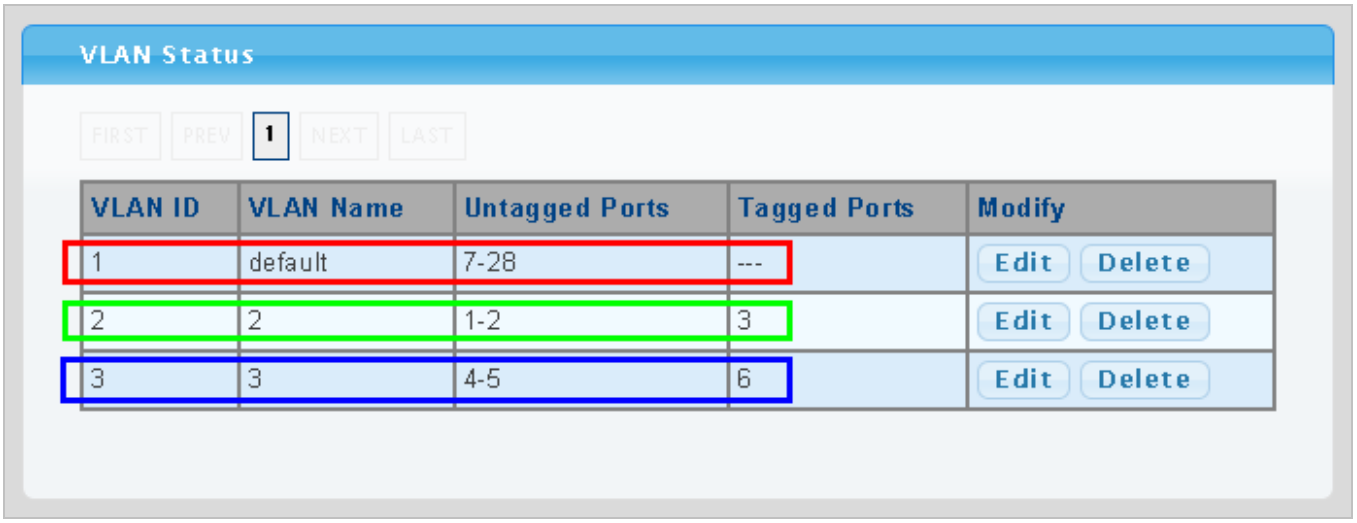


Figure 4-5-12 Add new VLAN group, assign VLAN members for VLAN 2 and VLAN 3 and remove specify ports from VLAN 1 member

Note

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

4. Assign PVID for each port:

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

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

The Per Port VLAN configuration in Figure 4-5-14 appears.

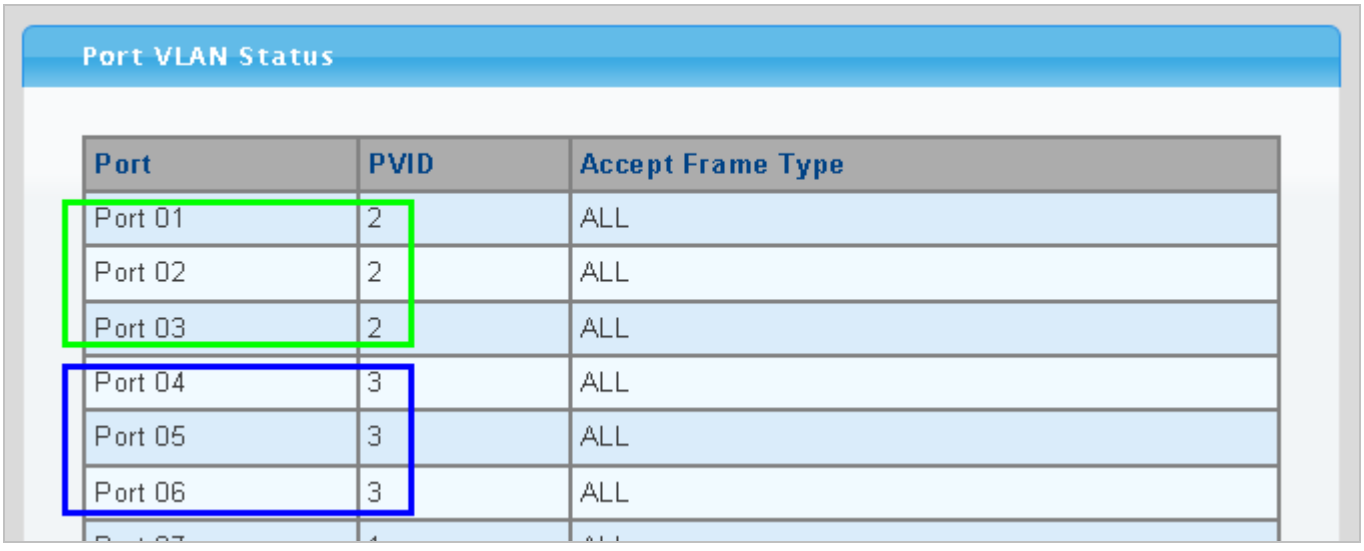
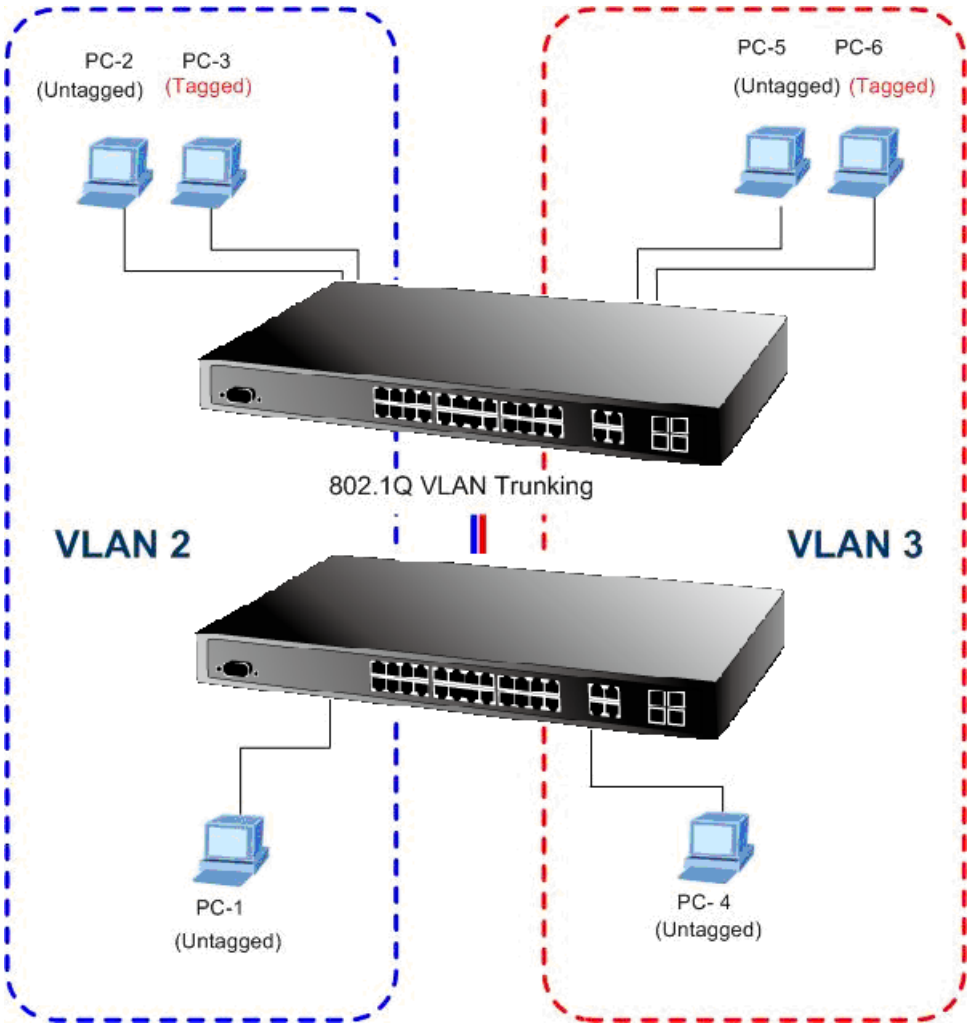


Figure 4-5-14 Port 1-Port 6 VLAN Configuration

4.5.6.2 VLAN Trunking between two 802.1Q aware switch

The most cases are used for "**Uplink**" to other switches. VLANs are separated at different switches, but they need to access with other switches within the same VLAN group. The screen in Figure 4-5-15 appears.



Setup steps

1. **Create VLAN 2 Group**

   Add VLAN Group 2 with VID=2

   Untagged Port : Port-1, Port-2 & Port-3

   Tagged Port : Port-7

2. **Create VLAN 3 Group**

   Add VLAN Group 3 with VID=3

   Untagged Port : Port-4, Port-5 & Port-6

   Tagged Port : Port-7

About the VLAN ports connect to the hosts, please refer to 4.5.7.1 examples. The following steps will focus on the VLAN **Trunk port** configuration.

1. Specify **Port-7** to be the 802.1Q VLAN **Trunk port**.

2. Assign **Port-7** to both **VLAN 2** and **VLAN 3** at the VLAN Member configuration page.

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

4. Assign the VLAN Trunk Port to be the member of each VLAN – which wants to be aggregated. At this sample, add **Port-7** to be **VLAN 2** and **VLAN 3** member port. The screen in Figure 4-5-16 appears.

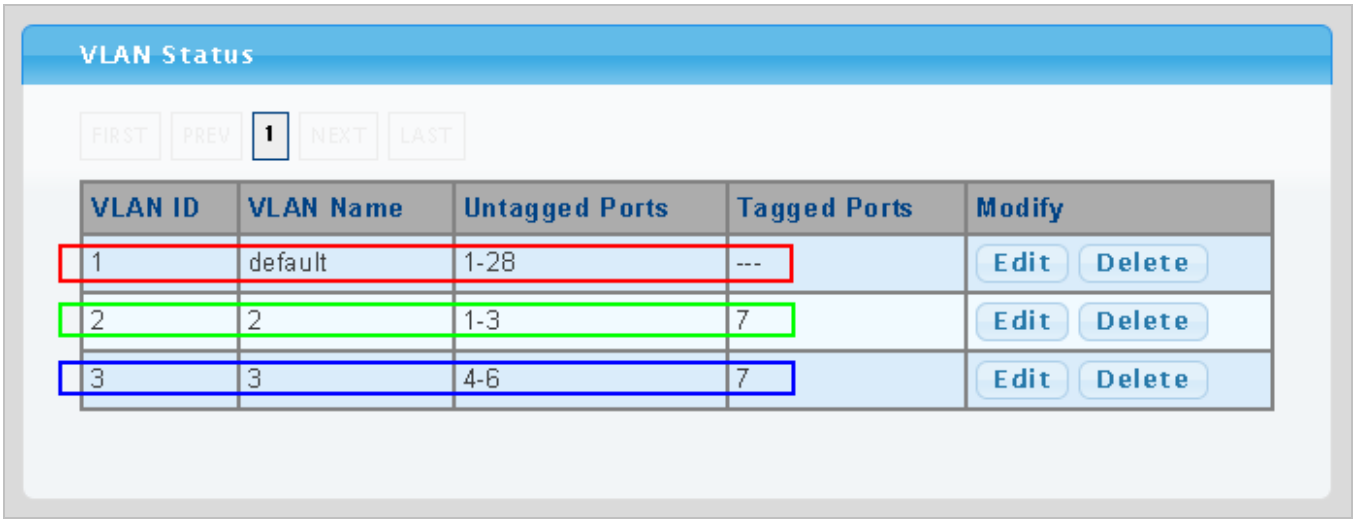


Figure 4-5-16 VLAN overlap port setting & VLAN 1 – The public area member assign

5. Specify **Port-7** to be the 802.1Q VLAN **Trunk port**, and the Trunking port must be a **Tagged** port while egress.

6. Assign PVID for each port:

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

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

The screen in Figure 4-5-17 appears.

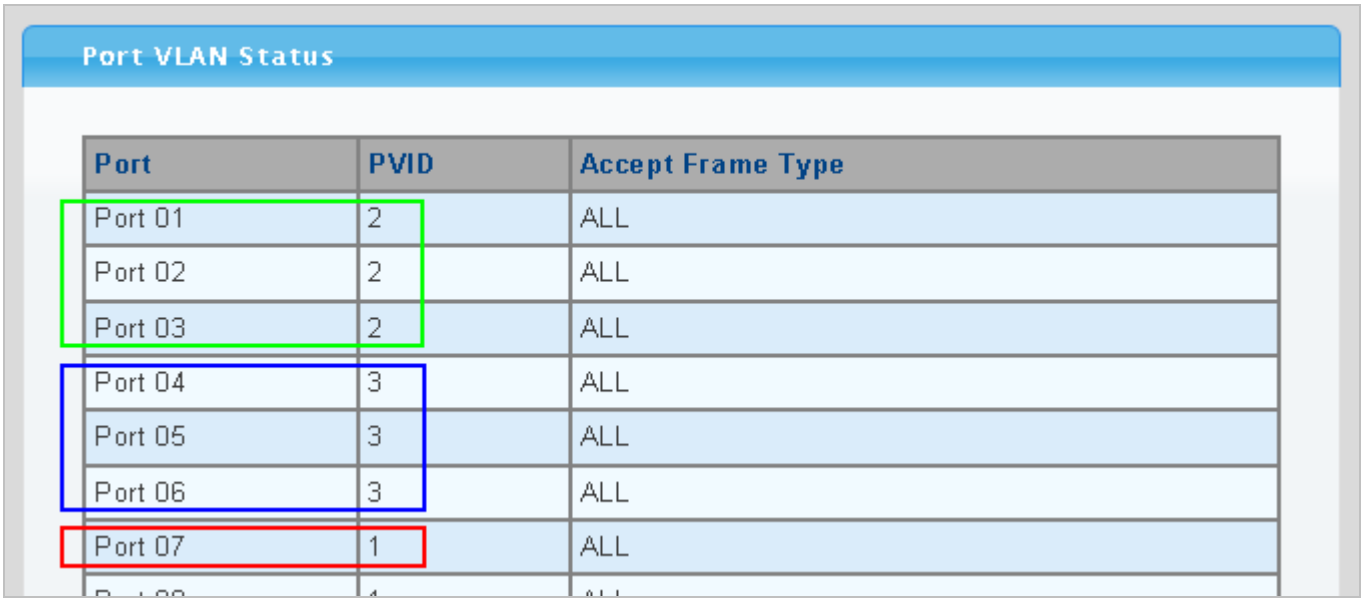


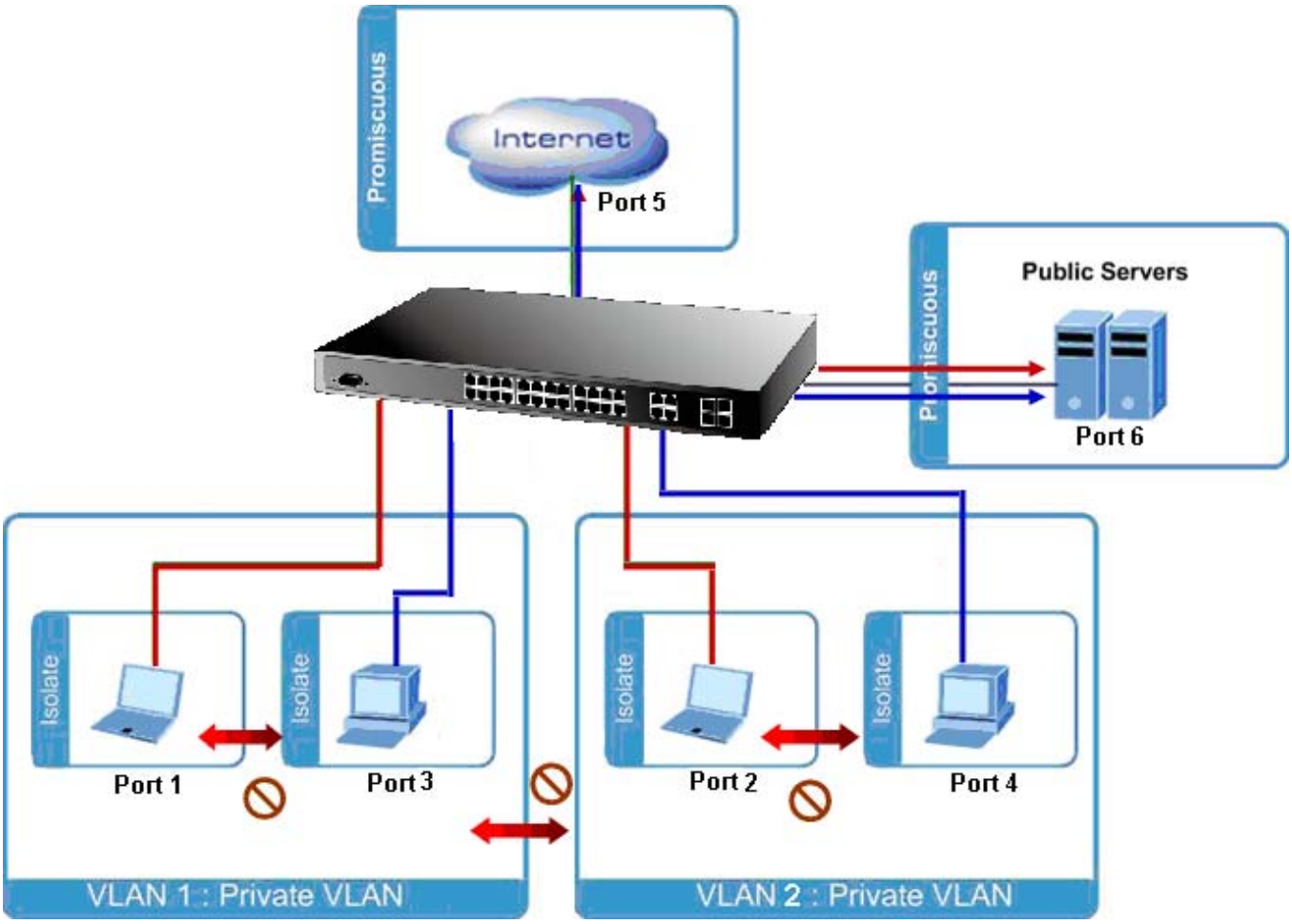
Figure 4-5-17 The configuration of VLAN Trunk port

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

7. Repeat Step 1 to 6, setup the VLAN Trunk port at the partner switch, add more VLANs to join the VLAN trunk and assign the Trunk port to the VLANs.

4.5.6.3 Port Isolate

The diagram shows how the Managed Switch handles isolate and promiscuous ports, and the each PCs are not able to access each other PCs of each isolate port. But they all need to access with the same server/AP/Printer. The screen in Figure 4-5-18 appears. This section will show you how to configure the port for the server – that could be accessed by each isolate port.



Setup steps

1. **Assign egress port list :**

   Protected port list: Port-1~Port-4

   Unprotected port list: Port-5~Port-28

   The screen in Figure 4-5-19 appears.

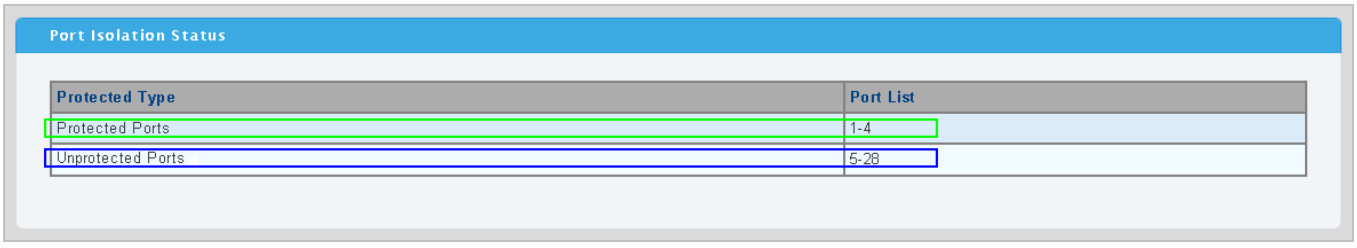


Figure 4-5-19 Protected port setting

4.6 Spanning Tree Protocol

4.6.1 Theory

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

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

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

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

The Switch STP performs the following functions:

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

Bridge Protocol Data Units

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

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

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

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

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

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

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.
When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

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

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

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

A port transitions from one state to another as follows:

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

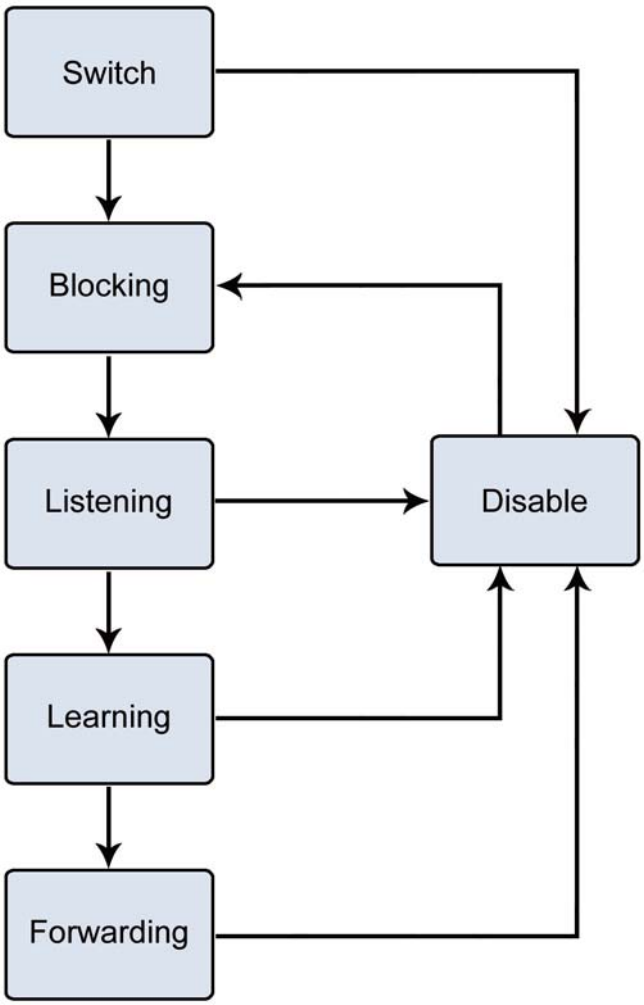


Figure 4-6-1 STP Port State Transitions

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

2. STP Parameters

STP Operation Levels

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

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

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

Parameter	Description	Default Value
Bridge Identifier(Not user configurable 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.

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

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

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

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

Observe the following formulas when setting the above parameters:

Max. Age _ 2 x (Forward Delay - 1 second)

Max. Age _ 2 x (Hello Time + 1 second)

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

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

3. Illustration of STP

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

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

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

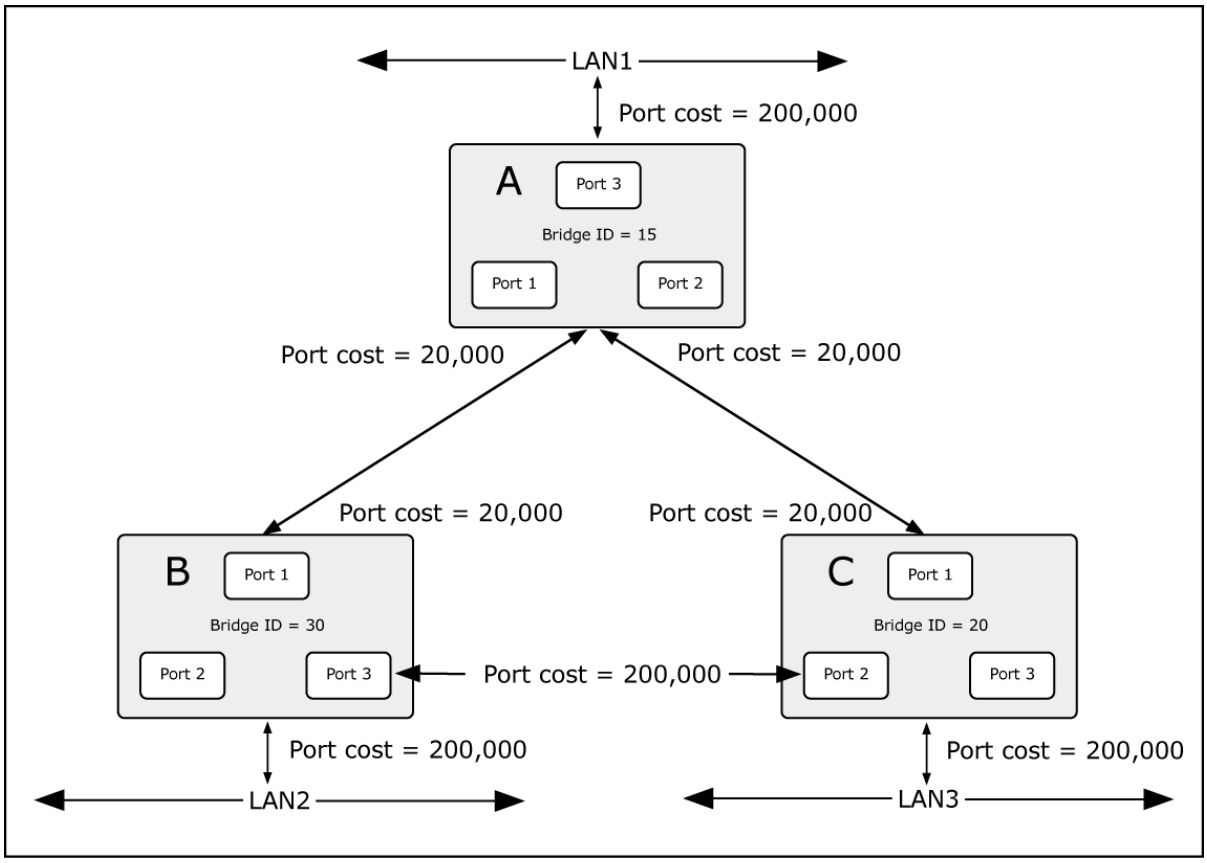


Figure 4-6-2 Before Applying the STA Rules

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

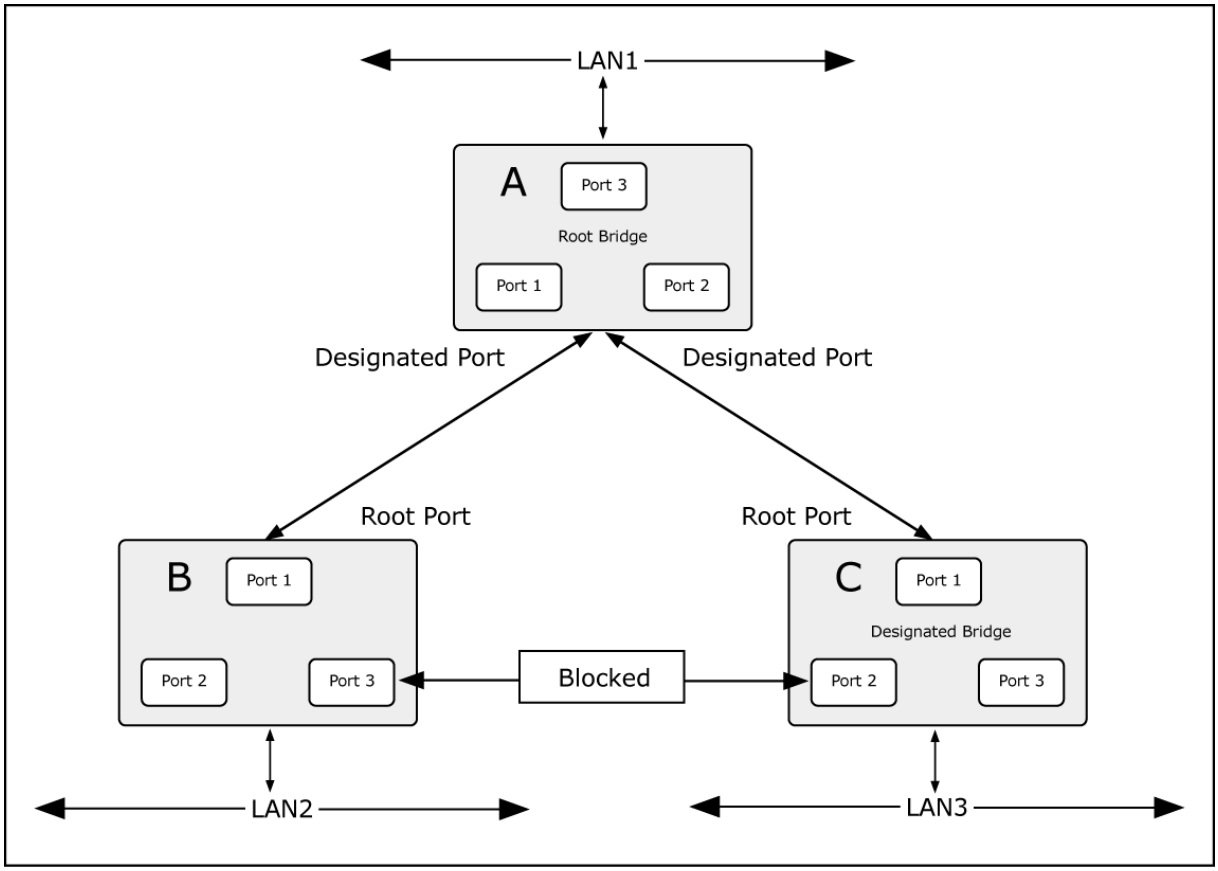


Figure 4-6-3 After Applying the STA Rules

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

This section has the following items:

- **STP Global Setting** Configures STP system settings
- **STP Port Setting** Configuration per port STP settings
- **MST Configuration** Configuration MST configuration
- **MST Instance Setting** Configuration each MST instance settings
- **MST Port Setting** Configuration per port MST setting

4.6.2 STP Global Settings

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch 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.
- **Extension – Multiple Spanning Tree Protocol (MSTP):** Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

The STP Global Settings screen in Figure 4-6-4 & Figure 4-6-5 appears.

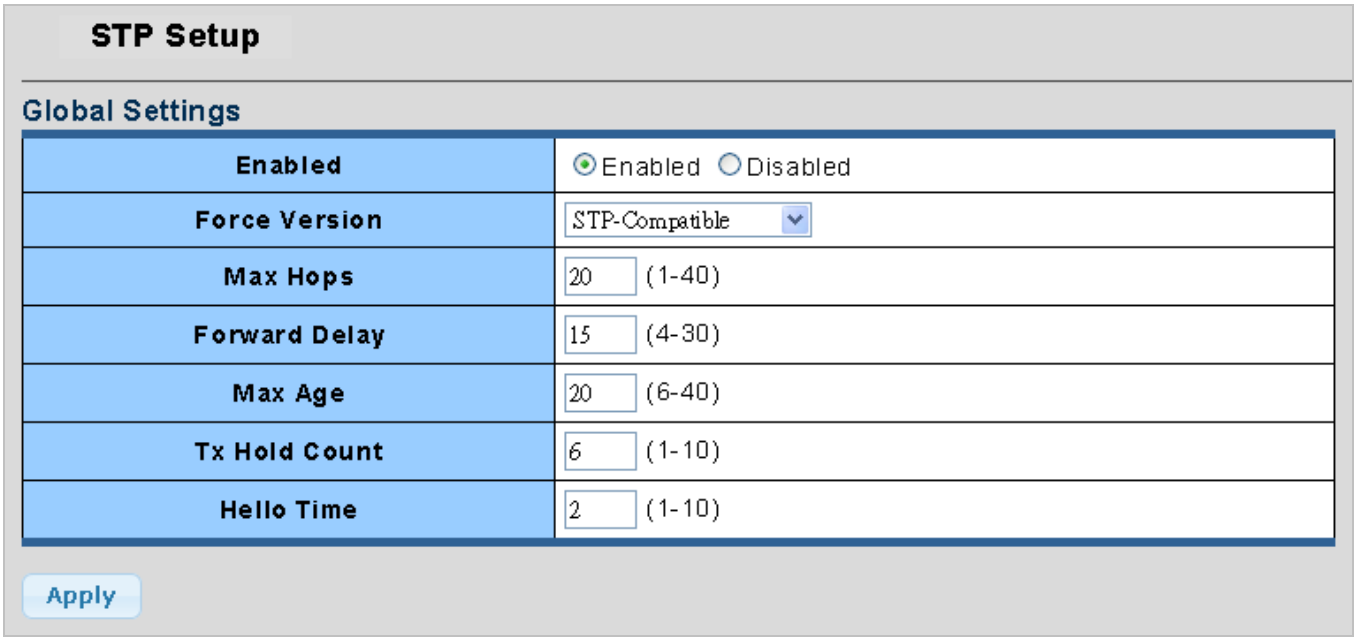


Figure 4-6-4 Global Settings page screenshot

The page includes the following fields:

Object	Description
• **Enable**	Enable or disable the STP function. The default value is "Disabled".
• **Force Version**	The STP protocol version setting. Valid values are **STP-Compatible**, **RSTP-Operation** and **MSTP-Operation**.
• **Max Hop**	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 6 to 40 hops.
• **Forward Delay**	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds -Default: 15 -Minimum: The higher of 4 or [(Max. Message Age / 2) + 1] -Maximum: 30
• **Max Age**	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 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)]
• **Tx Hold Count**	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

• **Hello Time**	The time that controls the switch to send out the BPDU packet to check STP current status. Enter a value between 1 through 10.

Buttons

Apply: Click to apply changes.

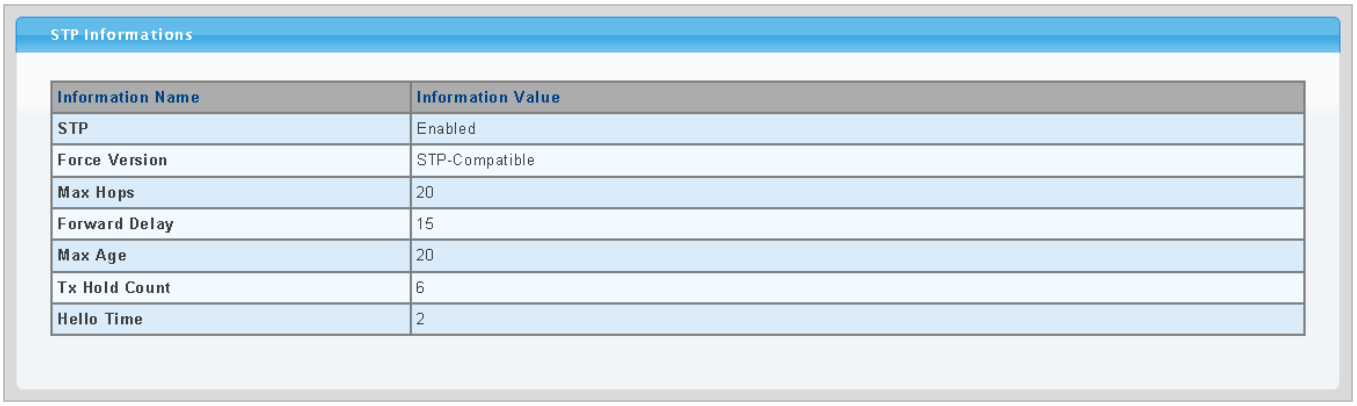


Figure 4-6-5 STP Infirmations page screenshot

The page includes the following fields:

Object	Description
• **STP**	Display the current STP state.
• **Force Version**	Display the current force version.
• **Max Hop**	Display the current Max. hop.
• **Forward Delay**	Display the current forward delay.
• **Max Age**	Display the current Max. age.
• **Tx Hold Count**	Display the current Tx hold count.
• **Hello Time**	Display the current hello time.

4.6.3 STP Port Setting

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

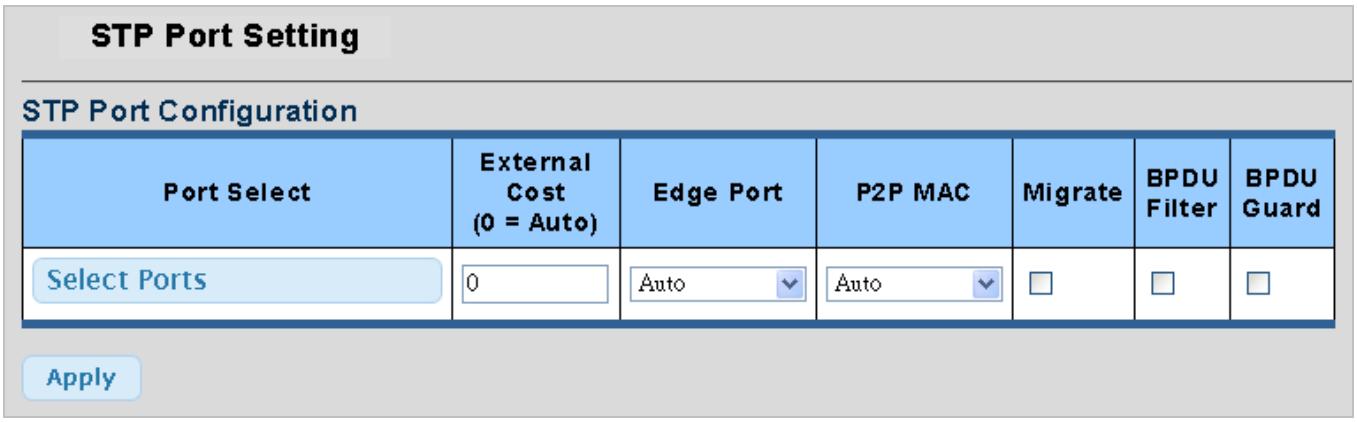


Figure 4-6-6 STP Port Configuration page screenshot

The page includes the following fields:

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

• **BPDU Guard**	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Buttons

Apply: Click to apply changes.

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

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

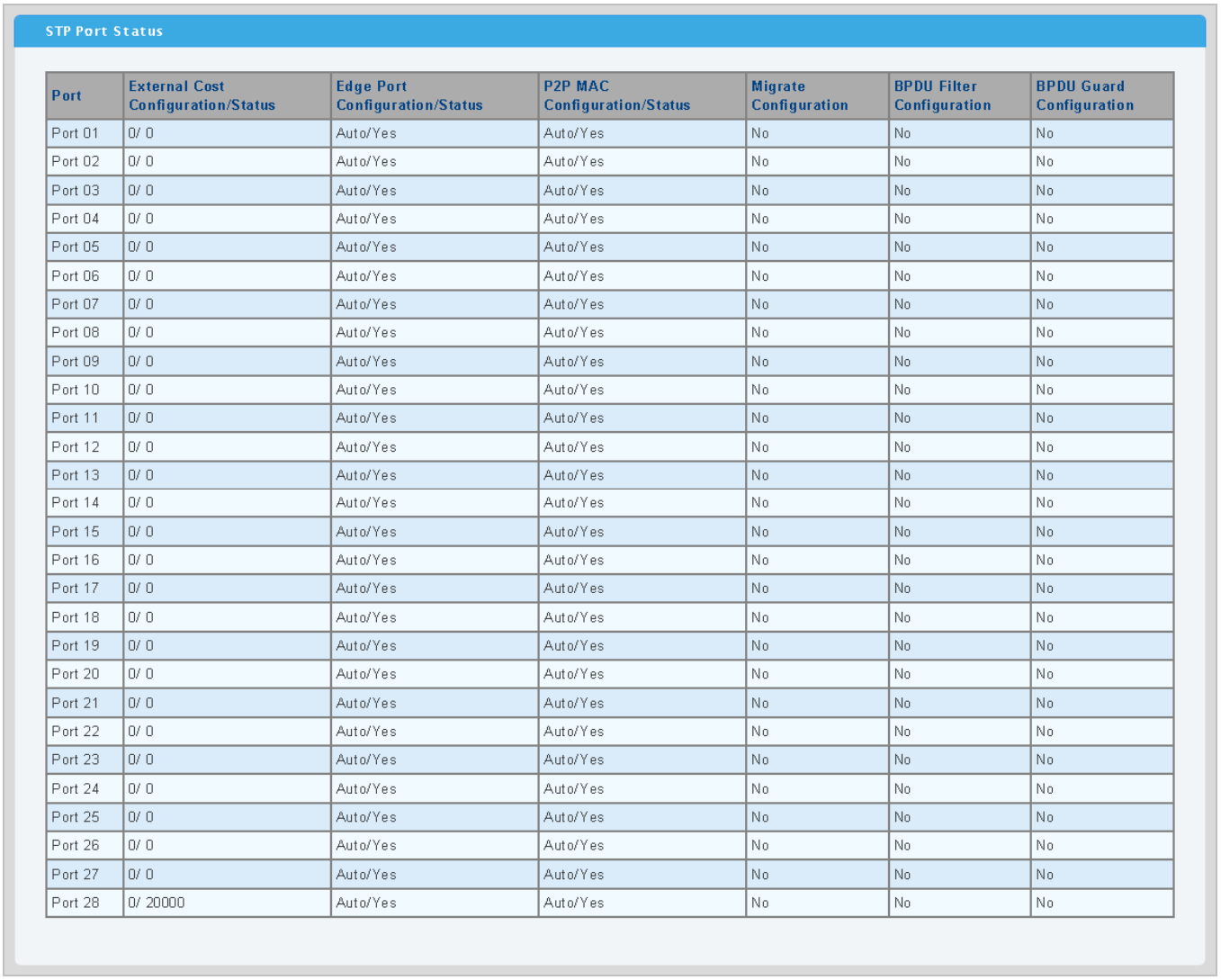
Table 4-6-1 Recommended STP Path Cost Range

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

Table 4-6-2 Recommended STP Path Costs

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

Table 4-6-3 Default STP Path Costs



STP Port Status

Port	External Cost Configuration/Status	Edge Port Configuration/Status	P2P MAC Configuration/Status	Migrate Configuration	BPDU Filter Configuration	BPDU Guard Configuration
Port 01	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 02	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 03	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 04	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 05	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 06	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 07	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 08	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 09	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 10	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 11	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 12	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 13	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 14	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 15	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 16	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 17	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 18	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 19	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 20	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 21	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 22	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 23	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 24	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 25	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 26	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 27	0/ 0	Auto/Yes	Auto/Yes	No	No	No
Port 28	0/ 20000	Auto/Yes	Auto/Yes	No	No	No

Figure 4-6-7 STP Port Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **External Cost Configuration/Status**	Display the current external cost configuration / status.
• **Edge Port Configuration/Status**	Display the current edge port configuration / status.
• **P2P MAC Configuration/Status**	Display the current P2P MAC configuration / status.
• **Migrate Configuration**	Display the current migrate configuration.
• **BPDU Filter Configuration**	Display the current BPDU filter configuration.
• **BPDU Guard Configuration**	Display the current BPDU guard configuration.

4.6.4 MST Configuration

This page allows the user to configure MST Configuration. The MST Configuration screen in Figure 4-6-8, Figure 4-6-9 & Figure 4-6-10 appears.

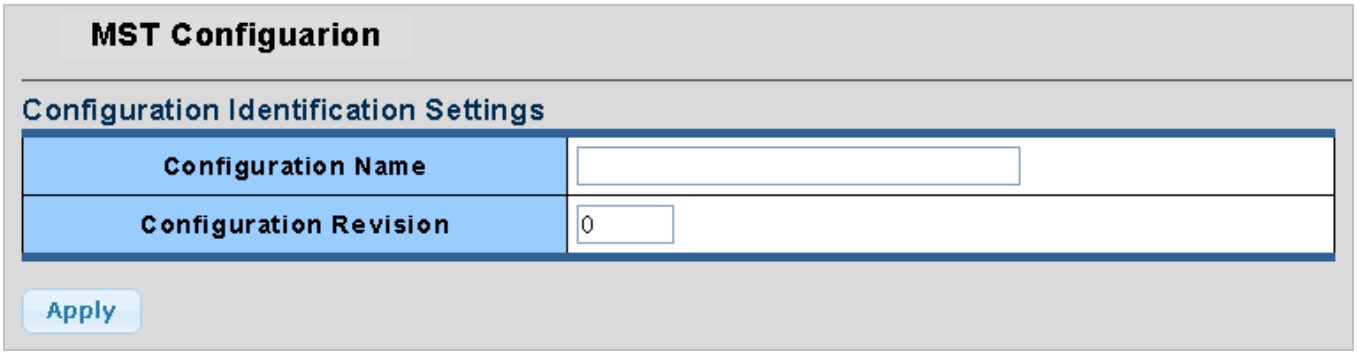


Figure 4-6-8 Configuration Identification Settings page screenshot

The page includes the following fields:

Object	Description
• **Configuration Name**	Identifier used to identify the configuration currently being used.
• **Configuration Revision**	Identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is **0**.

Buttons

Apply: Click to apply changes.

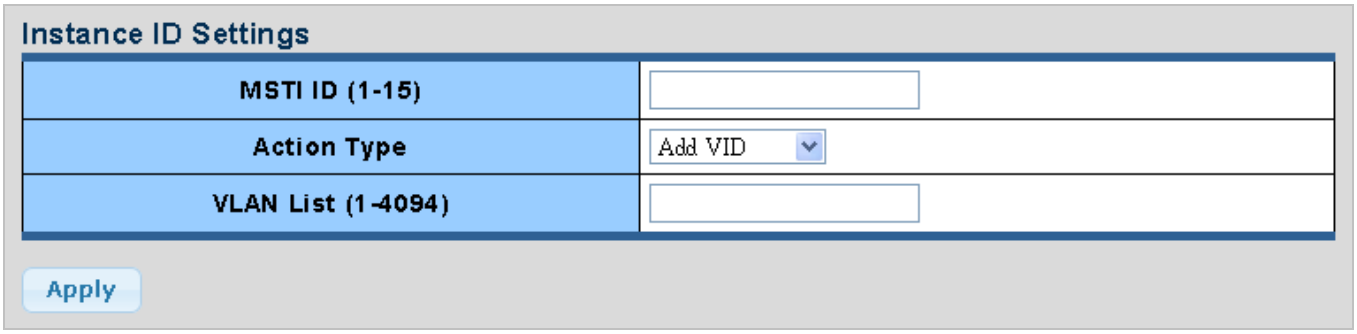


Figure 4-6-9 Instance ID Settings page screenshot

The page includes the following fields:

Object	Description
• **MSTI ID (1-15)**	Allow assign MSTI ID. The range for the MSTI ID is 1-15.
• **Action Type**	Add / remove a new VLAN group to the current list.
• **VLAN List (1-4094)**	Allow assign VLAN list for special MSTI ID. The range for the VLAN list is 1-4094.

Buttons

Apply: Click to apply changes.

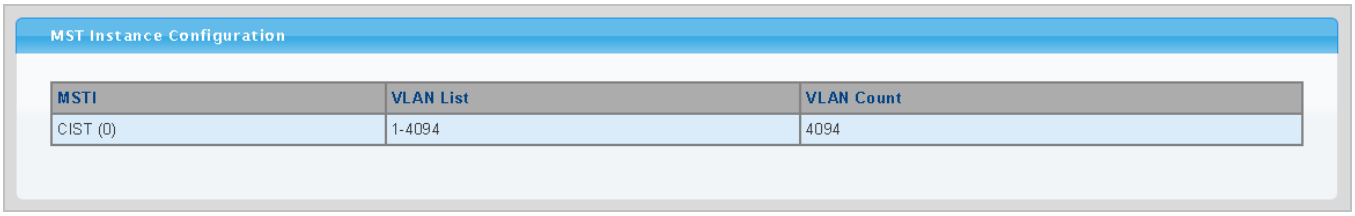


Figure 4-6-10 MASI Instance Configuration page screenshot

The page includes the following fields:

Object	Description
• **MSTI**	Display the current MSTI entry.
• **VLAN List**	Display the current VLAN list.
• **VLAN Count**	Display the current VLAN count.

4.6.5 MST Instance Setting

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MST Instance Setting screen in Figure 4-6-11, Figure 4-6-12 & Figure 4-6-13 appears.

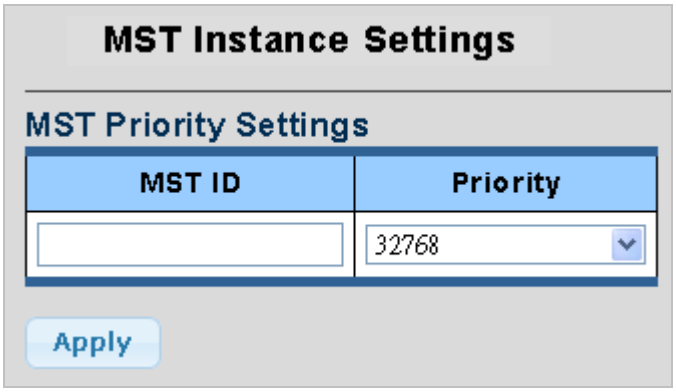


Figure 4-6-11 MST Instance Setting page screenshot

The page includes the following fields:

Object	Description
• **MST ID**	Enter the special MST ID to configure priority.
• **Priority**	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

Apply: Click to apply changes.

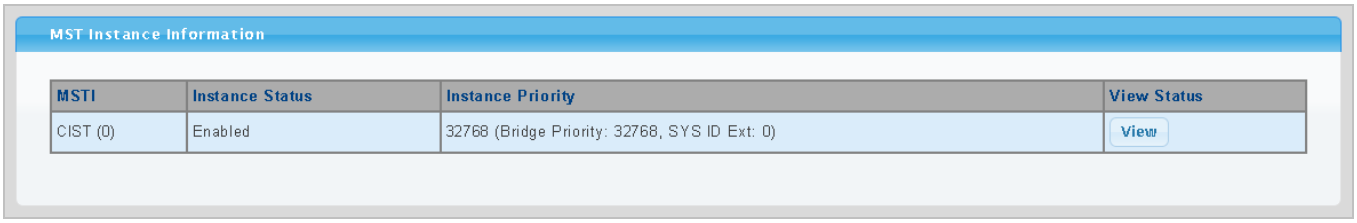


Figure 4-6-12 MST Instance Setting page screenshot

The page includes the following fields:

Object	Description
• **MSTI**	Display the current MSTI entry.
• **Instance Status**	Display the current instance status.
• **Instance Priority**	Display the current instance priority.
• **View Status**	Click to view detail information.

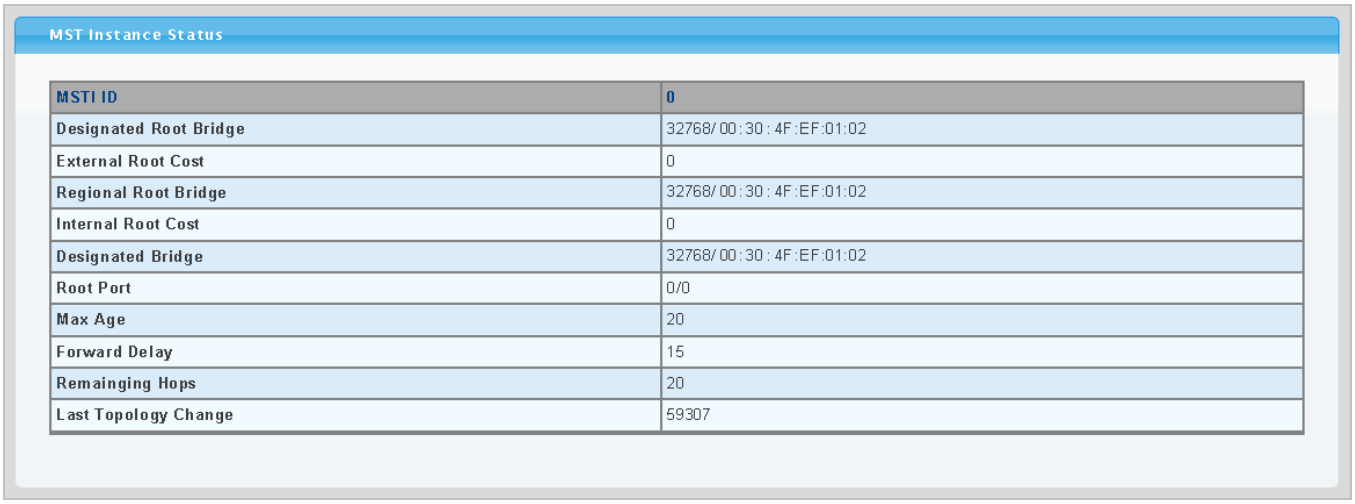


Figure 4-6-13 MST Instance Status page screenshot

The page includes the following fields:

Object	Description
• **MSTI ID**	Display the MSTI ID.
• **Designated Root Bridge**	Display the current designated root bridge.
• **External Root Cost**	Display the current external root cost.

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

4.6.6 MSTI Port Setting

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

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

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global. The MSTI Ports Setting screen in Figure 4-6-14 & Figure 4-6-15 appears.

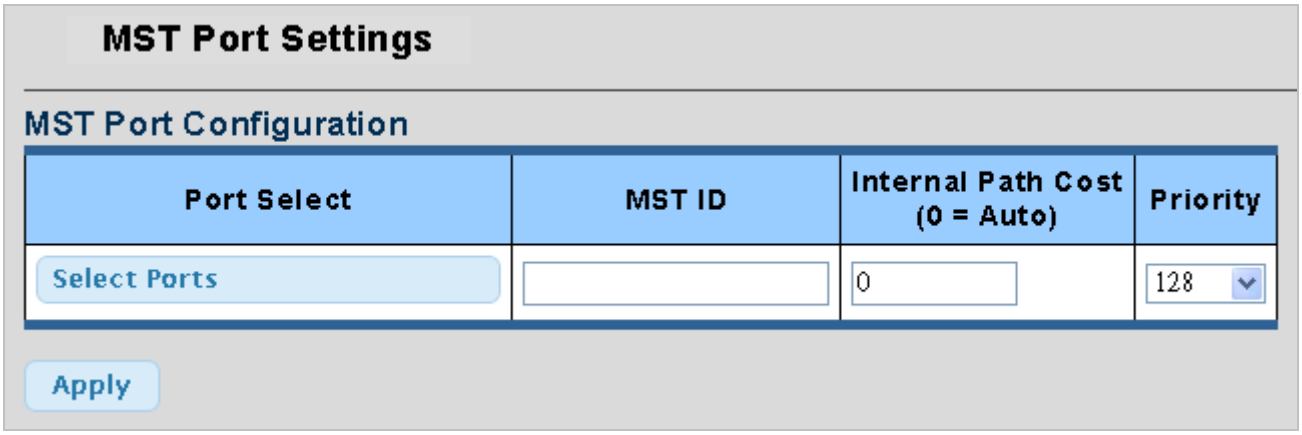


Figure 4-6-14 MST Port Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port number for this drop down list.
• **MST ID**	Enter the special MST ID to configure path cost & priority.
• **Internal Path Cost (0 = Auto)**	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path

	cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

Apply: Click to apply changes.

STP Port Status

Port	MSTI ID	Designated Bridge	Internal Path Cost Conf/Oper	Port Priority	Port Role	Port State
Port 01	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 02	0	32768/00:30: 4F:EF:01:02	0/ 20000	128	Designated	Forwarding
Port 03	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 04	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 05	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 06	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 07	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 08	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 09	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 10	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 11	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 12	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 13	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 14	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 15	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 16	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 17	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 18	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 19	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 20	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 21	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 22	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 23	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 24	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 25	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 26	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 27	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled
Port 28	0	0/00:00:00:00:00:00	0/ 0	128	Disabled	Disabled

Figure 4-6-15 MST Port Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **MSTI ID**	Display the current MSTI ID.

• **Designated Bridge**	Display the current designated bridge.
• **Internal Path Cost Conf/Oper**	Display the current internal path cost configuration / operation
• **Port Priority**	Display the current port priority.
• **Port Role**	Display the current port role.
• **Port State**	Display the current port state.

4.7 Multicast

4.7.1 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.

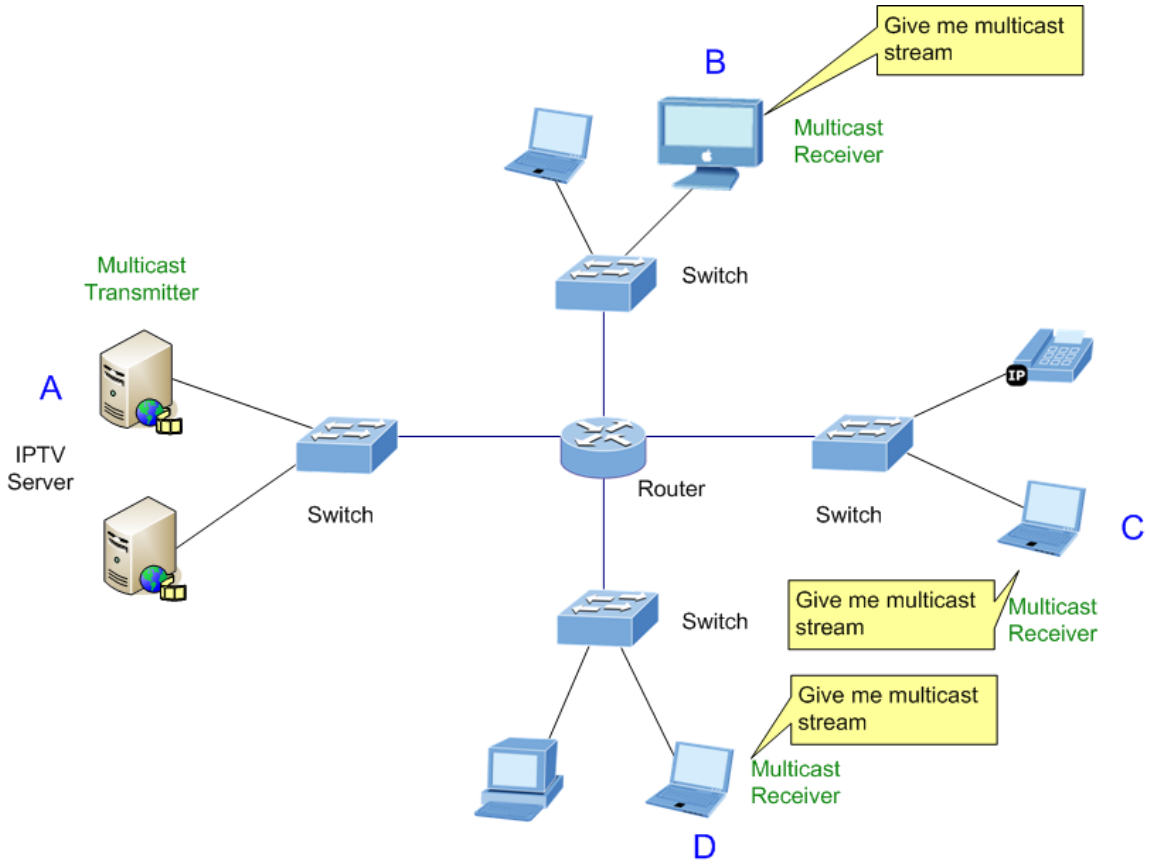


Figure 4-7-1 Multicast Service

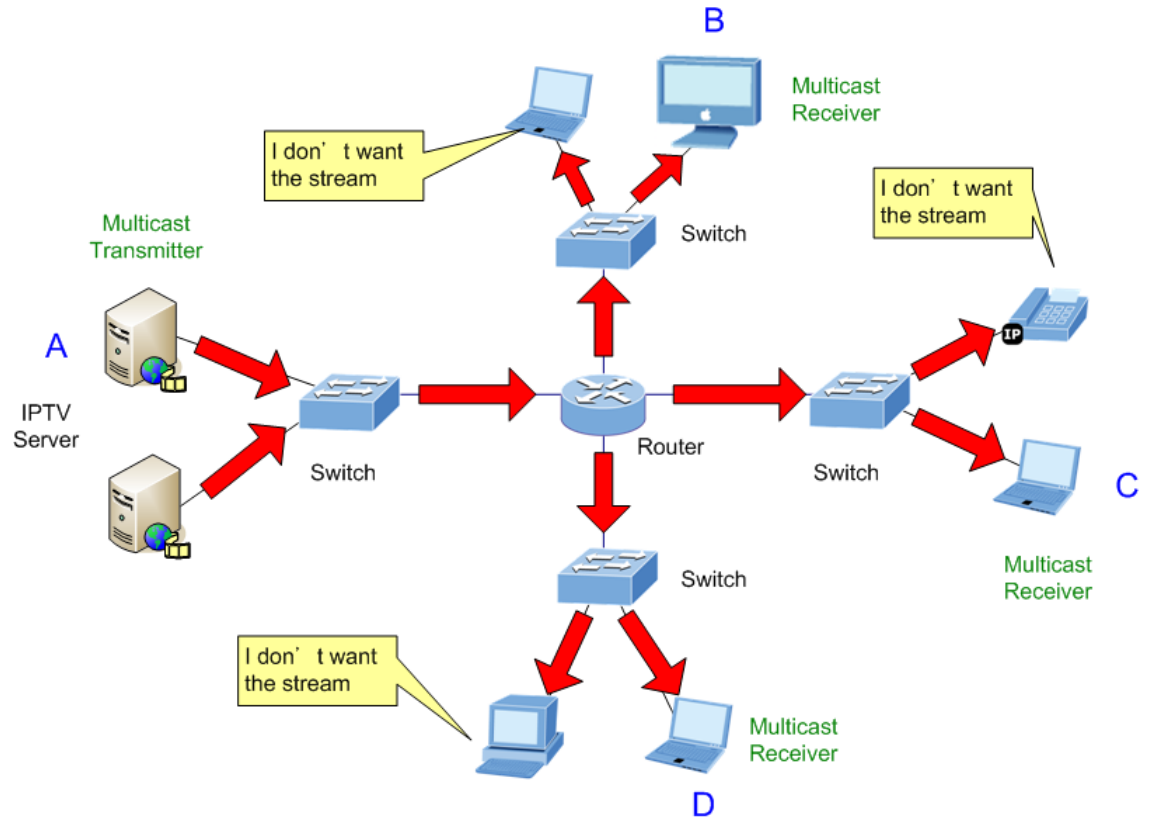


Figure 4-7-2 Multicast flooding

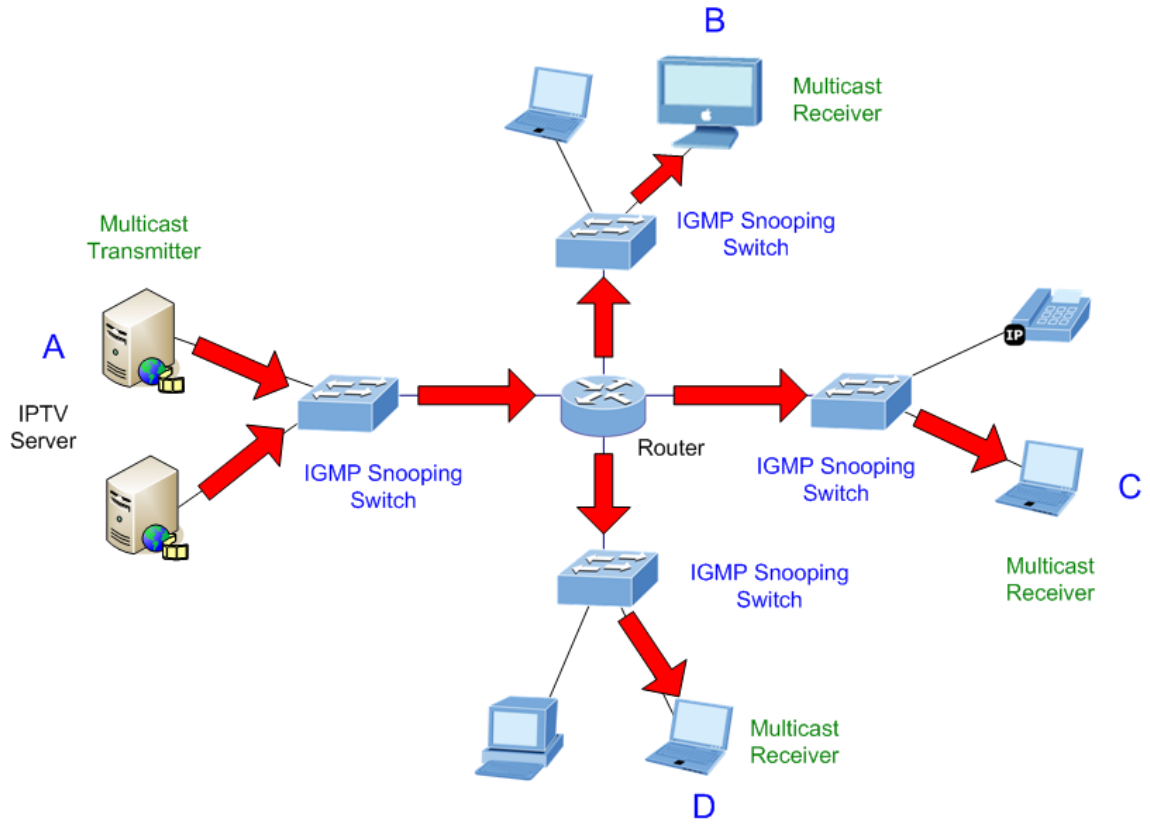


Figure 4-7-3 IGMP Snooping multicast stream control

IGMP Versions 1 and 2

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

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

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0	8	16	31
Type	Response Time	Checksum	
Group Address (all zeros if this is a query)			

The IGMP Type codes are shown below:

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

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

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

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

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

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

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

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

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

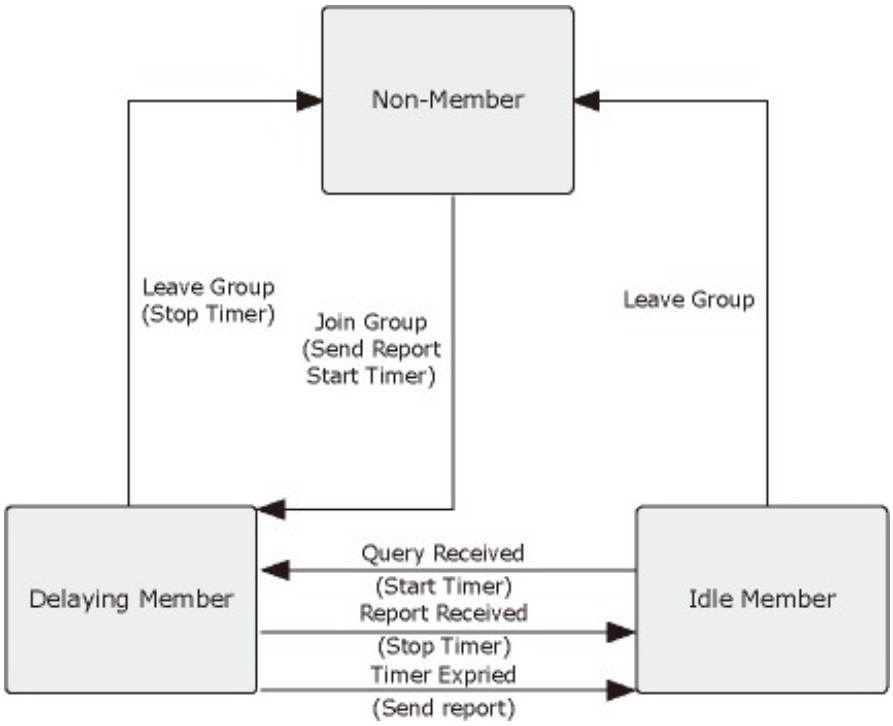


Figure 4-7-4 IGMP State Transitions

- **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.

This section has the following items:

- **IGMP Snooping Setting** Configures IGMP snooping settings
- **IGMP VLAN Setting** Configuration per VLAN LGMP snooping settings
- **Multicast Database** Display current multicast database
- **Router Table** Display current router table

4.7.2 IGMP Snooping Setting

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 Setting screen in Figure 4-7-5 & Figure 4-7-6 appears.

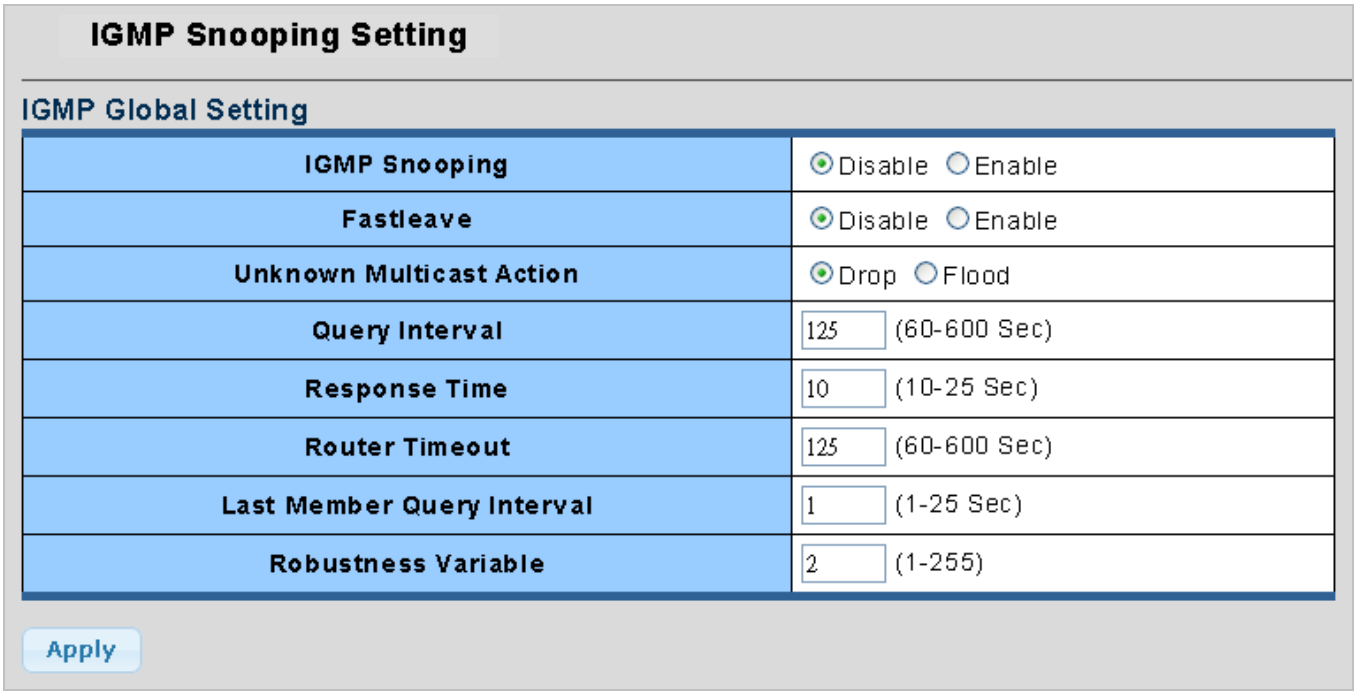


Figure 4-7-5 IGMP Global Setting page screenshot

The page includes the following fields:

Object	Description
• **IGMP Snooping**	Enable or disable the IGMP snooping. The default value is "Disabled".
• **Fastleave**	Enable or disable the fastleave. The default value is "Disabled".
• **Unknow Multicast Action**	Drop or flood unknown multicast traffic.
• **Query Interval**	Sets the frequency at which the switch sends IGMP host-query messages. Range: 60-600 seconds; Default: **125**
• **Response Time**	Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. Range: 10-25 seconds; Default: **10**
• **Router Timeout**	The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. Range: 60-600 seconds; Default: **125**
• **Last Member Query Interval**	The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages. You can also click the scroll arrows to select a new setting. Range: 1-25 seconds; Default: **1**
• **Robustness Variable**	The IGMP robustness variable provides fine-tuning to allow for expected packet loss on a subnet. The robust count automatically changes certain IGMP message intervals for IGMPv2 and IGMPv3. Increasing the robust count allows for more packet loss but increases the leave latency of the subnetwork. Range: 1-255; Default: **2**

Buttons

Apply: Click to apply changes.

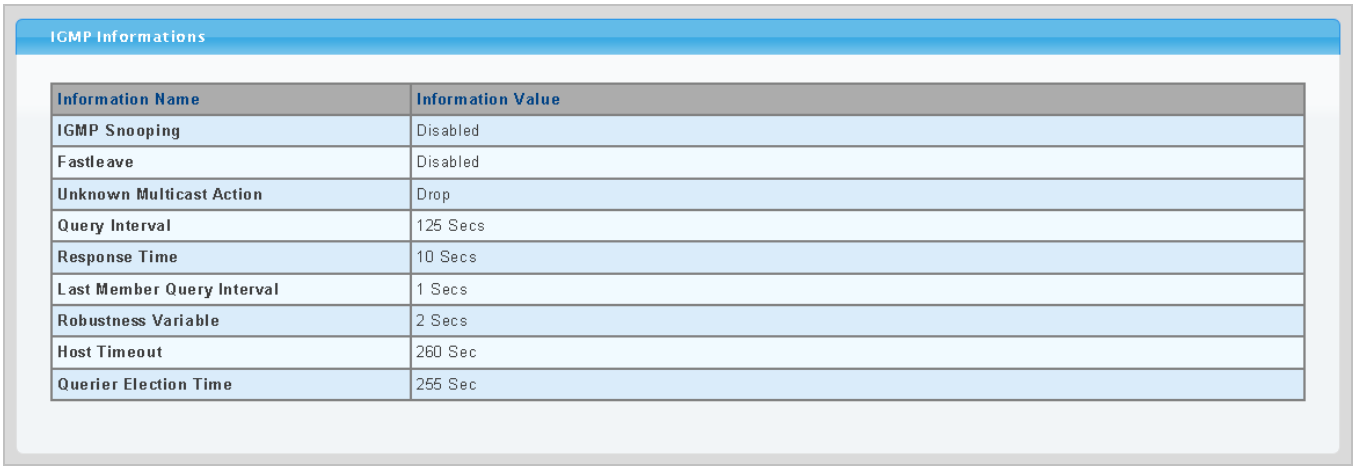


Figure 4-7-6 IGMP Inforamtion page screenshot

The page includes the following fields:

Object	Description
• **IGMP Snooping**	Display the current IGMP snooping status.
• **Fastleave**	Display the current fastleave status.
• **Unknow Multicast Action**	Display the current unknown multicast action status.
• **Query Interval**	Display the current query interval value.
• **Response Time**	Display the current response time.
• **Last Member Query Interval**	Display the current last member query interval value.
• **Robustness Variable**	Display the current robustness variable value.
• **Host Timeout**	Display the current host timeout value.
• **Querier Election Time**	Display the current querier election time.

4.7.3 IGMP VLAN Setting

This page provides IGMP VLAN Setting. The IGMP VLAN Setting screen in Figure 4-7-7 & Figure 4-7-8 appears.

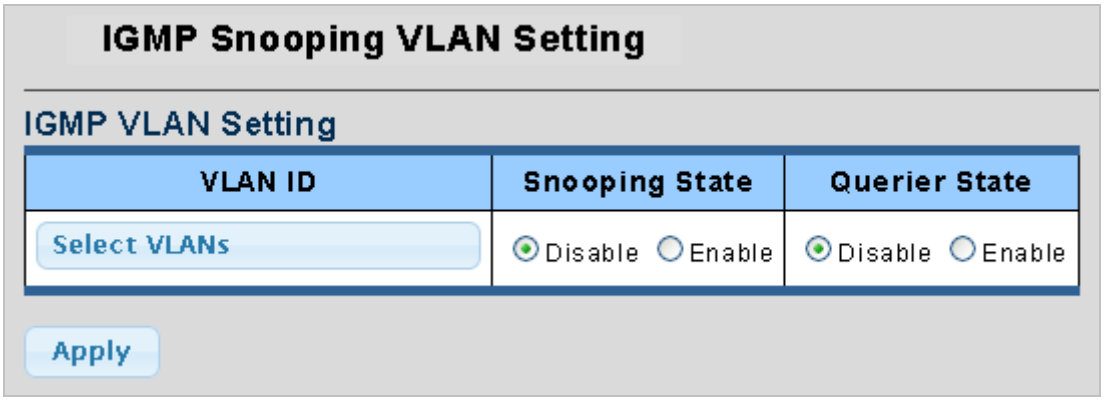


Figure 4-7-7 IGMP VLAN Setting page screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Select VLAN ID for this drop down list.
• **Snooping State**	Enable or disable the snooping state. The default value is "Disabled".
• **Querier State**	Enable or disable the querier state. The default value is "Disabled".

Buttons

Apply: Click to apply changes.

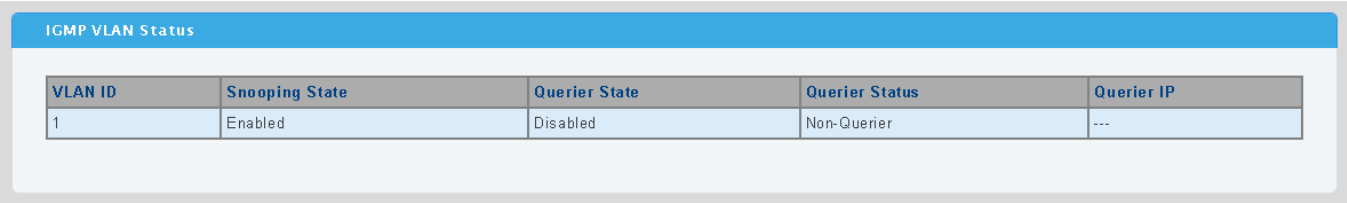


Figure 4-7-8 IGMP VLAN Status page screenshot

The page includes the following fields:

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

4.7.4 Multicast Database

This page provides Multicast Database. The Multicast Database screen in Figure 4-7-9 appears.

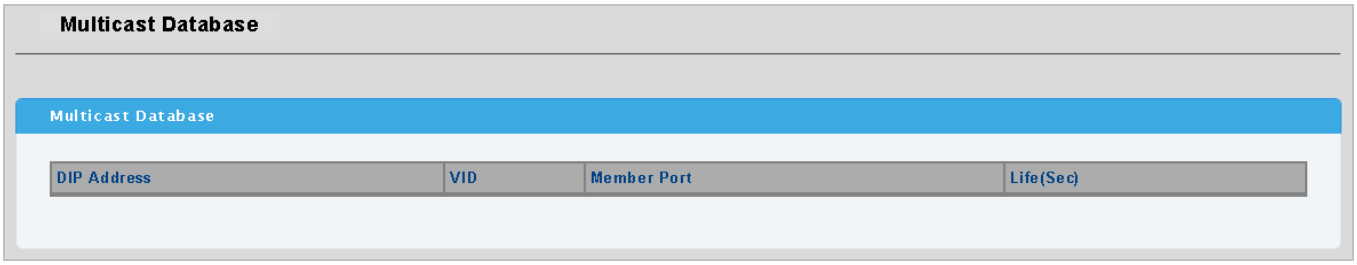


Figure 4-7-9 Multicast Database page screenshot

The page includes the following fields:

Object	Description
• **DIP Addresee**	Display the current DIP address.
• **VID**	Display the current VID.
• **Member Port**	Display the current member port.
• **Life(Sec)**	Display the current life.

4.7.5 Router Table

This page provides Router Table. The Multicast Database screen in Figure 4-7-10 appears.

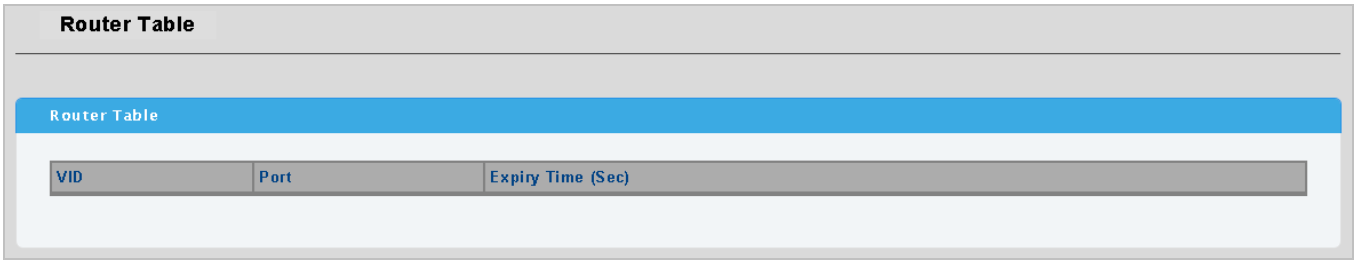


Figure 4-7-10 Router Table page screenshot

The page includes the following fields:

Object	Description
• **VID**	Display the current VID.
• **Port**	Display the current port.
• **Expiry Time (Sec)**	Display the current expiry time.

4.8 Quality of Service

4.8.1 Understand QoS

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

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

You can use QoS on your system to:

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

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

1. Define a service level to determine the priority that will be applied to traffic.
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Switch.
3. Create a QoS profile which associates a service level and a classifier.
4. Apply a QoS profile to a port(s).

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

- **802.1p Tag Priority** Mode –The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- **IP DSCP** Mode - The output queue assignment is determined by the TOS or DSCP field in the IP packets.
- **Port-Base Priority** Mode – Any packet received from the specify high priority port will treated as a high priority packet.

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

This section has the following items:

- **Port-based Priority** Configuration port-based priority

- **802.1p-based Priority** Configuration 802.1p-based priority
- **DSCP-based Priority** Configuration DSCP-based priority
- **Priority to Queue Mapping** Configuration priority to queue mapping
- **Packet Scheduling** Configuration packet scheduling
- **Queue Weught Setting** Configuration queue weight setting
- **QoS Remarking Status** Configuration QoS remarking stauts
- **QoS Remarking Table** Configuration QoS remarking table

4.8.2 Port-based Priority

This page provides Port-based Priority. The Port-based Priority screen in Figure 4-8-1 & Figure 4-8-2 appears.

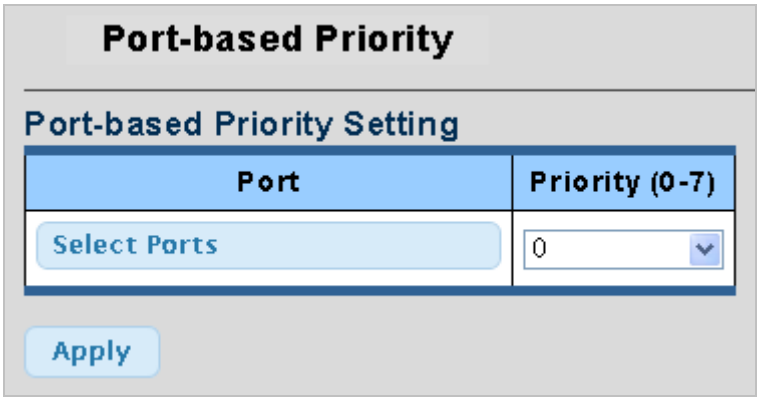


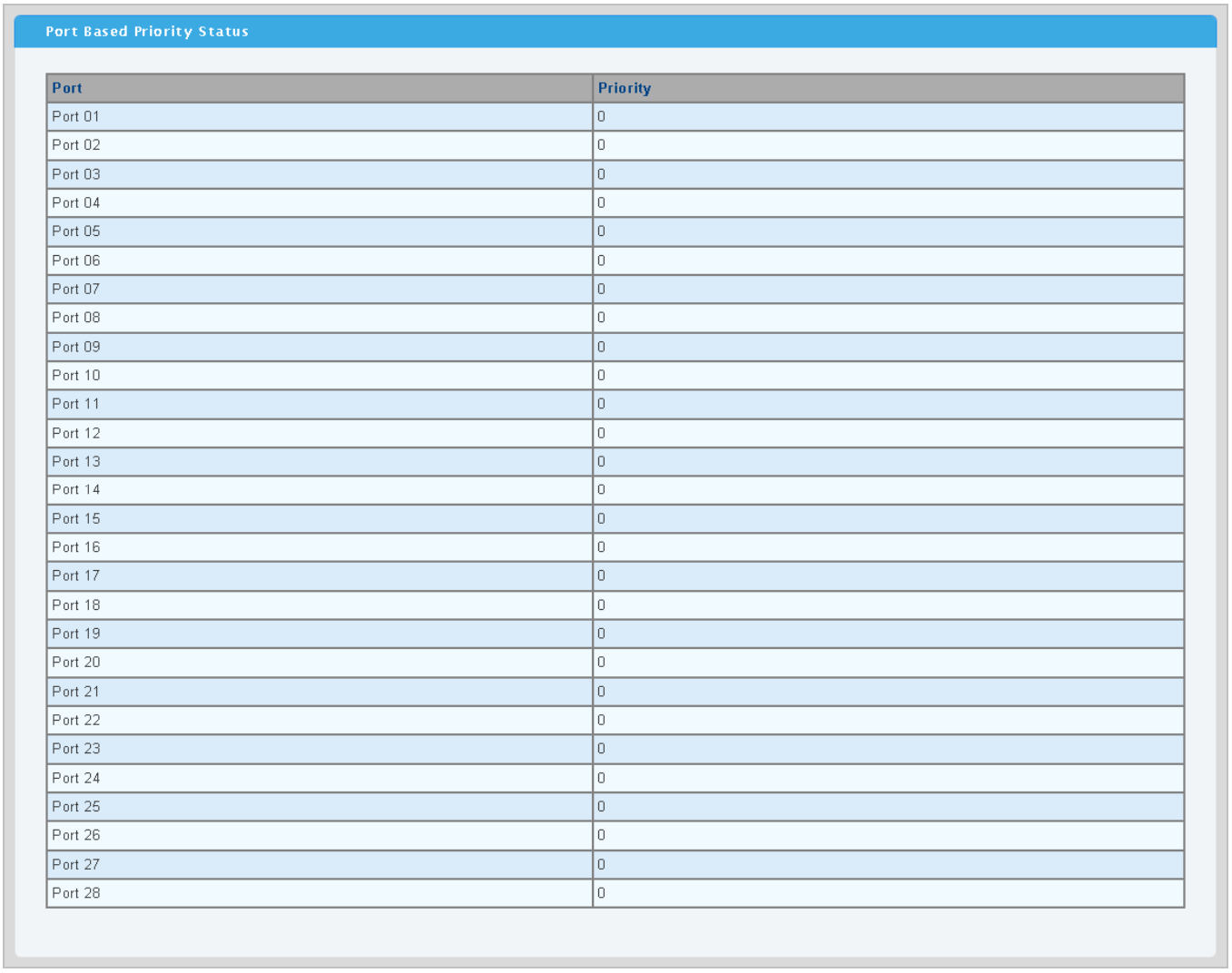
Figure 4-8-1 Port-based Priority page screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **Priority (0-7)**	Select priority for this drop down list.

Buttons

Apply: Click to apply changes.



Port Based Priority Status

Port	Priority
Port 01	0
Port 02	0
Port 03	0
Port 04	0
Port 05	0
Port 06	0
Port 07	0
Port 08	0
Port 09	0
Port 10	0
Port 11	0
Port 12	0
Port 13	0
Port 14	0
Port 15	0
Port 16	0
Port 17	0
Port 18	0
Port 19	0
Port 20	0
Port 21	0
Port 22	0
Port 23	0
Port 24	0
Port 25	0
Port 26	0
Port 27	0
Port 28	0

Figure 4-8-2 Port-based Priority Status page screenshot

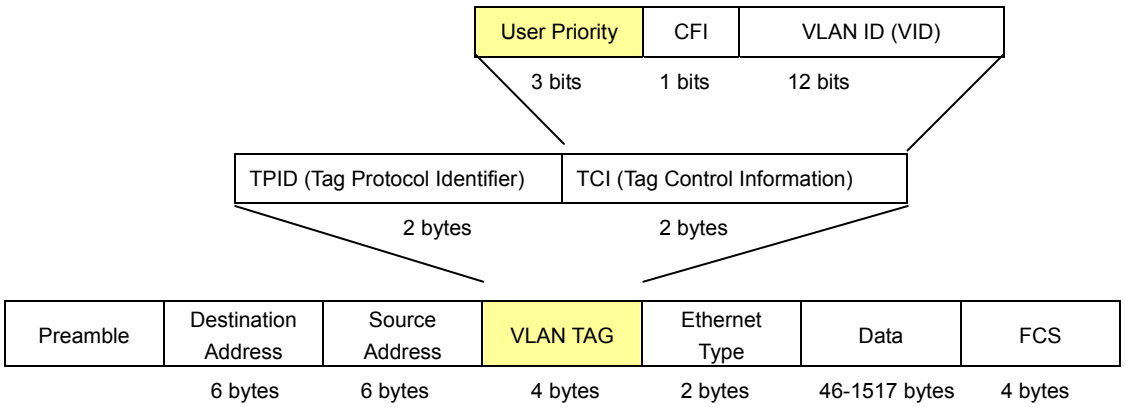
The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Priority (0-7)**	Display the current priority.

4.8.3 802.1p-based Priority

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

■ **802.1Q Tag and 802.1p priority**



This page provides 802.1p-based Priority. The 802.1p-based Priority screen in Figure 4-8-3 & Figure 4-8-4 appears.

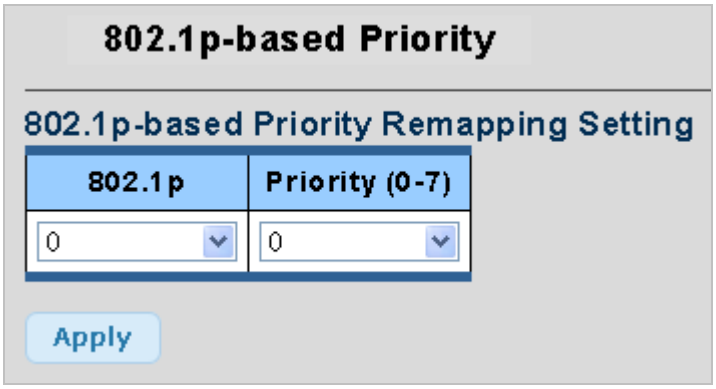


Figure 4-8-3 802.1p-based Priority Remapping Setting page screenshot

The page includes the following fields:

Object	Description
• **802.1p**	Select CoS value for this drop down list. (Range: 0-7, where **7** is the highest priority)
• **Priority (0-7)**	Select priority for this drop down list.

Buttons

Apply: Click to apply changes.

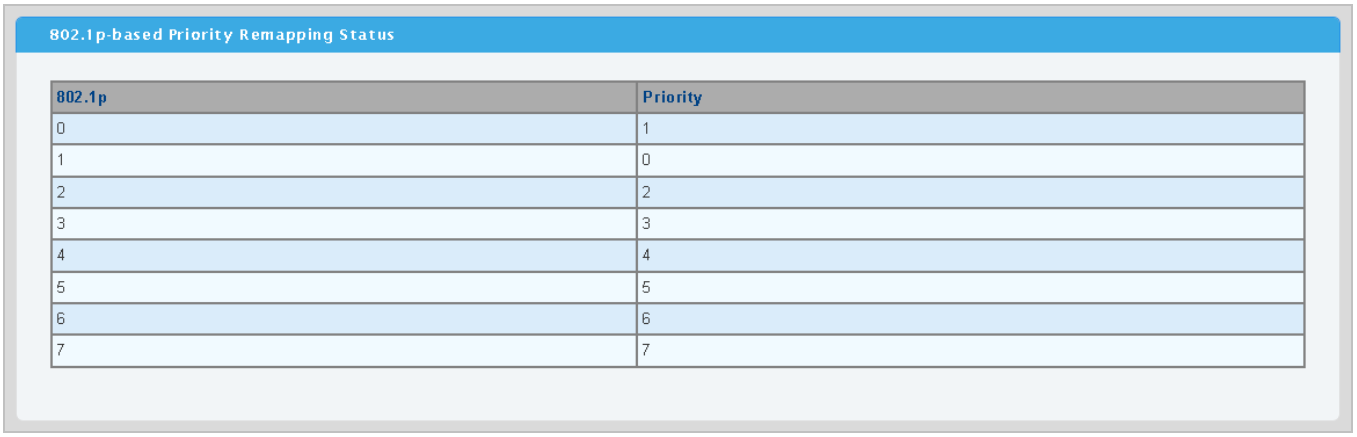


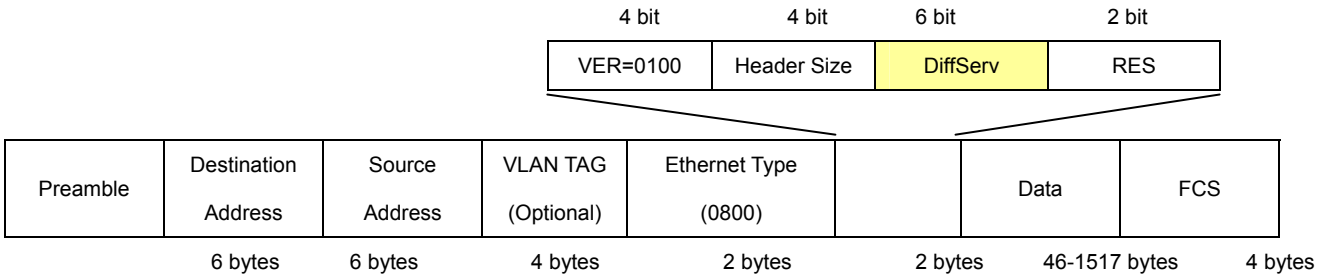
Figure 4-8-4 802.1p-based Priority Remapping Status page screenshot

The page includes the following fields:

Object	Description
• **802.1p**	Display the current 802.1p.
• **Priority (0-7)**	Display the current priority.

4.8.4 DSCP-based Priority

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



The **DSCP-based Priority** page provides fields for defining output queue to specific DSCP fields. When TCP/IP's TOS/DSCP mode is applied, the PoE Switch recognizes TCP/IP Differentiated Service Codepoint (DSCP) priority information from the DS-field defined in RFC2474.

This page provides DSCP-based Priority. The DSCP-based Priority screen in Figure 4-8-5 & Figure 4-8-6 appears.

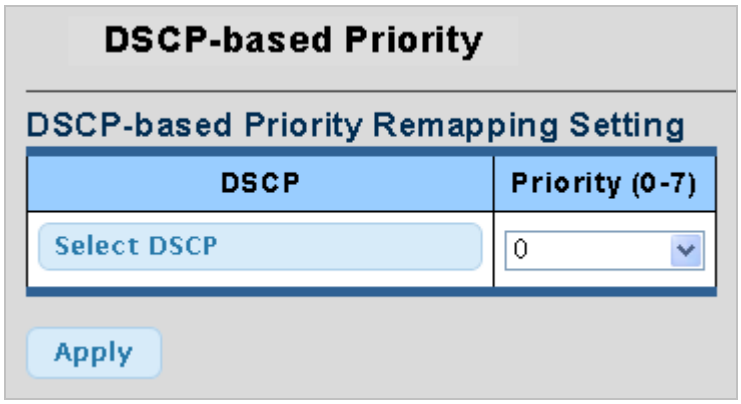


Figure 4-8-5 DSCP-based Priority Remapping Setting page screenshot

The page includes the following fields:

Object	Description
• **DSCP**	Select DSCP value for this drop down list.
• **Priority (0-7)**	Select priority for this drop down list.

Buttons

Apply: Click to apply changes.

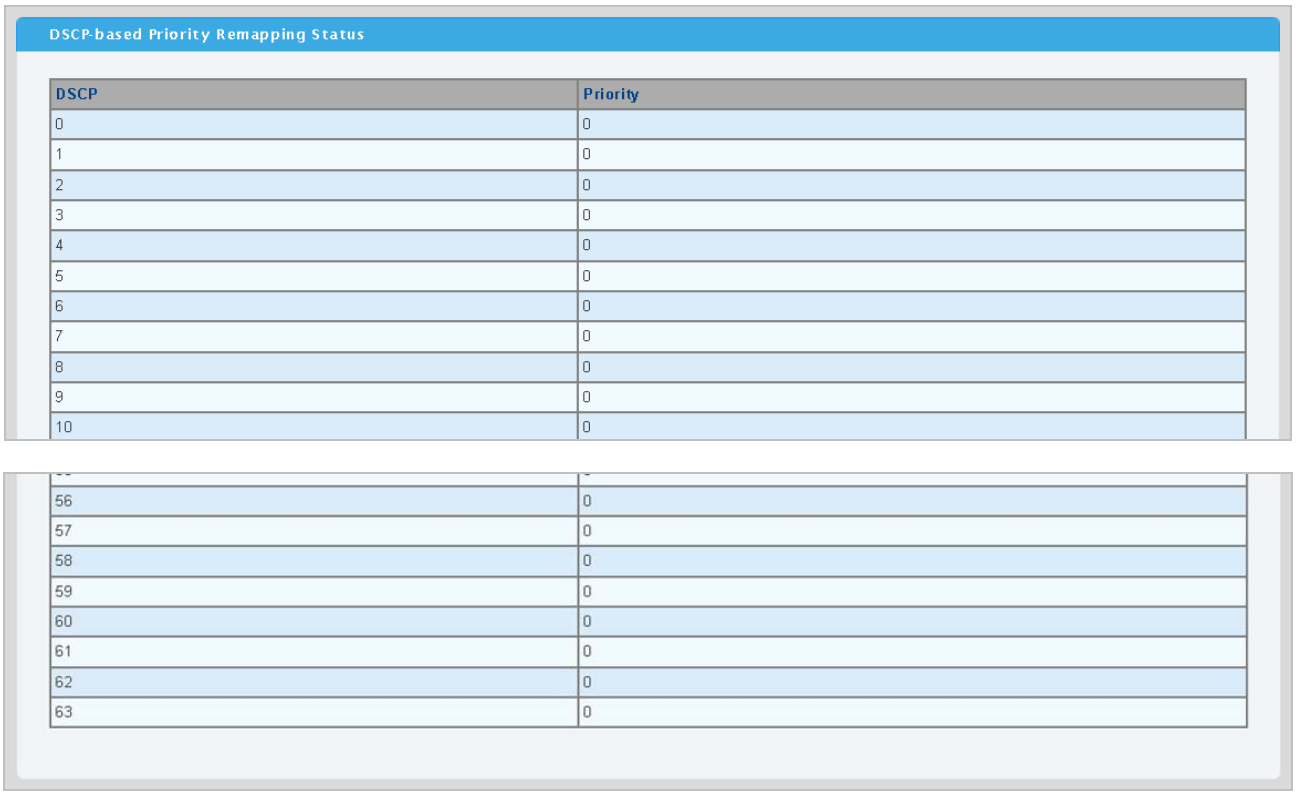


Figure 4-8-6 DSCP-based Priority Remapping Status page screenshot

The page includes the following fields:

Object	Description
• **DSCP**	Display the current DSCP.
• **Priority (0-7)**	Display the current priority.

4.8.5 Priority to Queue Mapping

This page provides Priority to Queue Mapping. The Priority to Queue Mapping screen in Figure 4-8-7 & Figure 4-8-8 appears.

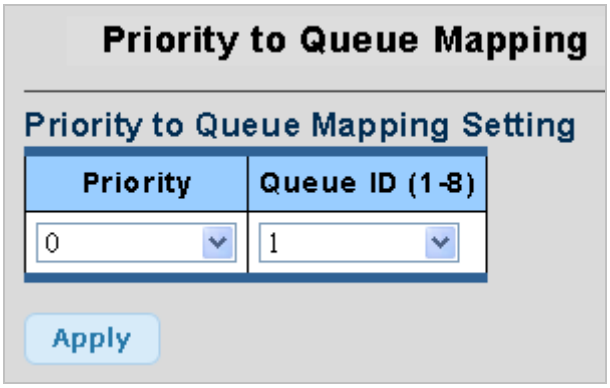


Figure 4-8-7 Priority to Queue Mapping Setting page screenshot

The page includes the following fields:

Object	Description
• **Priority**	Select priority for this drop down list.
• **Queue ID (1-8)**	Select queue ID for this drop down list.

Buttons

Apply: Click to apply changes.

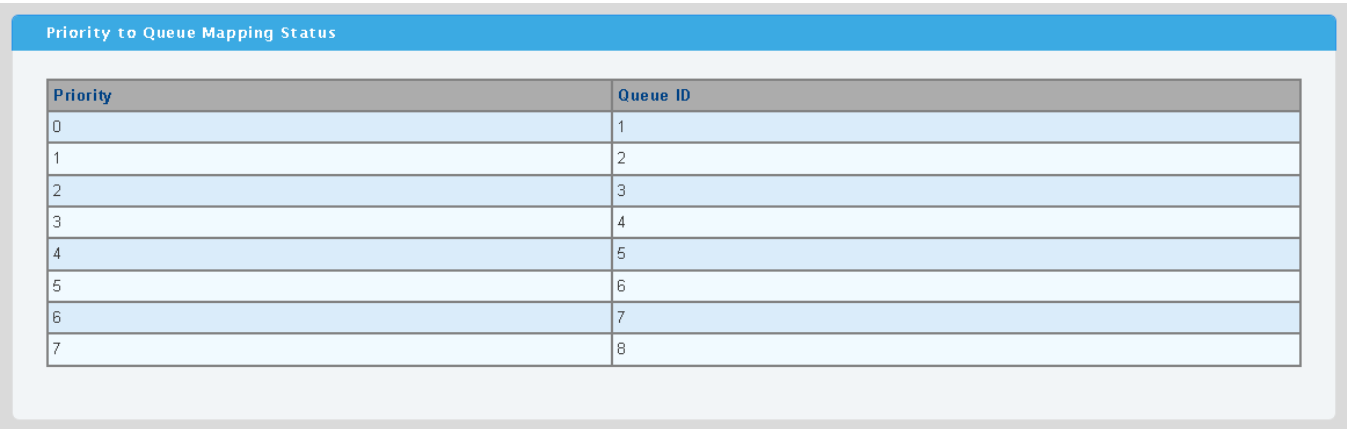


Figure 4-8-8 Priority to Queue Mapping Status page screenshot

The page includes the following fields:

Object	Description
• **Priority**	Display the current priority.
• **Queue ID (1-8)**	Display the current queue ID.

4.8.6 Packet Scheduling

This page provides Packet Scheduling. The Packet Scheduling screen in Figure 4-8-9 & Figure 4-8-10 appears.

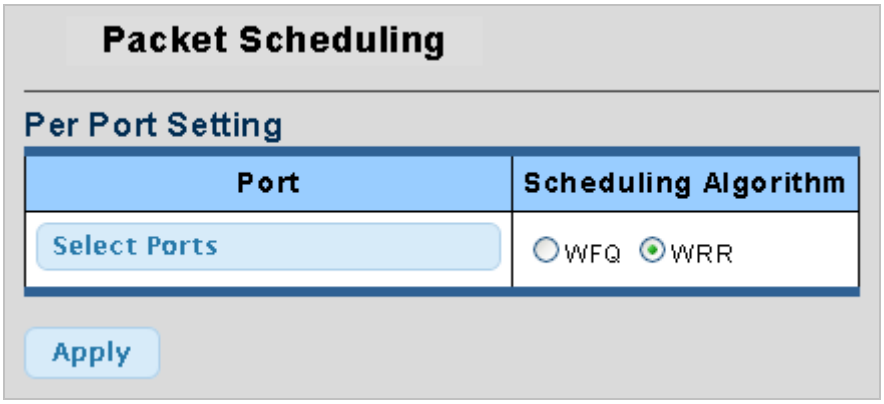


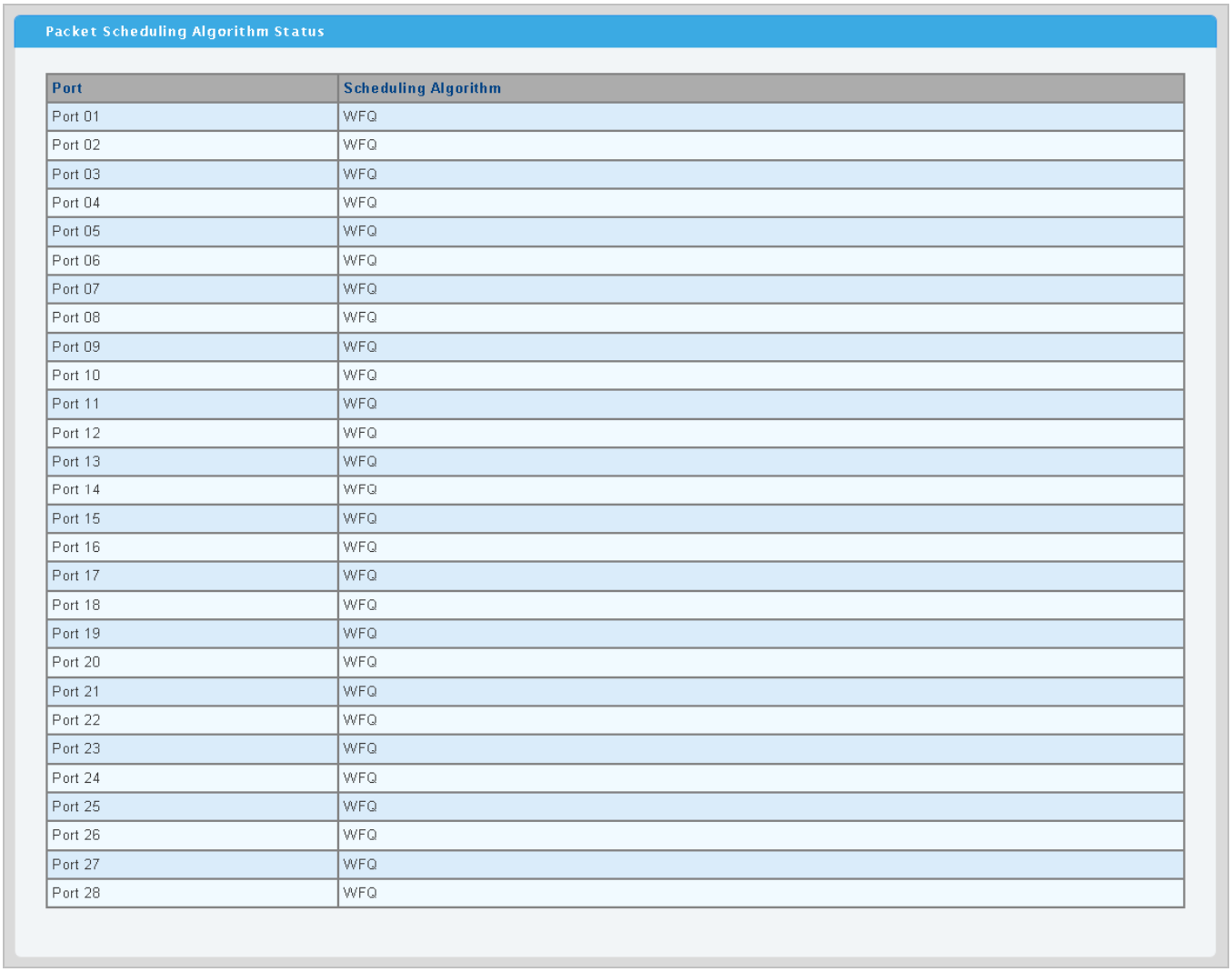
Figure 4-8-9 Per Port Setting page screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **Schedule Algorithm**	Select schedule algorithm mode.

Buttons

Apply: Click to apply changes.



Packet Scheduling Algorithm Status

Port	Scheduling Algorithm
Port 01	WFQ
Port 02	WFQ
Port 03	WFQ
Port 04	WFQ
Port 05	WFQ
Port 06	WFQ
Port 07	WFQ
Port 08	WFQ
Port 09	WFQ
Port 10	WFQ
Port 11	WFQ
Port 12	WFQ
Port 13	WFQ
Port 14	WFQ
Port 15	WFQ
Port 16	WFQ
Port 17	WFQ
Port 18	WFQ
Port 19	WFQ
Port 20	WFQ
Port 21	WFQ
Port 22	WFQ
Port 23	WFQ
Port 24	WFQ
Port 25	WFQ
Port 26	WFQ
Port 27	WFQ
Port 28	WFQ

Figure 4-8-10 Per Port Setting page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Schedule Algorithm**	Display the current schedule algorithm.

4.8.7 Queue Weight Setting

This page provides Queue Weight Setting. The Queue Weight Setting screen in Figure 4-8-11 & Figure 4-8-12 appears.

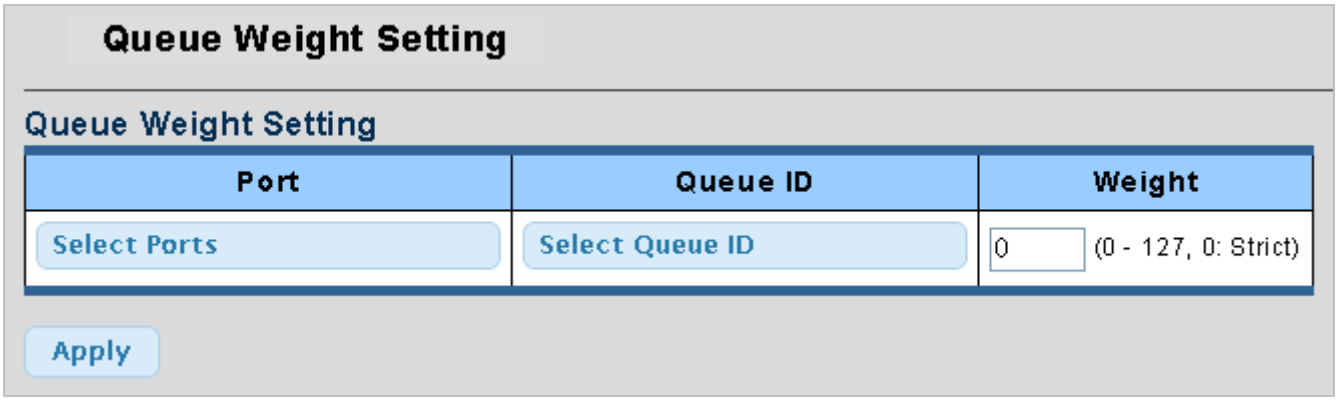


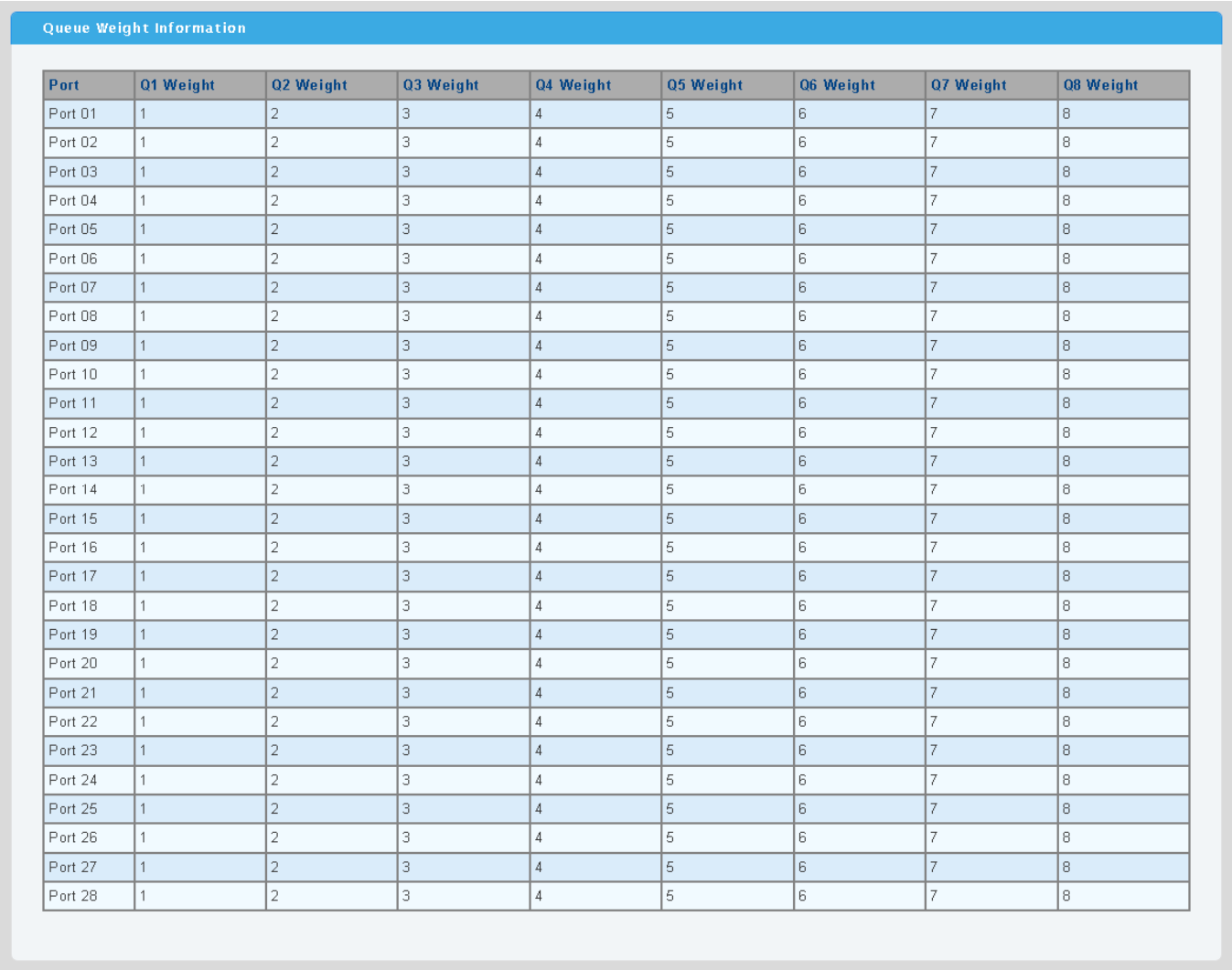
Figure 4-8-11 Queue Weight Setting page screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **Queue ID**	Select queue ID for this drop down list.
• **Weight**	Sets the queue weight. Range: 0-127; Default: **0**

Buttons

Apply: Click to apply changes.



Queue Weight Information

Port	Q1 Weight	Q2 Weight	Q3 Weight	Q4 Weight	Q5 Weight	Q6 Weight	Q7 Weight	Q8 Weight
Port 01	1	2	3	4	5	6	7	8
Port 02	1	2	3	4	5	6	7	8
Port 03	1	2	3	4	5	6	7	8
Port 04	1	2	3	4	5	6	7	8
Port 05	1	2	3	4	5	6	7	8
Port 06	1	2	3	4	5	6	7	8
Port 07	1	2	3	4	5	6	7	8
Port 08	1	2	3	4	5	6	7	8
Port 09	1	2	3	4	5	6	7	8
Port 10	1	2	3	4	5	6	7	8
Port 11	1	2	3	4	5	6	7	8
Port 12	1	2	3	4	5	6	7	8
Port 13	1	2	3	4	5	6	7	8
Port 14	1	2	3	4	5	6	7	8
Port 15	1	2	3	4	5	6	7	8
Port 16	1	2	3	4	5	6	7	8
Port 17	1	2	3	4	5	6	7	8
Port 18	1	2	3	4	5	6	7	8
Port 19	1	2	3	4	5	6	7	8
Port 20	1	2	3	4	5	6	7	8
Port 21	1	2	3	4	5	6	7	8
Port 22	1	2	3	4	5	6	7	8
Port 23	1	2	3	4	5	6	7	8
Port 24	1	2	3	4	5	6	7	8
Port 25	1	2	3	4	5	6	7	8
Port 26	1	2	3	4	5	6	7	8
Port 27	1	2	3	4	5	6	7	8
Port 28	1	2	3	4	5	6	7	8

Figure 4-8-12 Queue Weight Information page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Q1~Q8 Weight**	Display the current queue weught.

4.8.8 Queue Remarking Status

This page provides Queue Remarking Status. The Queue Remarking Status screen in Figure 4-8-13 & Figure 4-8-14 appears.

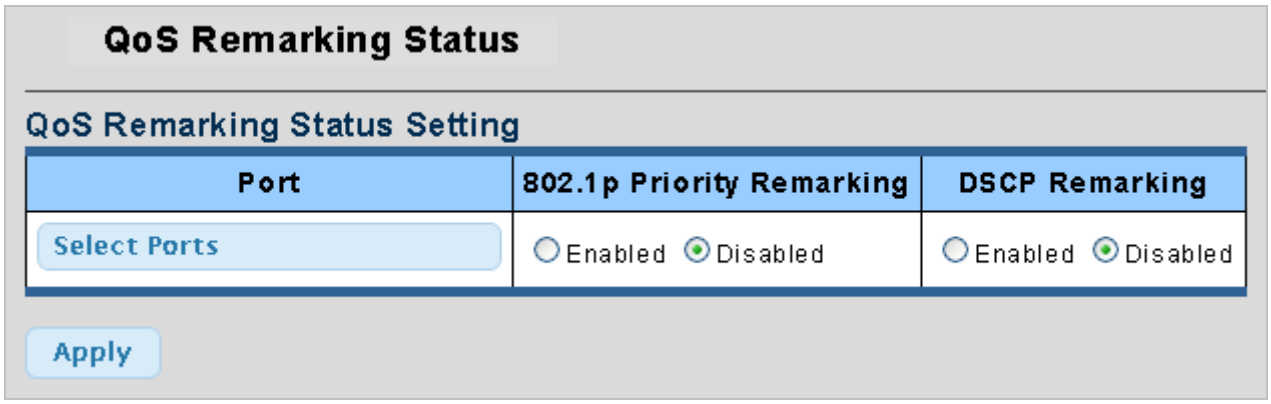


Figure 4-8-13 Queue Remarking Status Setting page screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **802.1p Priority Remarking**	Enable or disable the 802.1p priority remarking. The default value is "Disabled".
• **DSCP Remarking**	Enable or disable the DSCP remarking. The default value is "Disabled".

Buttons

Apply: Click to apply changes.

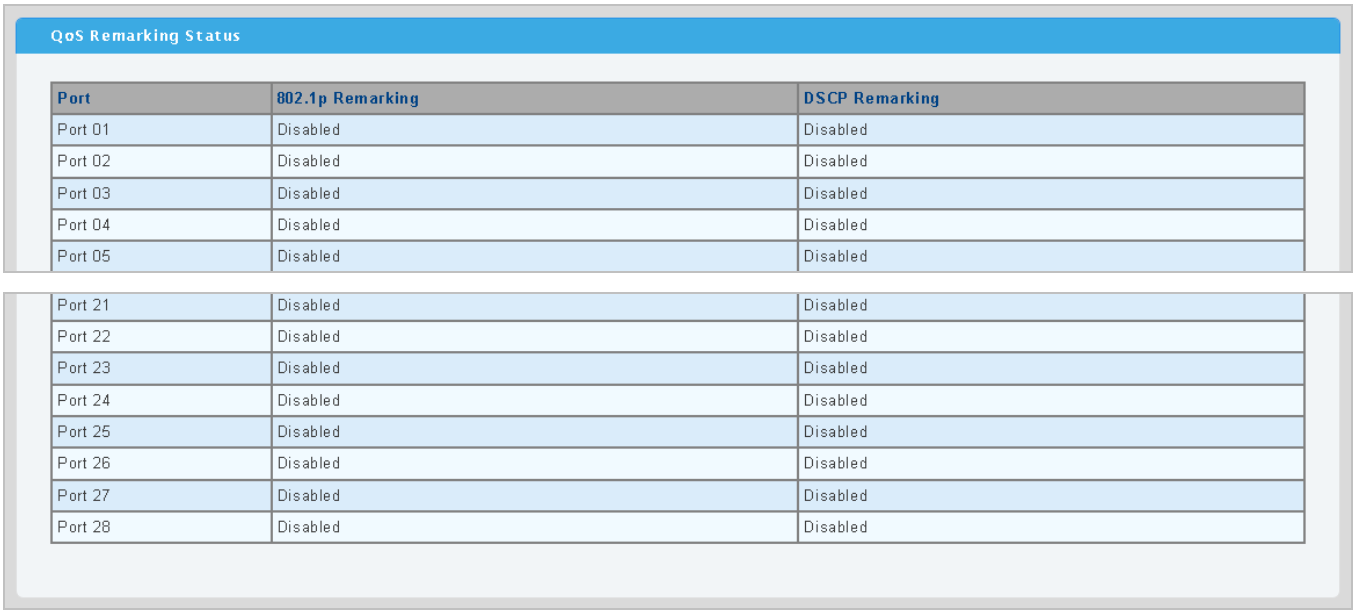


Figure 4-8-14 Queue Remarking Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **802.1p Priority Remarking**	Display the current 802.1p priority remarking.
• **DSCP Remarking**	Display the current DSCP remarking.

4.8.9 Queue Remarking Table

This page provides Queue Remarking Table. The Queue Remarking Status screen in Figure 4-8-15 & Figure 4-8-16 appears.

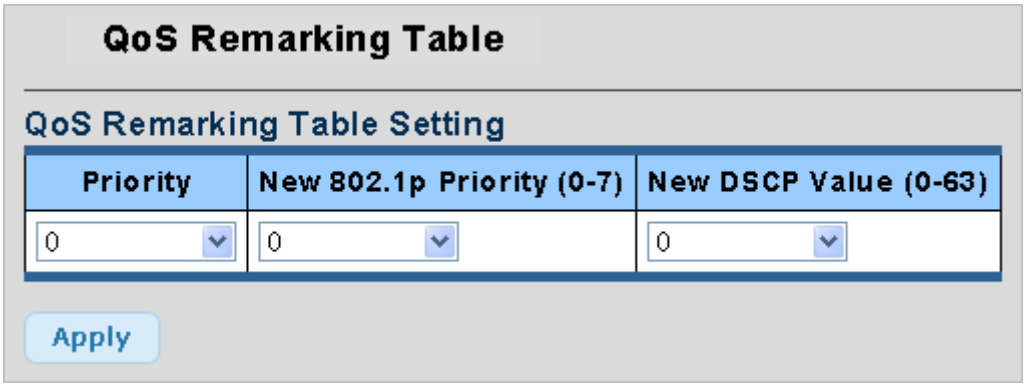


Figure 4-8-15 Queue Remarking Table Setting page screenshot

The page includes the following fields:

Object	Description
• **Priority**	Select port for this drop down list.
• **New 802.1p Priority (0-7)**	Select new 802.1p priority for this drop down list.
• **New DSCP Value (0-63)**	Select new DSCP value for this drop down list.

Buttons

Apply: Click to apply changes.

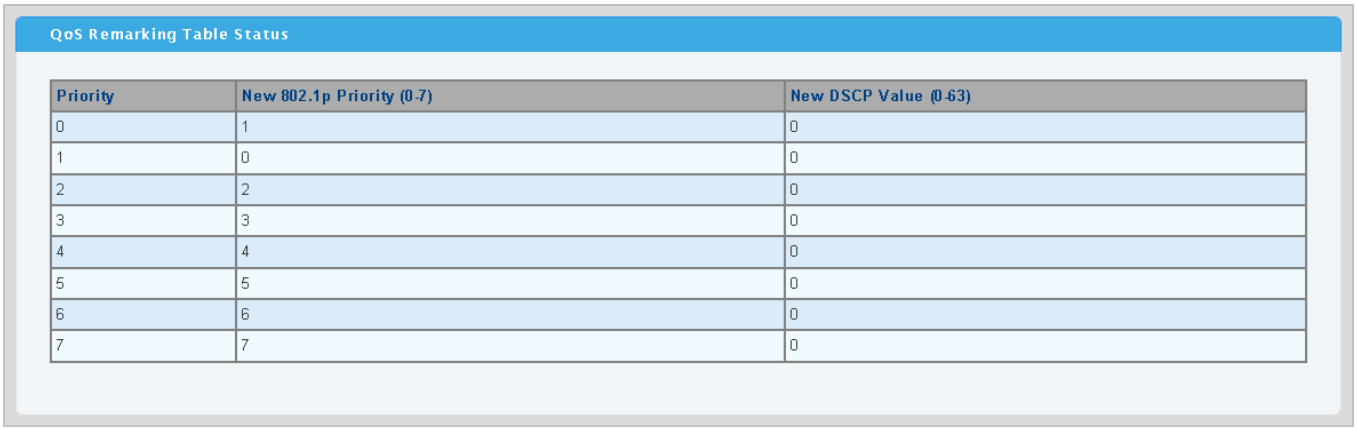


Figure 4-8-16 Queue Remarking Table Status page screenshot

The page includes the following fields:

Object	Description
• **Priority**	Display the current priority.
• **New 802.1p Priority (0-7)**	Display the current new 802.1p priority.
• **New DSCP Value (0-63)**	Display the current new DSCP value.

4.9 Security

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

The Security page contains links to the following main topics:

- **Storm Control** Configuration storm control
- **MAC Filtering** Configuration MAC filtering
- **Port Security** Configuration port security
- **802.1X Access Control** Configuration 802.1X access control

4.9.1 Storm Control

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

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

The unit of the rate can be either pps (packets per second). The configuration indicates the permitted packet rate for unknown unicast, multicast, unknown multicast, or broadcast traffic across the switch. The Storm Control Configuration screen in Figure 4-9-1 & Figure 4-9-2 appears.

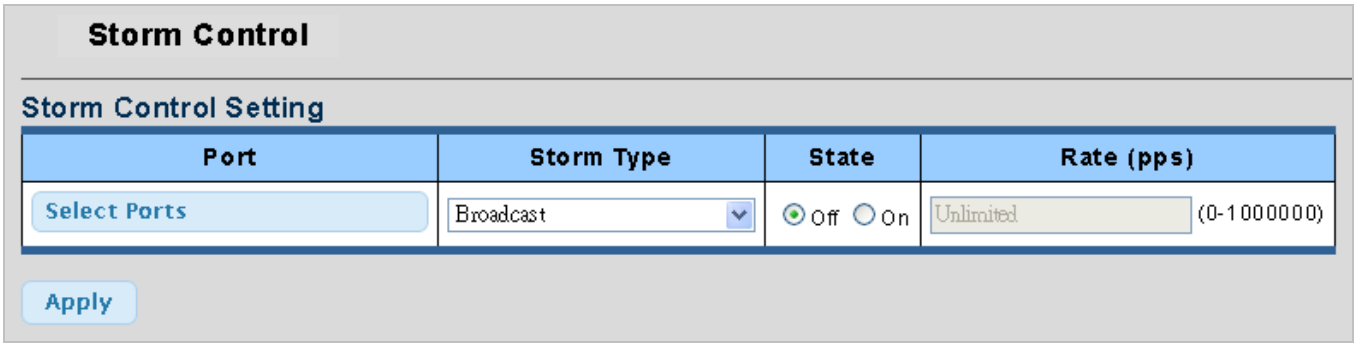


Figure 4-9-1 Storm Control Setting page screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **Storm Type**	The settings in a particular row apply to the frame type listed here: **broadcast** **multicast** **known unicast** **known multicast**
• **State**	Enable or disable the storm control status for the given storm type.

• **Rate (pps)**	The rate unit is packet per second (pps), the 1 kpps is actually 1002.1 pps.

Buttons

Apply: Click to apply changes.

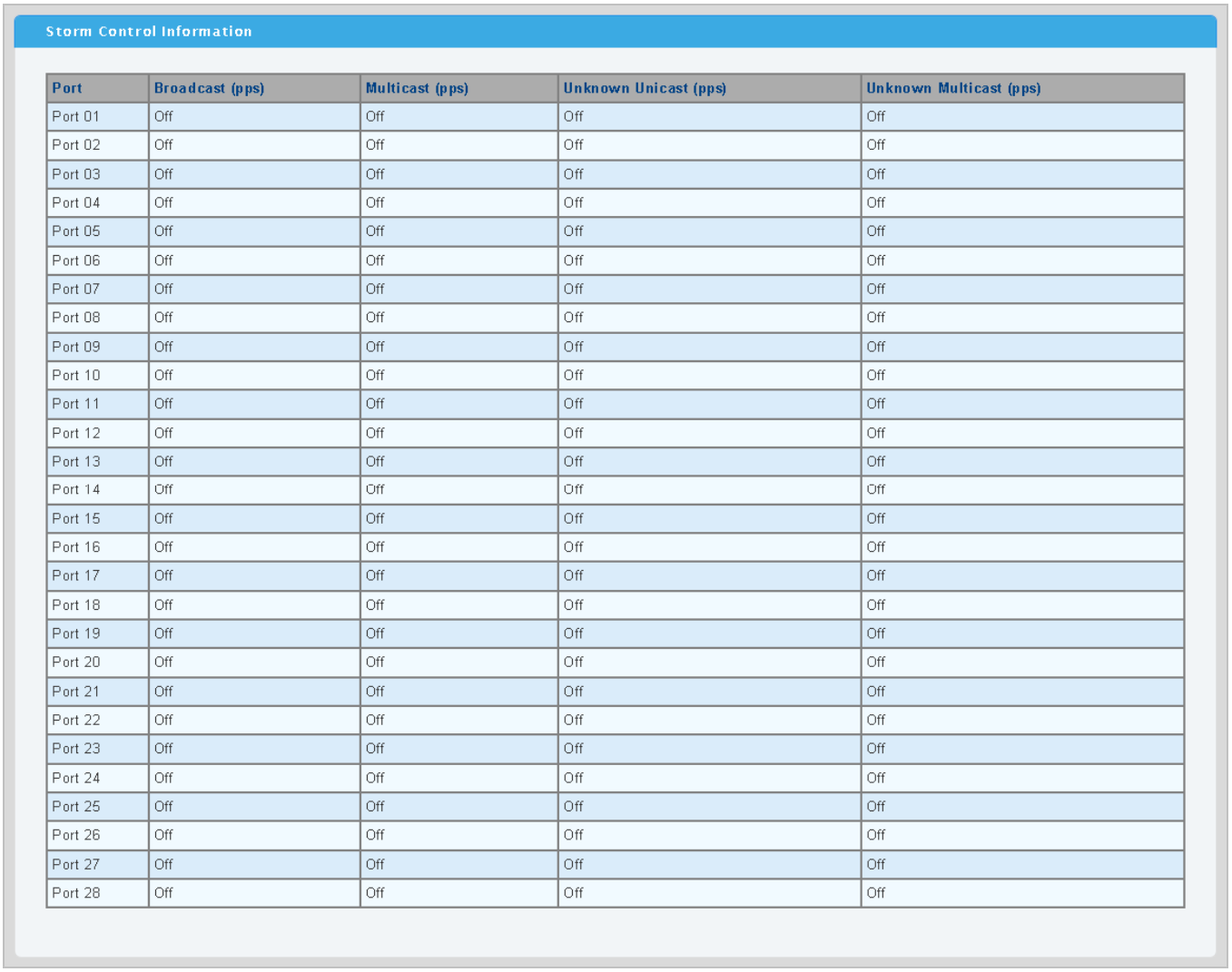


Figure 4-9-2 Storm Control Information page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Broadcast (pps)**	Display the current broadcast rate.
• **Multicast (pps)**	Display the current multicast rate.
• **Unknown Unicast (pps)**	Display the current unknown unicast rate.
• **Unknown Multicast (pps)**	Display the current unknown multicast rate.

4.9.2 MAC Filtering

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 4-9-3 & Figure 4-9-4 appears.

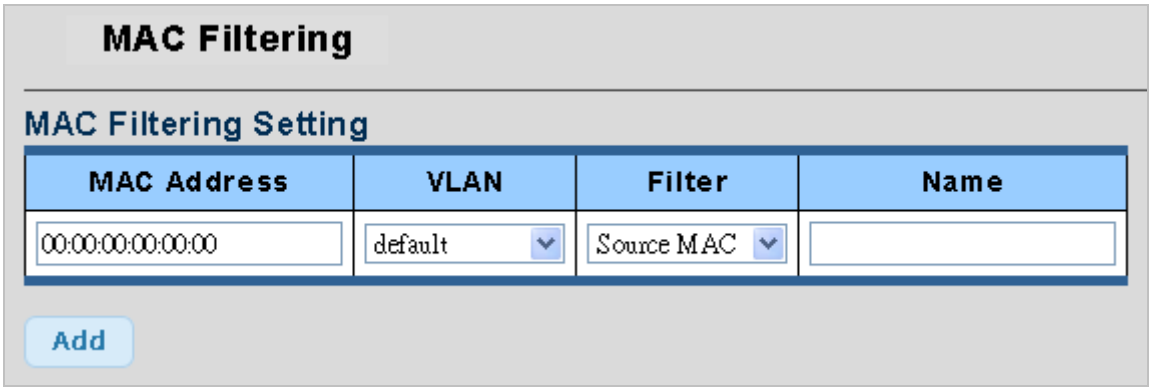


Figure 4-9-3 MAC Filtering Setting page screenshot

The page includes the following fields:

Object	Description
• **MAC Address**	Physical address of a device mapped to this interface.
• **VLAN**	ID of configured VLAN (1-4094).
• **Filter**	Select MAC filter type for this drop down list.
• **Name**	Indicates the filter name.

Buttons

Add: Click to add new MAC filter entry.

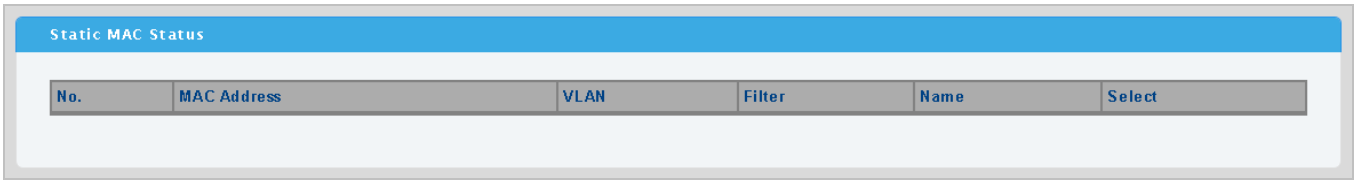


Figure 4-9-4 Statics MAC Status page screenshot

The page includes the following fields:

Object	Description
• **No.**	This is the number for entries
• **MAC Address**	Display the current MAC address.
• **VLAN**	Display the current VLAN.
• **Filter**	Display the current filter type.
• **Name**	Display the current name.
• **Select**	Click to delete the filter entry.

4.9.3 Port Security

This page allows you to configure the Port Security Limit Control system and port settings.

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of four different as described below.

The Limit Control module is one of a range of modules that utilizes a lower-layer module, the Port Security module, which manages MAC addresses learned on the port.

The Limit Control configuration consists of two sections, a system- and a port-wide. The Port Security screen in Figure 4-9-5 & Figure 4-9-6 appears.

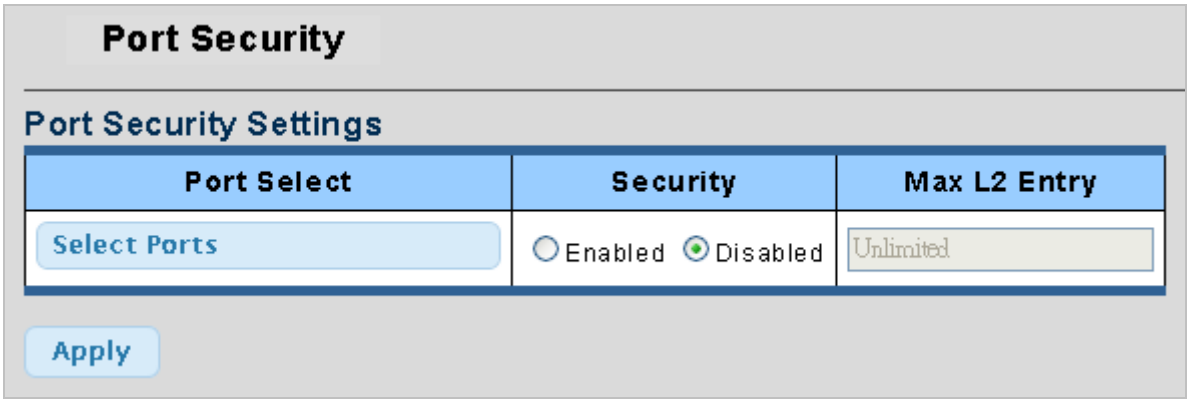


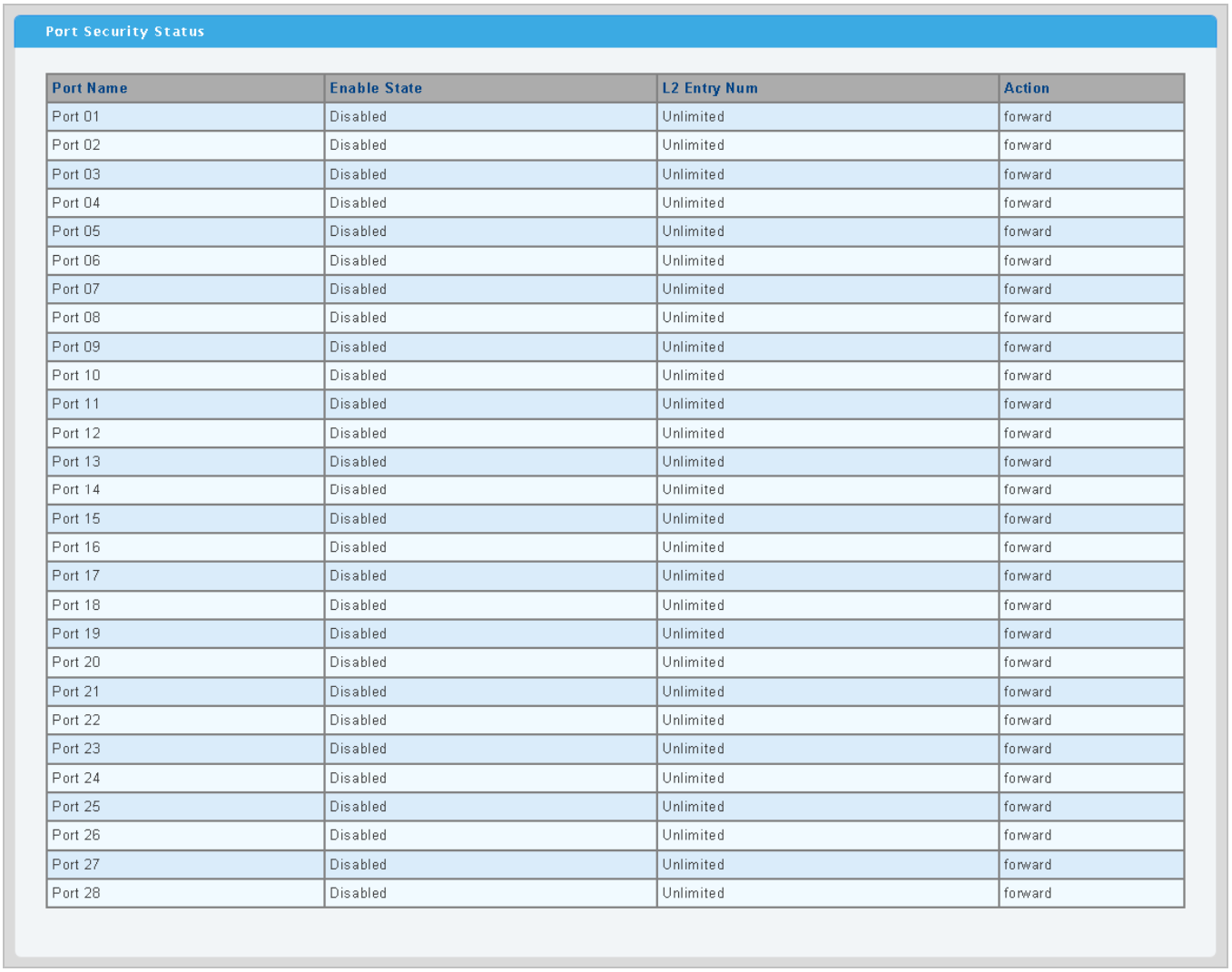
Figure 4-9-5 Port Security Settings page screenshot

The page includes the following fields:

Object	Description
• **Port Select**	Select port for this drop down list.
• **Security**	Enable or disable the port security.
• **Max L2 Entry**	The maximum number of MAC addresses that can be secured on this port. If the limit is exceeded, the corresponding action is taken. The stackswitch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Buttons

Apply: Click to apply changes.



Port Security Status

Port Name	Enable State	L2 Entry Num	Action
Port 01	Disabled	Unlimited	forward
Port 02	Disabled	Unlimited	forward
Port 03	Disabled	Unlimited	forward
Port 04	Disabled	Unlimited	forward
Port 05	Disabled	Unlimited	forward
Port 06	Disabled	Unlimited	forward
Port 07	Disabled	Unlimited	forward
Port 08	Disabled	Unlimited	forward
Port 09	Disabled	Unlimited	forward
Port 10	Disabled	Unlimited	forward
Port 11	Disabled	Unlimited	forward
Port 12	Disabled	Unlimited	forward
Port 13	Disabled	Unlimited	forward
Port 14	Disabled	Unlimited	forward
Port 15	Disabled	Unlimited	forward
Port 16	Disabled	Unlimited	forward
Port 17	Disabled	Unlimited	forward
Port 18	Disabled	Unlimited	forward
Port 19	Disabled	Unlimited	forward
Port 20	Disabled	Unlimited	forward
Port 21	Disabled	Unlimited	forward
Port 22	Disabled	Unlimited	forward
Port 23	Disabled	Unlimited	forward
Port 24	Disabled	Unlimited	forward
Port 25	Disabled	Unlimited	forward
Port 26	Disabled	Unlimited	forward
Port 27	Disabled	Unlimited	forward
Port 28	Disabled	Unlimited	forward

Figure 4-9-6 Port Security Status page screenshot

The page includes the following fields:

Object	Description
• **Port Name**	The switch port number of the logical port.
• **Enable State**	Display the current port security state.
• **L2 Entry Num**	Display the current L2 entry number.
• **Action**	Display the current action.

4.9.4 802.1X 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 PDU**s (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like **MD5-Challenge**, **PEAP**, and **TLS**. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

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

Overview of User Authentication

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

- **Remote Authentication Dial-in User Service (RADIUS)**

4.9.4.1 Port Isolate

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

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

This section includes this conceptual information:

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

- **Device Roles**

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

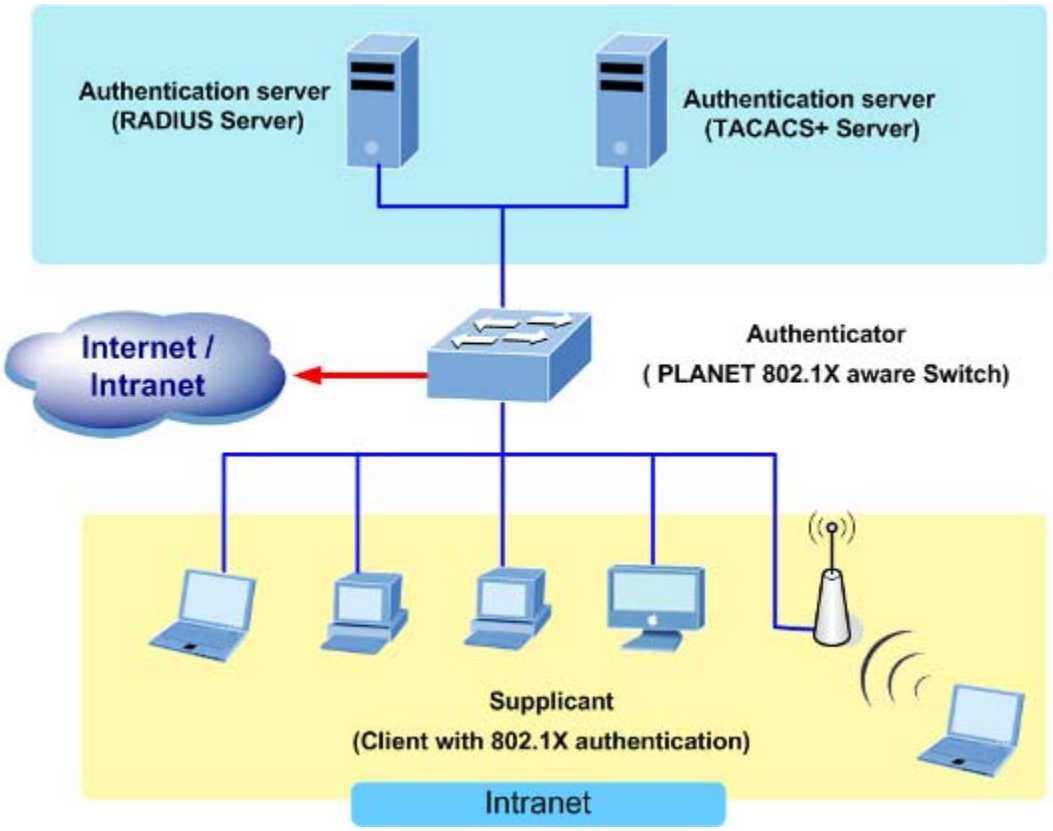


Figure 4-9-7

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

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

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

authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

■ **Authentication Initiation and Message Exchange**

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

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

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

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

The specific exchange of EAP frames depends on the authentication method being used. "Figure 4-9-8" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

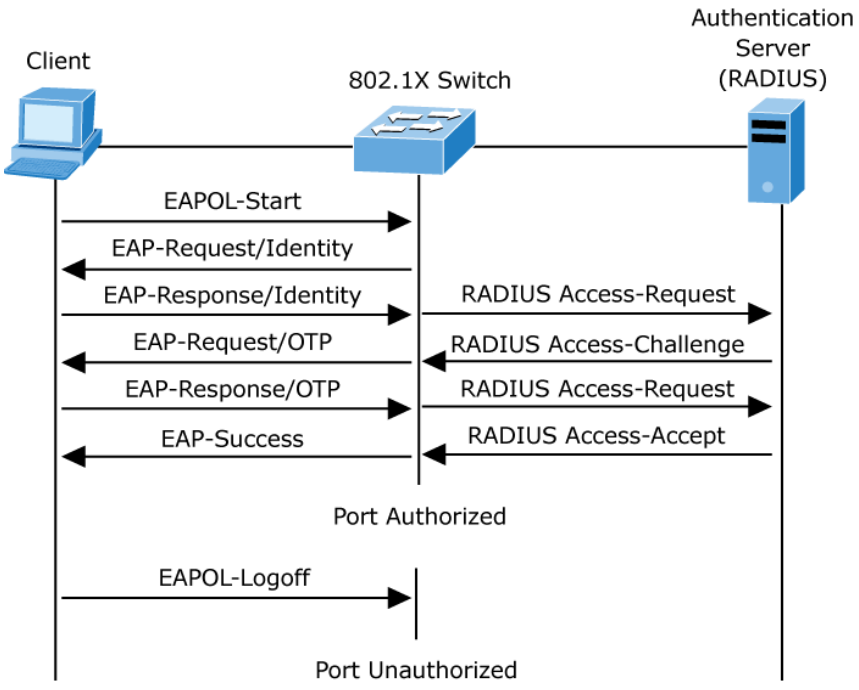


Figure 4-9-8 EAP message exchange

■ **Ports in Authorized and Unauthorized States**

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

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

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

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

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

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

4.9.4.2 802.1X Setting

This page allows you to configure the IEEE 802.1X authentication system.
The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Security→802.1X Access Control→802.1X Setting" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.
The 802.1X Setting screen in Figure 4-9-9 & Figure 4-9-10 appears.

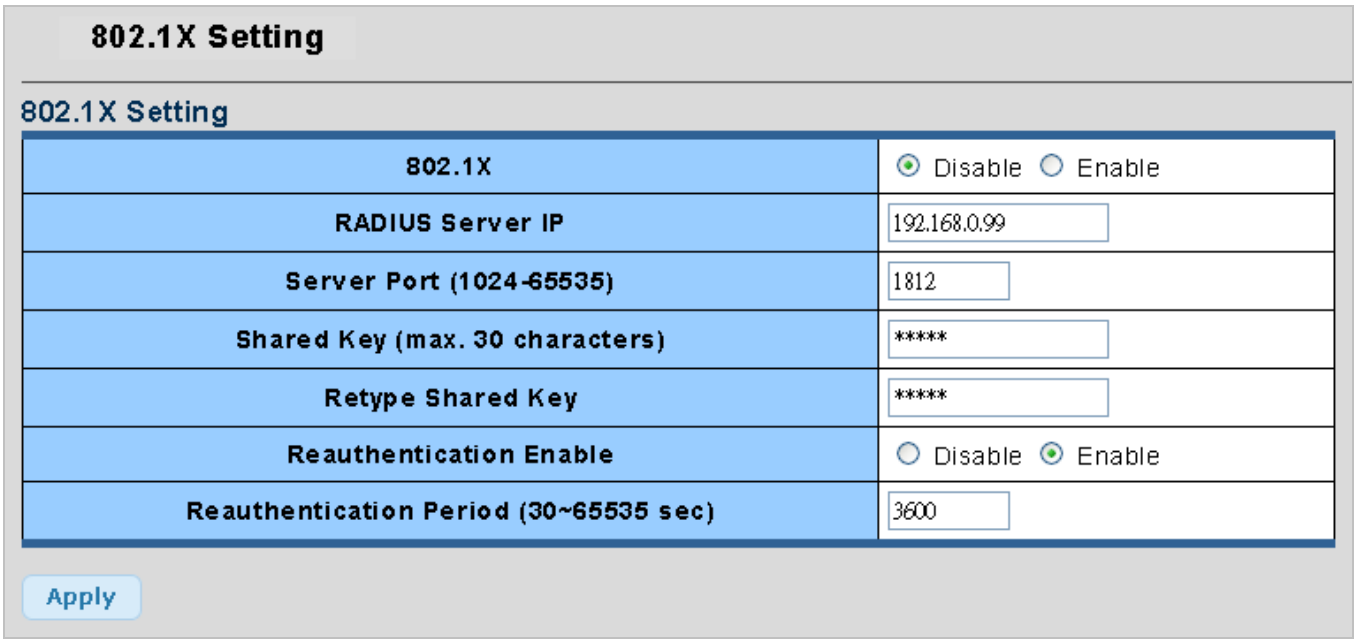


Figure 4-9-9 802.1X Setting page screenshot

The page includes the following fields:

Object	Description
• **802.1X**	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
• **RADIUS Server IP**	The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
• **Server Port (1024-65535)**	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
• **Shared Key** • **(max. 30 characters)**	The shared key - up to 30 characters long - shared between the RADIUS Authentication Server and the switch.
• **Retype Shared Key**	Please enter the shared key here again to confirm.
• **Reauthentication State**	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.
• **Reauthentication Period (30~65535 sec)**	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 30 to 65535 seconds.

Buttons

Apply: Click to apply changes.

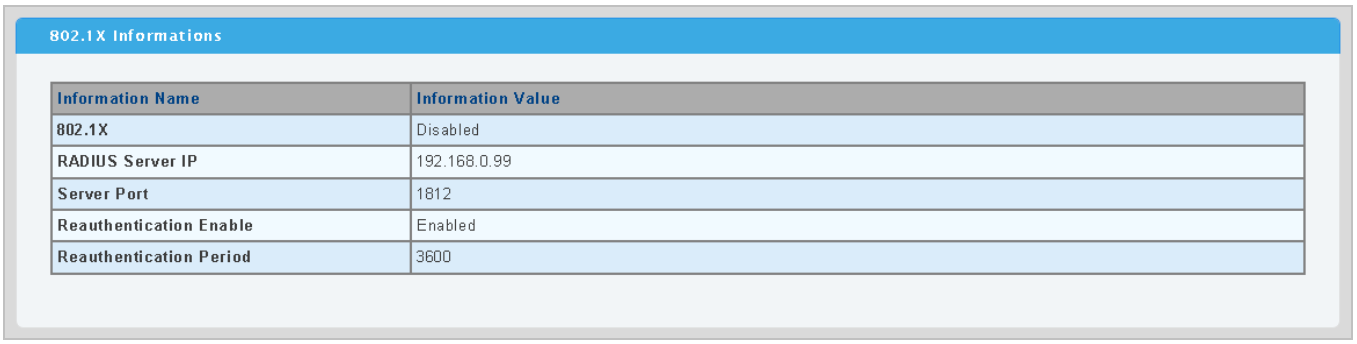


Figure 4-9-10 802.1X Informations page screenshot

The page includes the following fields:

Object	Description
• **802.1X**	Display the current 802.1X state.
• **RADIUS Server IP**	Display the current IP address of RADIUS server.
• **Server Port**	Display the current RADIUS server port.
• **Reauthentication State**	Display the current reauthentication state.
• **Reauthentication Period**	Display the current reauthentication period value.

4.9.4.3 802.1X Port Setting

This page allows you to configure the IEEE 802.1X Port Setting. The 802.1X Port Setting screen in Figure 4-9-11 & Figure 4-9-12 appears.

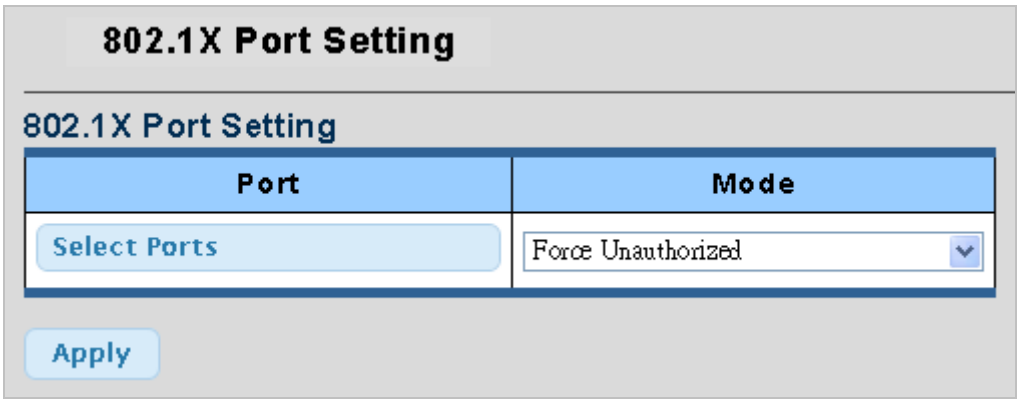


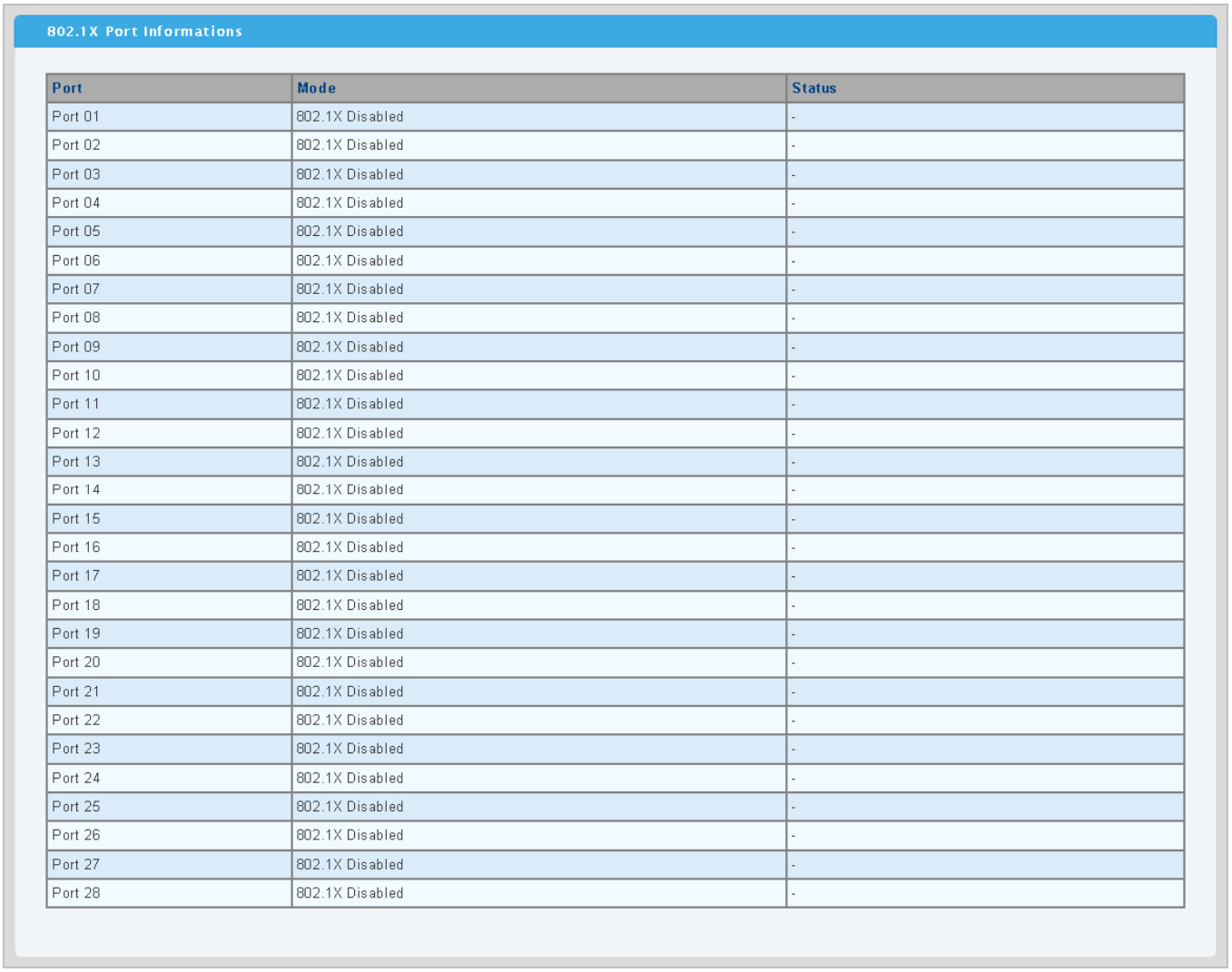
Figure 4-9-11 802.1X Port Setting page screenshot

The page includes the following fields:

Object	Description
• **Port**	Select port for this drop down list.
• **Mode**	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication. **Force Unauthorized** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Buttons

Apply: Click to apply changes.



802.1X Port Informations

Port	Mode	Status
Port 01	802.1X Disabled	-
Port 02	802.1X Disabled	-
Port 03	802.1X Disabled	-
Port 04	802.1X Disabled	-
Port 05	802.1X Disabled	-
Port 06	802.1X Disabled	-
Port 07	802.1X Disabled	-
Port 08	802.1X Disabled	-
Port 09	802.1X Disabled	-
Port 10	802.1X Disabled	-
Port 11	802.1X Disabled	-
Port 12	802.1X Disabled	-
Port 13	802.1X Disabled	-
Port 14	802.1X Disabled	-
Port 15	802.1X Disabled	-
Port 16	802.1X Disabled	-
Port 17	802.1X Disabled	-
Port 18	802.1X Disabled	-
Port 19	802.1X Disabled	-
Port 20	802.1X Disabled	-
Port 21	802.1X Disabled	-
Port 22	802.1X Disabled	-
Port 23	802.1X Disabled	-
Port 24	802.1X Disabled	-
Port 25	802.1X Disabled	-
Port 26	802.1X Disabled	-
Port 27	802.1X Disabled	-
Port 28	802.1X Disabled	-

Figure 4-9-12 802.1X Port Informations page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Mode**	Display the current 802.1X port mode.
• **Status**	Display the current 802.1X port status.

4.10 ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.
Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.
ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.
There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.
The ACL page contains links to the following main topics:

- **ACL Setting** Configuration ACL setting
- **ACL Template Setting** Configuration ACL templatefiltering
- **ACL Index Range Setting** Configuration ACL index range setting
- **ACL Policy Setting** Configuration ACL policy setting

4.10.1 ACL Setting

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The Voice VLAN OUI Table screen in Figure 4-10-1, Figure 4-10-2 & Figure 4-10-3 appears.

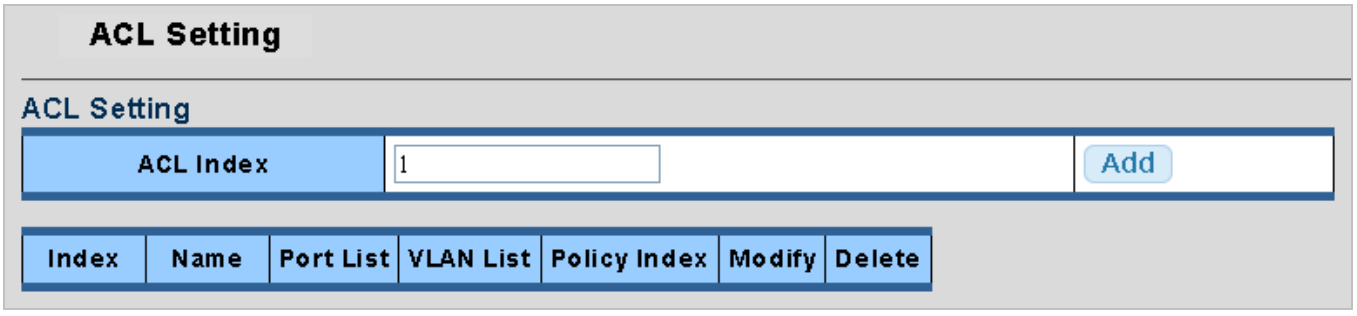


Figure 4-10-1 ACL Setting page screenshot

The page includes the following fields:

Object	Description
• **ACL Index**	Indicates the ACL index.
• **Index**	Display the current index.
• **Name**	Display the current name.

• **Port List**	Display the current port list.
• **VLAN List**	Display the current VLAN list.
• **Policy Index**	Display the current policy list.
• **Modify**	Click to modify the entry.
• **Delete**	Click to delete the entry.

Buttons

Add: Click to add new ACL index.

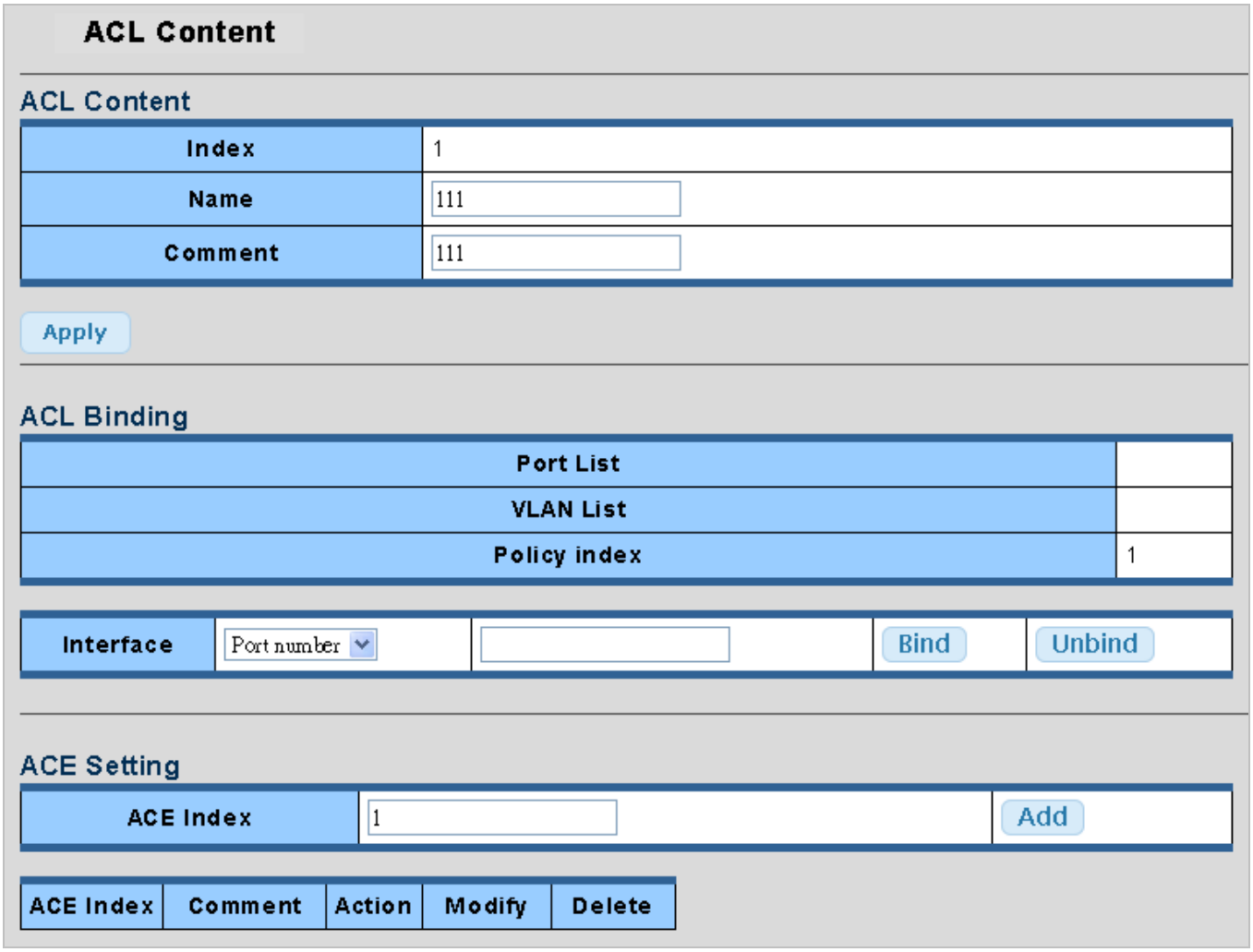


Figure 4-10-2 ACL Content page screenshot

ACL Content:

Object	Description
• **Index**	Display the current index.
• **Name**	Indicates the name.
• **Comment**	Indicates the comment.

ACL Binding:

Object	Description
• **Port List**	Display the current port list.
• **VLAN List**	Display the current VLAN list.
• **Policy Index**	Display the current policy index.
• **Interface**	Select interface for this drop down list that include: **Port number** **VLAN ID** **Policy ID**

ACE Setting:

Object	Description
• **ACE Index**	Indicates the ACE index.
• **ACE Index**	Display the current ACE index.
• **Comment**	Display the current comment.
• **Action**	Display the action.
• **Modify**	Click to modify the entry.
• **Delete**	Click to delete the entry.

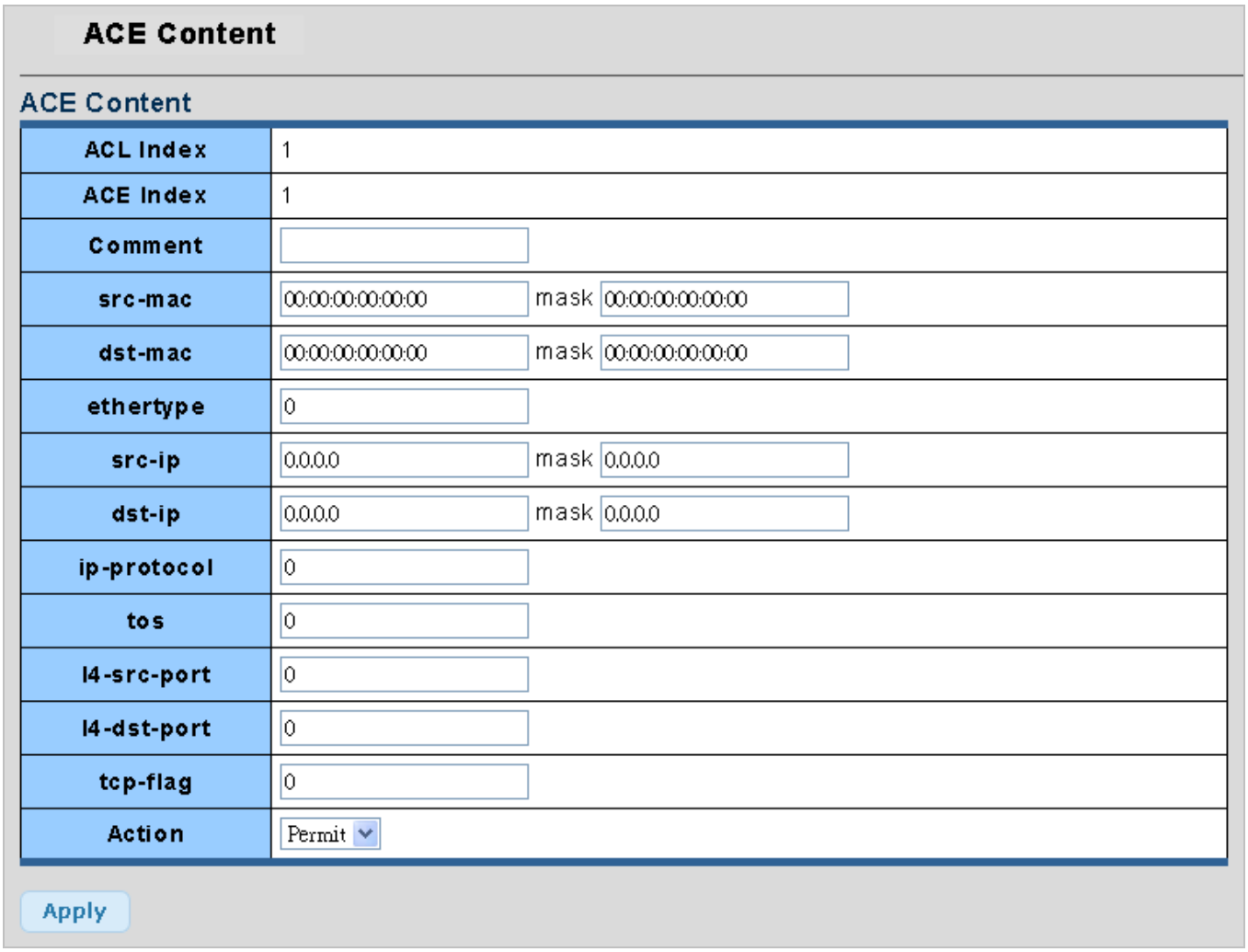


Figure 4-10-3 ACE Content page screenshot

The page includes the following fields:

Object	Description
• **ACL Index**	Display the current ACL index.
• **ACE Index**	Display the current ACE index.
• **Comment**	Indicates the comment.
• **Src-mac**	Source MAC address. Hexadecimal mask for source MAC address.
• **Dst-mac**	Destination MAC address. Hexadecimal mask for destination MAC address.
• **Ethertype**	This option can only be used to filter Ethernet II formatted packets.
• **Src-ip**	Source IP address. A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

• **Dst-ip**	Destination IP address. A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
• **Ip-portocol**	Specifies the protocol type to match as TCP or UDP.
• **Tos**	Specifies the ToS value.
• **L4-src-port**	Specifies the L4 source protocol port.
• **L4-dst-port**	Specifies the L4 destination protocol port.
• **Tcp-flag**	Specifies the TCP flag value.
• **Action**	An ACE can contain any combination of permit or deny rules. (Default: **Permit** rules)

4.10.2 ACL Template Setting

This page allows you to configure the ACL Template Setting. The ACL Template Setting screen in Figure 4-10-4 appears.

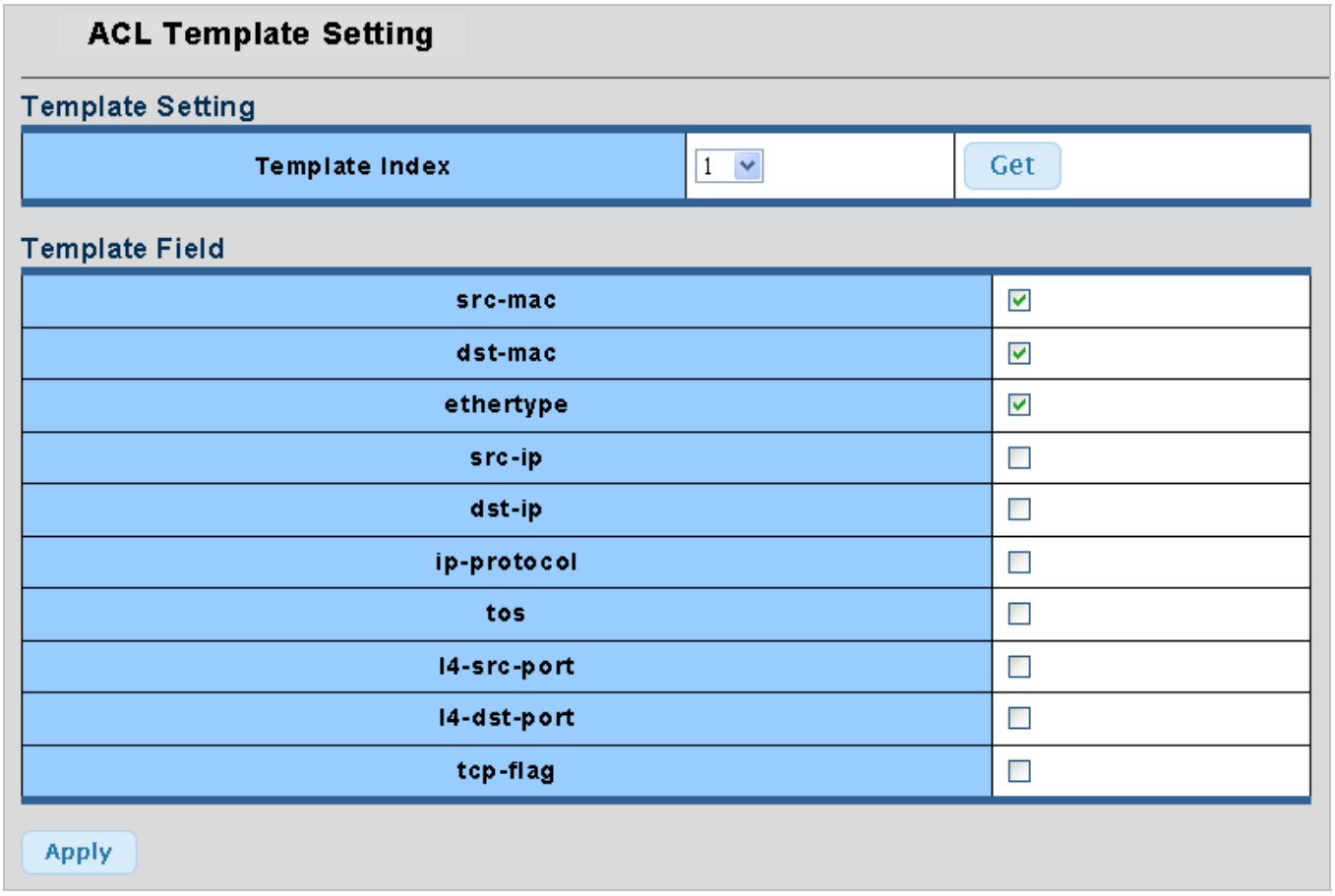


Figure 4-10-4 ACL Template Setting page screenshot

The page includes the following fields:

Object	Description
• **Template Index**	Select port for this drop down list.
• **Src-mac**	Enable or disable the source MAC address rule.
• **Dst-mac**	Enable or disable the destination MAC address rule.
• **Ethertype**	Enable or disable the Ethernet type rule.
• **Src-ip**	Enable or disable the source IP address rule.
• **Dst-ip**	Enable or disable the destination IP address rule.
• **Ip-protocol**	Enable or disable the IP protocol rule.
• **Tos**	Enable or disable the ToS value rule.
• **L4-src-port**	Enable or disable the L4 source port rule.
• **L4-dst-port**	Enable or disable the L4 destionation port rule.
• **Tcp-flag**	Enable or disable the TCP flag rule.

Buttons

: Click to apply changes.

4.10.3 ACL Index Range Setting

This page allows you to configure the ACL Index Range Setting. The ACL Index Range Setting screen in Figure 4-10-5 appears.

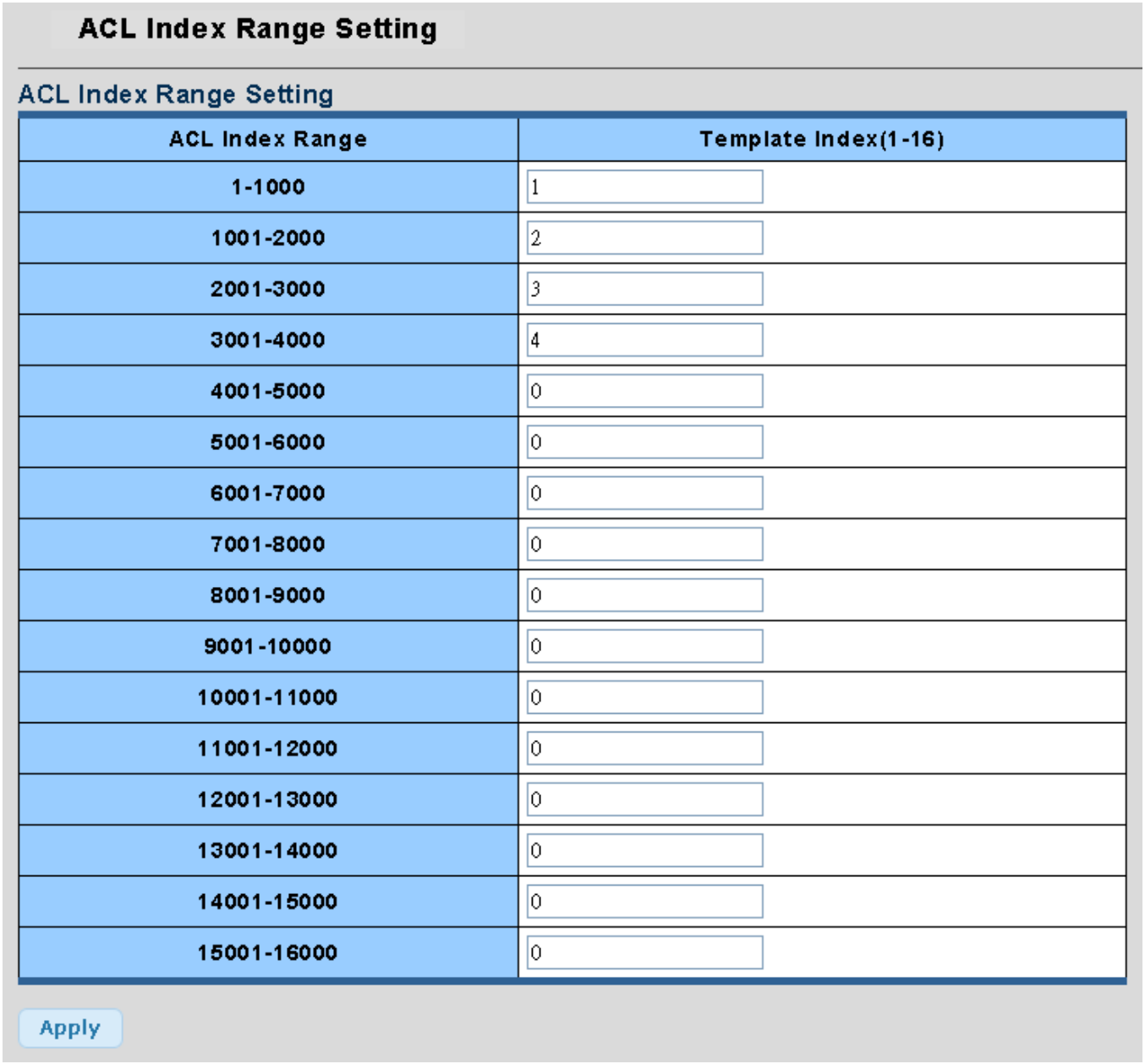


Figure 4-10-5 ACL Index Range Setting page screenshot

The page includes the following fields:

Object	Description
• **ACL Index Range**	Display the current ACL index.
• **Template Index**	Assign the current template index.

Buttons

Apply: Click to apply changes.

4.10.4 ACL Policy Setting

This page allows you to configure the ACL Policy Setting. The ACL Policy Setting screen in Figure 4-10-6 appears.

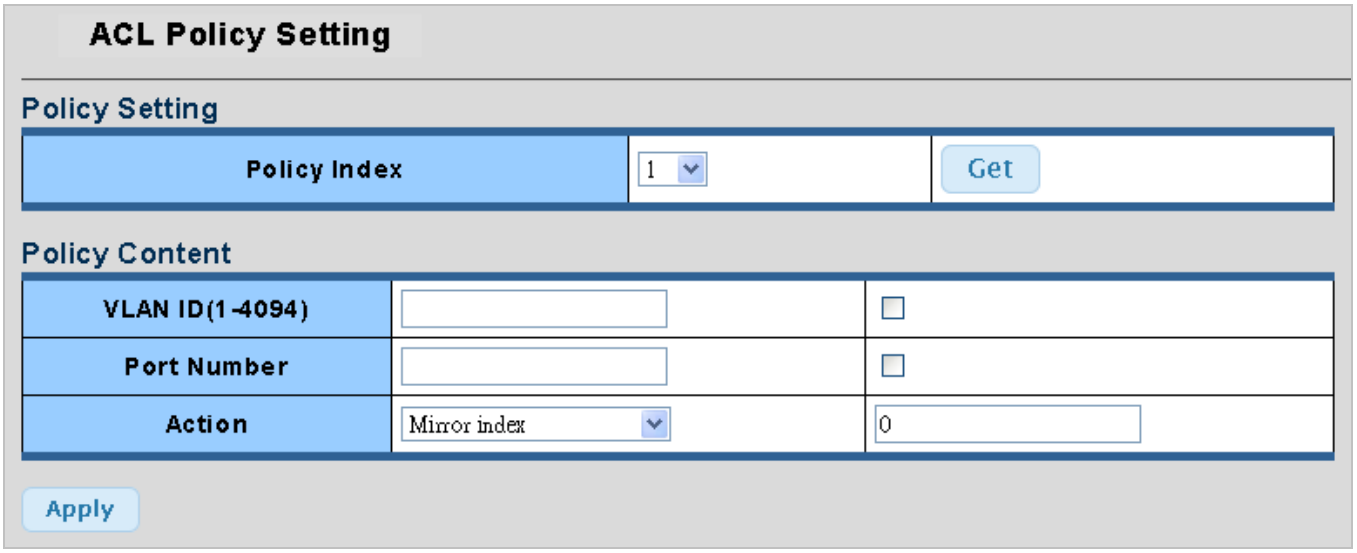


Figure 4-10-6 ACL Policy Setting page screenshot

The page includes the following fields:

Object	Description
• **Policy Index**	Select port for this drop down list.
• **VLAN ID (1-4094)**	Specifies the ToS value.
• **Port Number**	Specifies the ToS value.
• **Action**	Assign the ACL policy rule.

Buttons

Apply: Click to apply changes.

4.11 MAC Address Table

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

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

4.11.1 Dynamic Learned

Dynamic MAC Table

Dynamic Learned MAC Table are shown on this page. The MAC Table is sorted first by VLAN ID, then by MAC address. The Dynamic Learned screen in Figure 4-11-1 appears.

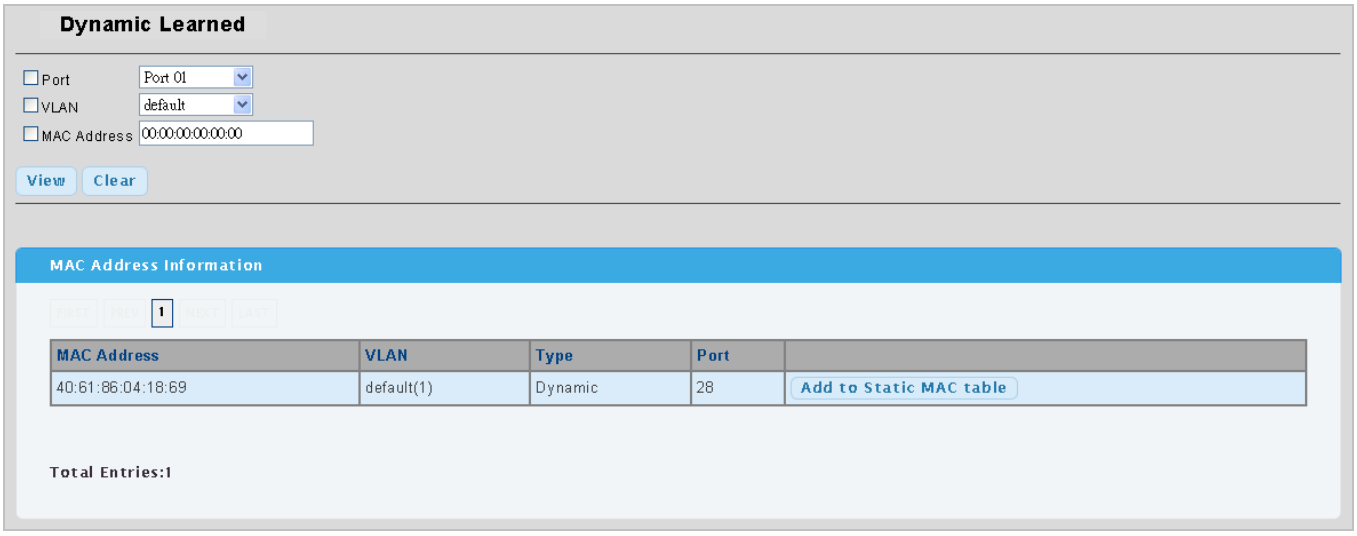


Figure 4-11-1 Dynamic Learned page screenshot

The page includes the following fields:

Object	Description
• **Port**	Indicates a port.
• **VLAN**	ID of configured VLAN (1-4094).
• **MAC Address**	Physical address associated with this interface.
• **MAC Address**	The MAC address of the entry.
• **VLAN**	The VLAN ID of the entry.
• **Type**	Indicates whether the entry is a static or dynamic entry.
• **Port**	The ports that are members of the entry.

Buttons

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

Clear: Flushes all dynamic entries.

Add to Static MAC table: Click to add dunamic MAC address to static MAC address.

4.11.1 Statics MAC Table Setting

The static entries in the MAC table are shown in this table. The MAC table is sorted first by VLAN ID and then by MAC address.

The Static MAC Setting screen in Figure 4-11-2 appears.

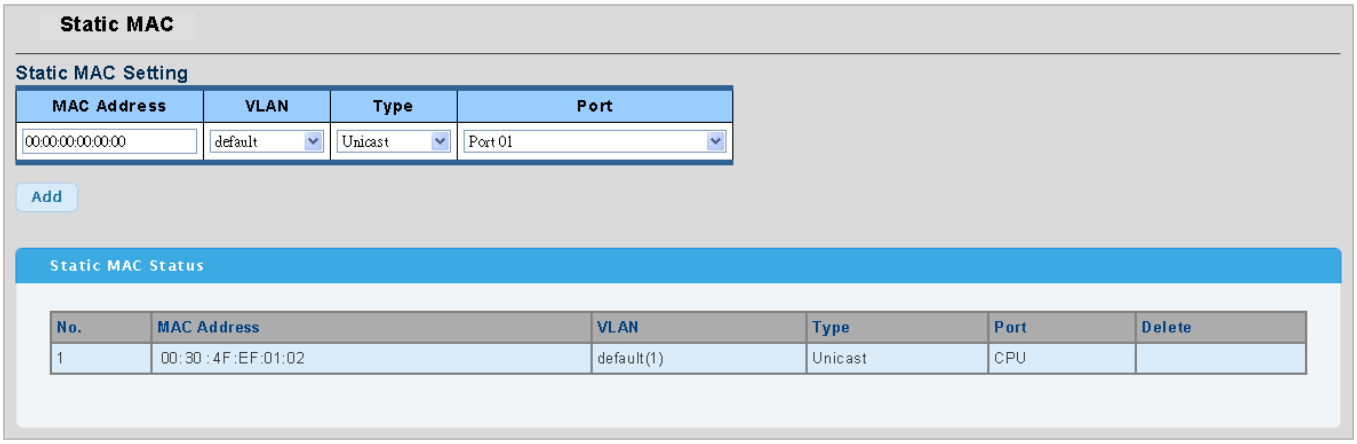


Figure 4-11-2 Statics MAC Setting page screenshot

The page includes the following fields:

Object	Description
• **MAC Address**	Physical address associated with this interface.
• **VLAN**	ID of configured VLAN (1-4094).
• **Type**	Specifies the MAC address type.
• **Port**	Select port for this drop down list.
• **No.**	This is the number for entries
• **MAC Address**	The MAC address for the entry.
• **VLAN**	The VLAN ID for the entry.
• **Type**	Display the current type.
• **Port**	Display the current port.
• **Delete**	Check to delete the entry.

Buttons

: Click to add new static MAC address.

4.12 Diagnostics

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

Use the Diagnastics 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:

■ **Ping Test**	The ping allow you to issue ICMP PING packets to troubleshoot IP connectivity issues. The Managed Switch transmit ICMP packets, and the sequence number and roundtrip time are displayed upon reception of a reply.

4.12.1 Ping Test

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

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

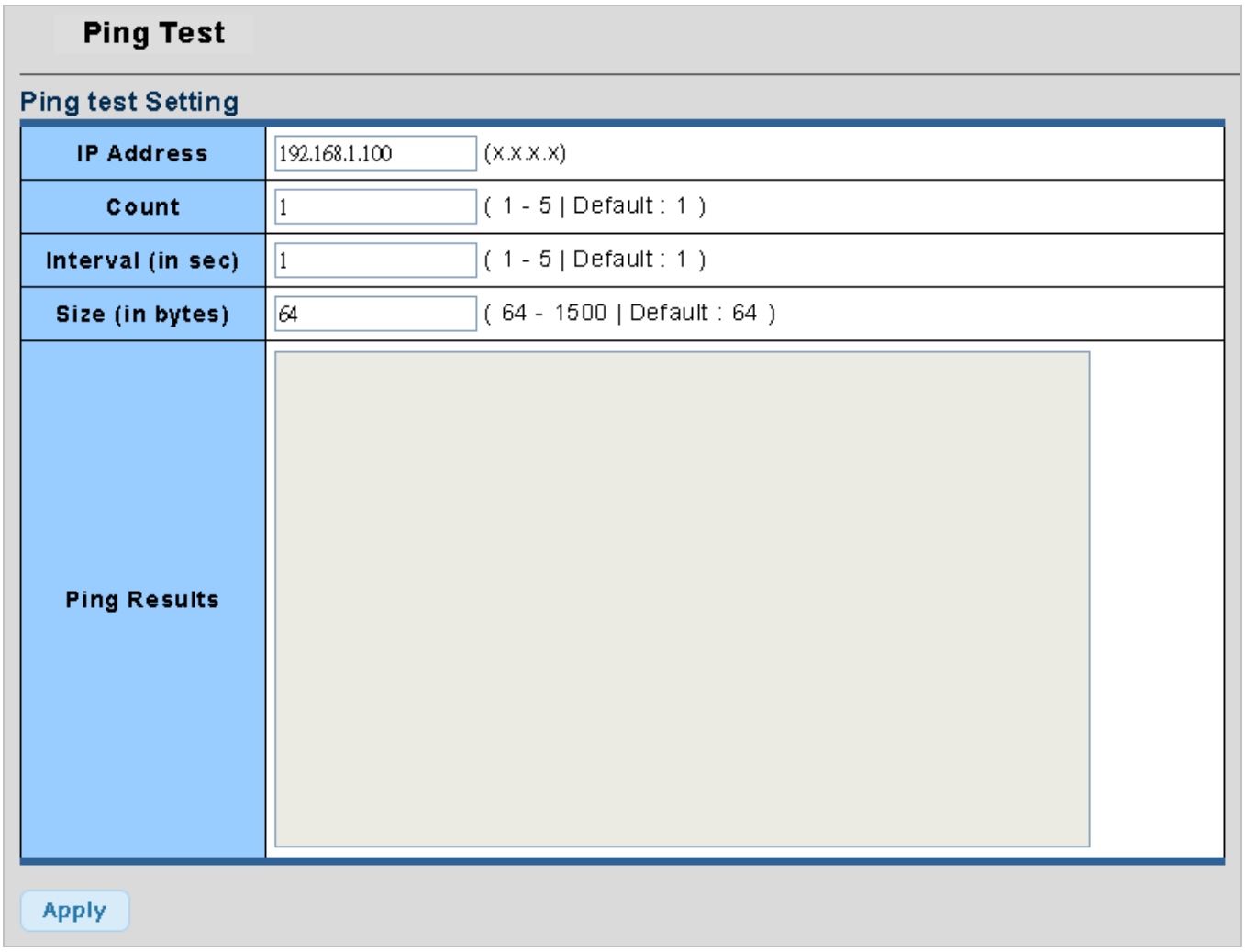


Figure 4-12-1 ICMP Ping page screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address.
• **Count**	Number of echo requests to send.
• **Interval (in sec)**	Send interval for each ICMP packet.
• **Size (in bytes)**	The payload size of the ICMP packet. Values range from 64 bytes to 1500 bytes.
• **Ping Results**	Display the current ping result.

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

Buttons

Apply: Click to transmit ICMP packets.

4.13 Power over Ethernet (WGSW-28040P Only)

Providing up to 24 PoE, in-line power interface, the WGSW-28040PPoE 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.

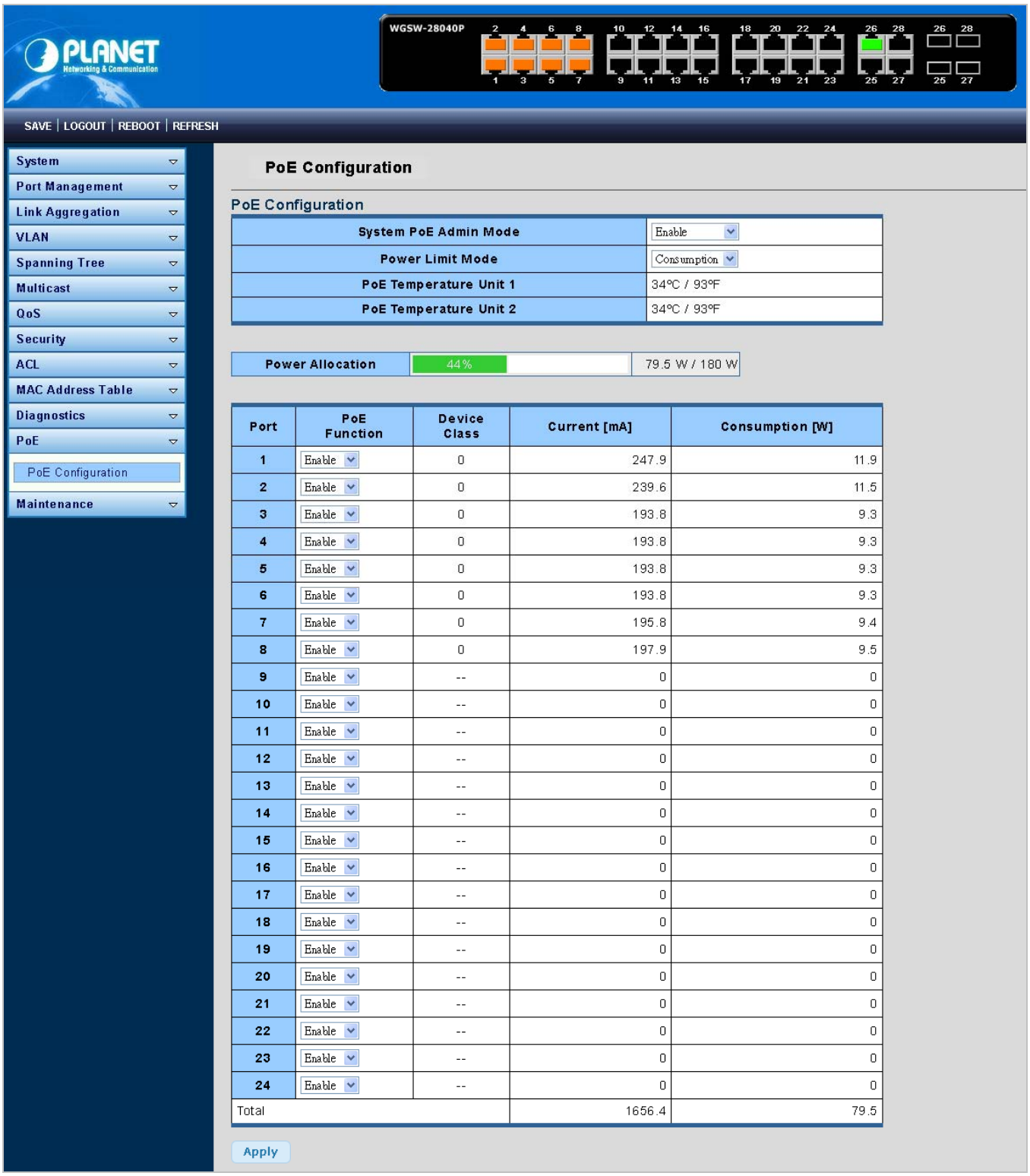


Figure 4-13-1 Power over Ethernet Status

4.13.1 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.

4.13.2 PoE 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.

This section allows the user to inspect and configure the current PoE port settings and the current status for all PoE ports; screen in Figure 4-13-2 appears.

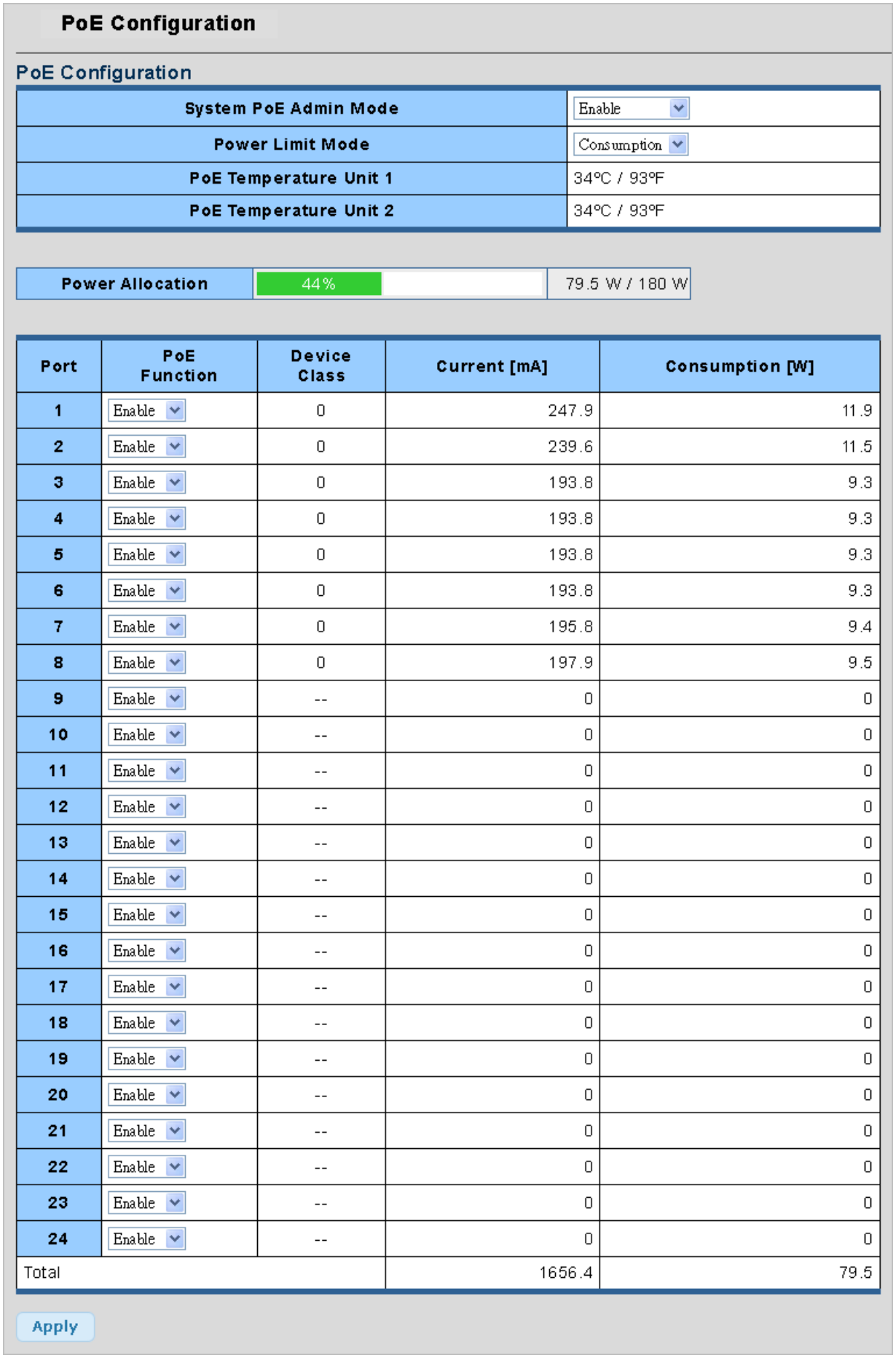


Figure 4-13-2 PoE Configuration screenshot

The page includes the following fields:

Object	Description
• **System PoE Admin Mode**	Allows user enable or disable PoE function. It will causes all of PoE ports supply or not supply power.
• **Power Limit Mode**	There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports. **Consumption mode** The default PoE management mode is "**Consumption mode**".
• **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
• **Power Allocation**	Show the total watts usage of PoE Switch.
• **Port**	This is the logical port number for this row.
• **PoE Function**	There are two modes for PoE mode. **Enable**: enable PoE function.. **Disable**: disable PoE function.
• **Device Class**	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 4-13-1**.
• **Current [mA]**	Shows how much ampere the PD currently is using.
• **Consumption [W]**	Shows how much power the PD currently is using.

Buttons

Apply: Click to save changes.

4.14 Maintenance

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

- **Backup Manager** You can backup the switch configuration.
- **Upgrade Manager** You can upgrade the switch configuration.
- **Save Configuration** You can save the switch configuration.
- **Factory Default** You can reset the configuration of the stack switch on this page.
- **Reboot Switch** You can restart the stack switch on this page. After restart, the stack switch will boot normally.

4.14.1 Backup Manager

This function allows backup the current image or configuration of the Managed Switch to the local management station. The Backup Manager screen in Figure 4-14-1 appears.

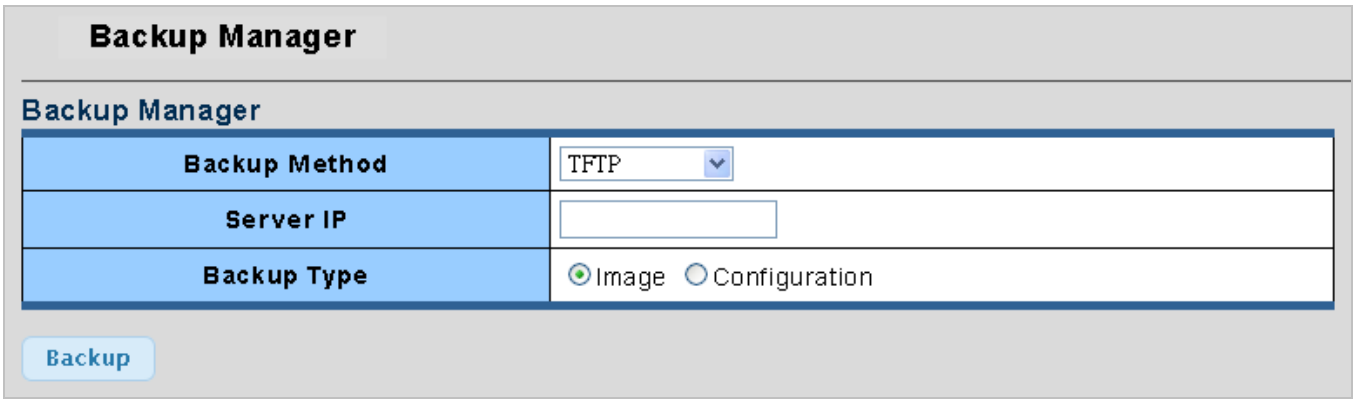


Figure 4-14-1 Backup Manager page screenshot

The page includes the following fields:

Object	Description
• **Backup Method**	Select backup method for this drop down list.
• **Server IP**	Fill in your TFTP server IP address.
• **Backup Type**	Select backup type.

Buttons

Backup: Click to backup image or configuration.

4.14.2 Upgrade Manager

This function allows reload the current image or configuration of the Managed Switch to the local management station. The Upgrade Manager screen in Figure 4-14-2 appears.

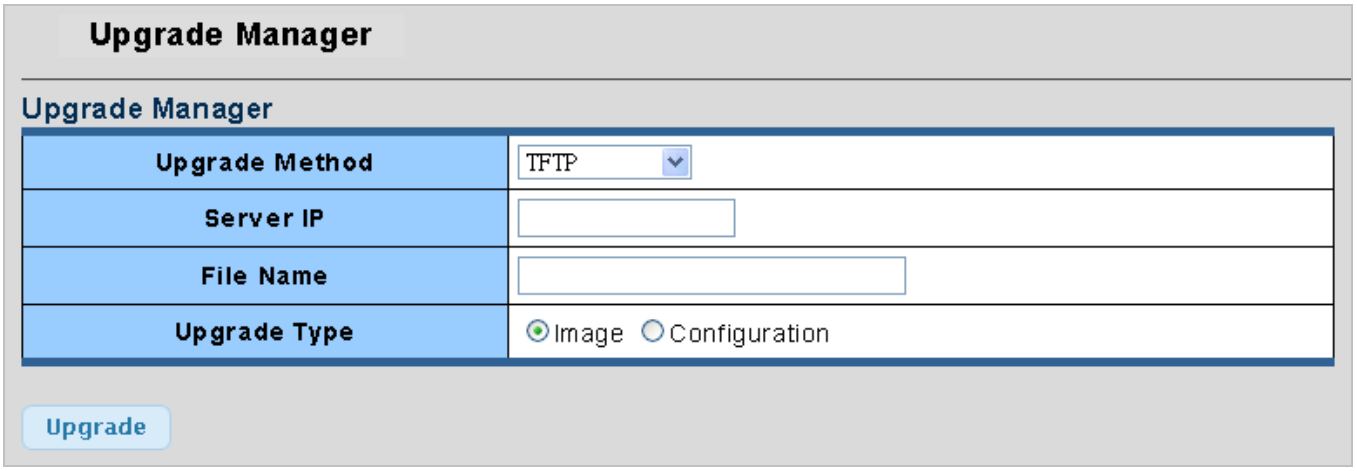


Figure 4-14-2 Upgrade Manager page screenshot

The page includes the following fields:

Object	Description
• **Upgrade Method**	Select upgrade method for this drop down list.
• **Server IP**	Fill in your TFTP server IP address.
• **File Name**	The name of firmware image or configuration.
• **Upgrade Type**	Select upgrade type.

Buttons

Upgrade: Click to upgrade image or configuration.

4.14.3 Save Configuration

This function allows save the current configuration of the Managed Switch to the local management station. The Save Configuration screen in Figure 4-14-3 appears.

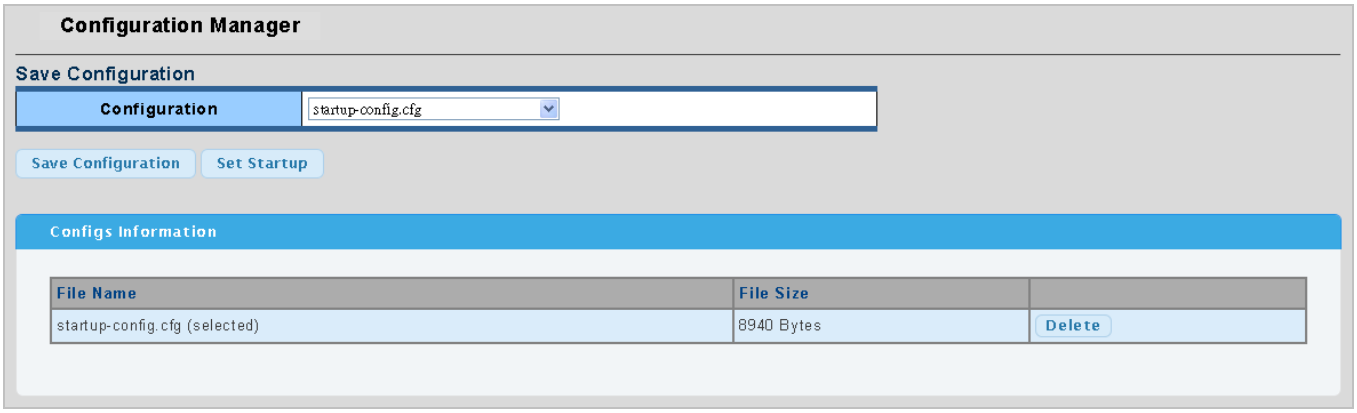


Figure 4-14-3 Configuration Manager page screenshot

The page includes the following fields:

Object	Description
• **Configuration**	Select configuration name for this drop down list.
• **File Name**	Display the current file name.
• **File Size**	Display the current file size.

Buttons

Save Configuration: Click to save configuration.

Set Startup: Click to set startup configuration.

4.14.4 Factory Default

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in Figure 4-14-4 appears.

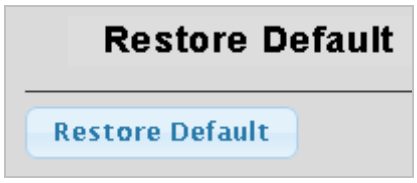


Figure 4-14-4 Factory Default page screenshot

Buttons

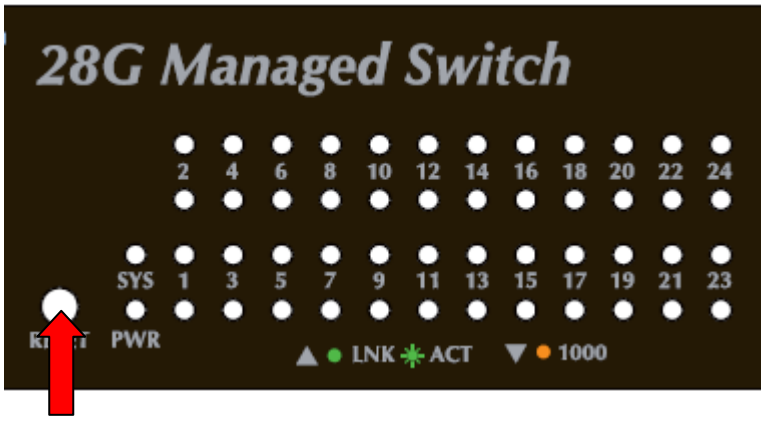
Restore Default: Click to reset the configuration to Factory Defaults.

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.

Note

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

4.14.5 Reboot Switch

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 Reboot Switch screen in Figure 4-14-5 appears.

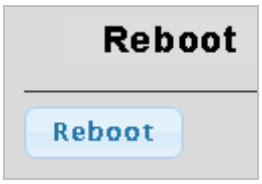


Figure 4-14-5 Reboot Switch page screenshot

Buttons

Reboot: Click to reboot the system.

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 off, then it is in the firmware load stage; if the SYS LED light on, you can use the WEB browser to login the Switch.

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 Managed Switch, the terminal will display that it is running testing procedures.

Then, the following message asks the login username & password. The factory default password as following and the login screen in Figure 5-1 appears.

Username: **admin**
Password: **admin**

1. On "**Username**" & "**Password**"prompt, enter "**admin**".
2. On "**WGSW-28040>**" prompt, enter "**enable**".
3. On "**Username**" & "**Password**"prompt, enter "**admin**".

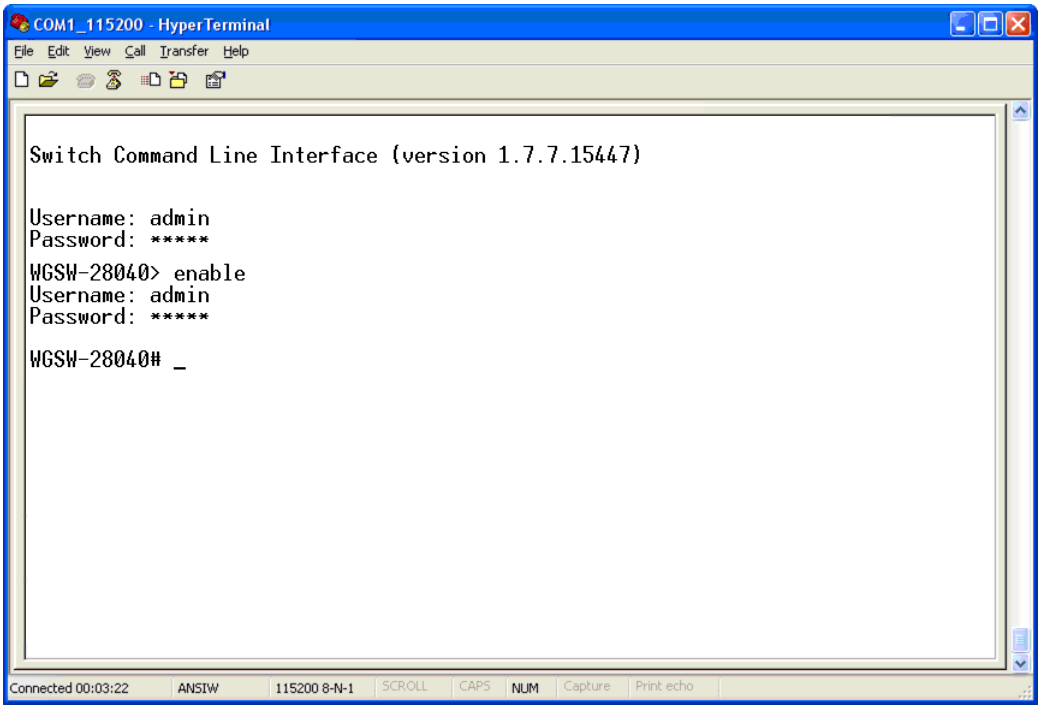


Figure 5-1 WGSW Managed Switch Console Login screen

Note

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

Configure IP address

The 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 "**WGSW-28040#**" prompt, enter "**config**".
2. On "**WGSW-28040(config)#**" prompt, enter "**show ip**".
3. The screen displays the current IP address, Subnet Mask and Gateway. As show in Figure 5-2.

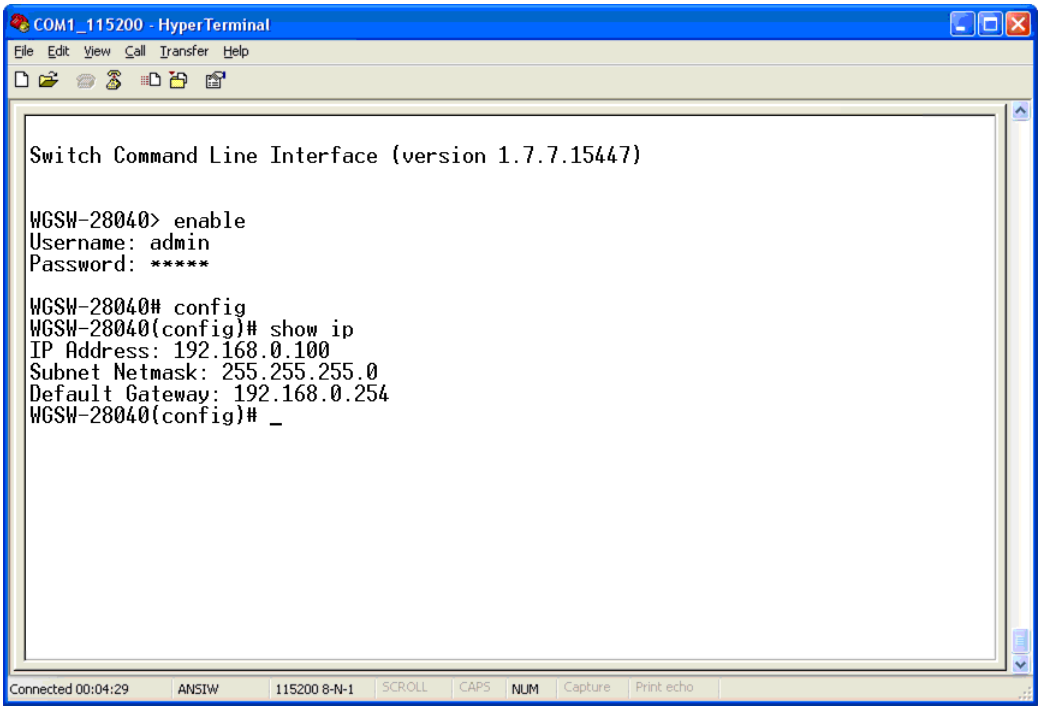


Figure 5-2 Show IP information screen

■ **Configure IP address**

4. On "**WGSW-28040(config)#**" prompt, enter the following command and press **<Enter>**. As show in Figure 5-3.

```
WGSW-28040(config)# ip address 192.168.1.100 255.255.255.0
WGSW-28040(config)# ip default-gateway 192.168.1.254
```

The previous command would apply the follow settings for the Switch.

IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254

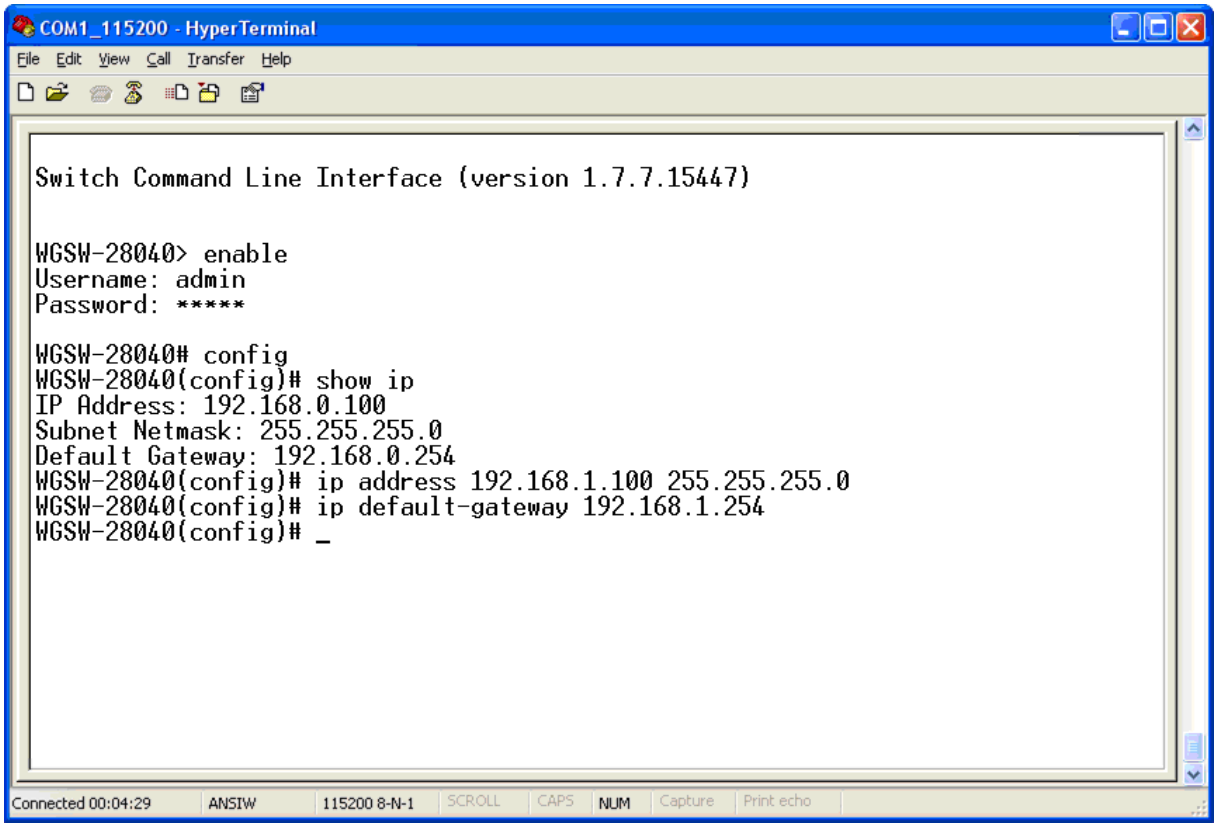


Figure 5-3 Set IP address screen

5. Repeat Step 1 to check if the IP address is changed.

If the IP address is successfully configured, the Managed Switch will apply the new IP address setting immediately. You can access the Web interface of WGSW Managed Switch through the new IP address.

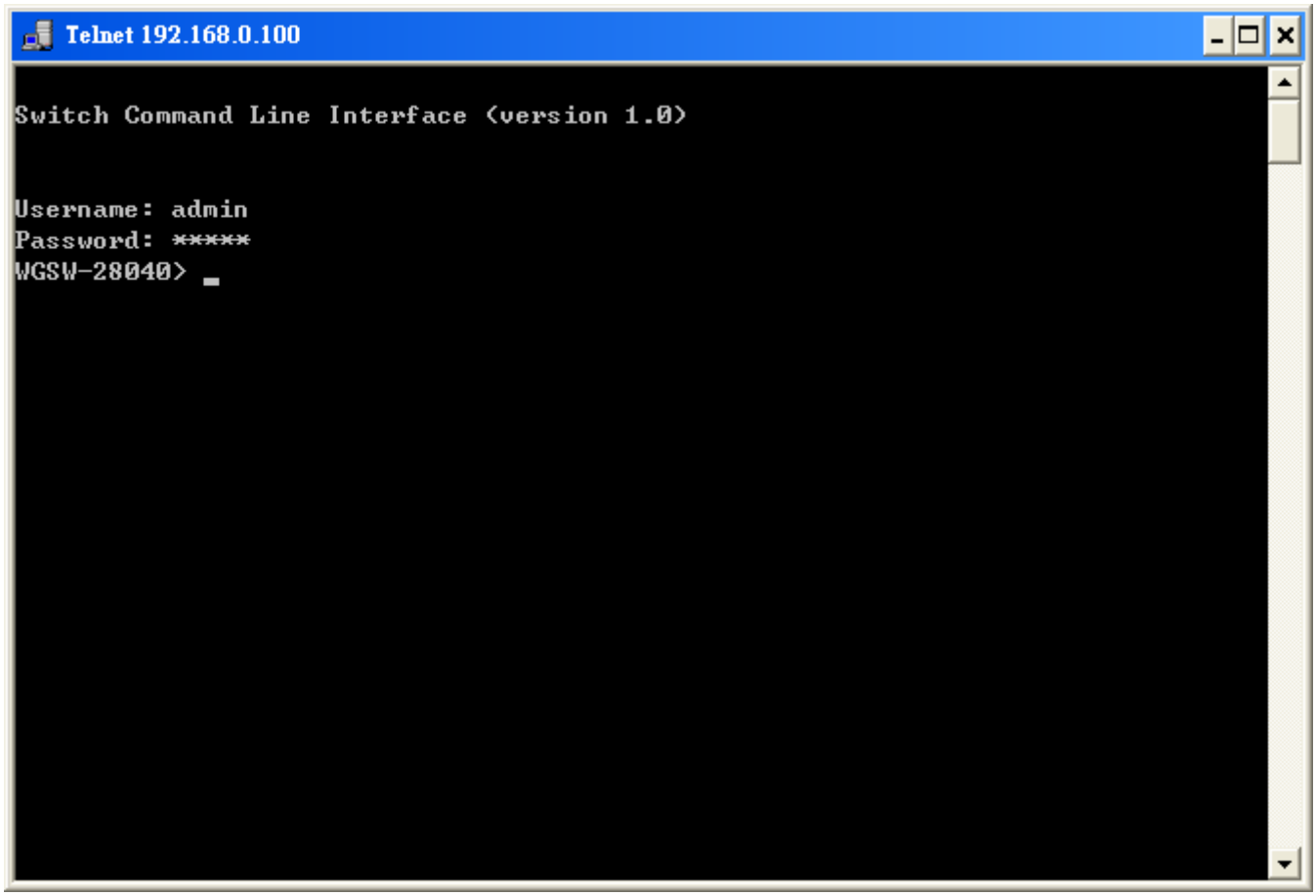
Note

If you do not familiar with console command or the related parameter, enter "**?**" 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 username & 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.

Mode-based Command Hierarchy

The **Command Line Interface (CLI)** groups all the commands in appropriate modes by the nature of the commands. Examples of the CLI command modes are described below. Each of the command modes supports specific switch's commands.

The CLI Command Modes table captures the command modes, the prompts visible in that mode and the exit method from that mode.

Command Mode	Access Method	Prompt	Exit or Access Previous Mode
User Mode	This is the first level of access. Perform basic tasks and list system information.	WGSW-28040>	Enter Logout command
Privileged Mode	From the User Mode, enter the enable command.	WGSW-28040#	To exit to the User Mode, enter exit or Logout.
Global Config Mode	From the Privileged Mode, enter the configuration command.	WGSW-28040 (Config)#	To exit to the Privileged Mode, enter the exit command.

Table 6-1 CLI Command Modes

The CLI is divided into various modes. The commands in one mode are not available until the operator switches to that particular mode. The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, and displayss a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

User Mode

When the operator logs into the CLI, the User Mode is the initial mode. The User Mode contains a limited set of commands. The command prompt shown at this level is:

Command Prompt: WGSW-28040>

Privileged Mode

To have access to the full suite of commands, the operator must enter the Privileged Mode. The Privileged Mode requires password authentication. From Privileged Mode, the operator can issue any Exec command to enter the Global Configuration mode. The command prompt shown at this level is:

Command Prompt: WGSW-28040#

Global Config Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the Interface Configuration mode. The command prompt at this level is:

Command Prompt: WGSW-28040(Config)#

From the Global Config mode, the operator may enter the following configuration modes:

6.1 User Mode Commands

6.1.1 Show Command

Show Version

Description:

Display software version

Syntax:

Show version

Example:

To display system version:

```
WGSW-28040> show version
PLANET v1.0 (WGSW-28040)
Copyright (C) 2011 Planet Technology Corporation.
WGSW-28040>
```

Show History

Description:

List the last several history commands

Syntax:

Show history

Example:

To display history:

```
WGSW-28040> show history
```

Show Info

Description:

Basic information

Syntax:

Show info

Example:

To display system information:

```
WGSW-28040> show info
MAC Address          : 00:30:4F:EF:01:02
IP Address           : 192.168.0.100
Subnet Mask          : 255.255.255.0
Loader Version       : 1.3.0
Loader Date          : Feb 10 2011 - 02:04:21
Firmware Version : 1.0
Firmware Date        : Tue Apr 12 10:12:44 CST 2011
System Object ID : 1.3.6.1.4.1.10456.1.1509
WGSW-28040>
```

Show Privilege

Description:

Local user privilege level

Syntax:

Show privilege

Example:

To display username privilege:

```
WGSW-28040> show privilege
Current CLI Username:    admin
Current CLI Privilege: Admin
WGSW-28040>
```

6.1.2 Enable Command

Enable

Description:

Turn on privileged mode command

Syntax:

enable

Example:

To turn on privileged mode command:

```
WGSW-28040> enable
WGSW-28040#
```

6.2 Privileged Mode Commands

6.2.1 Show Command

Show History

Description:

List the last several history commands

Syntax:

Show history

Example:

To display history:

```
WGSW-28040# show history
```

Show Startup-config

Description:

Contentes of startup configuration

Syntax:

Show startup-config

Example:

To display system startup-config:

```
WGSW-28040# show startup-config
```

Show Version

Description:

Display software version

Syntax:

Show version

Example:

To display system version:

```
WGSW-28040# show version
PLANET v1.0 (WGSW-28040)
Copyright (C) 2011 Planet Technology Corporation.
WGSW-28040#
```

Show Running-config

Description:

Running configurations

Syntax:

Show running-config

Example:

To display system running-config:

```
WGSW-28040# show running-config
```

Show Privilege

Description:

Local user privilege level

Syntax:

Show privilege

Example:

To display username privilege:

```
WGSW-28040# show privilege
Current CLI Username:    admin
Current CLI Privilege: Admin
WGSW-28040#
```

6.2.2 Configuration Command

Config

Description:

Configuration from vty interface

Syntax:

config

Example:

To turn on global config mode command:

```
WGSW-28040# config
WGSW-28040(config)#
```

6.2.3 Disable Command

Disable

Description:

Turn off privileged mode command

Syntax:

disable

Example:

To turn off privileged mode command:

```
WGSW-28040# disable
WGSW-28040>
```

6.3 Global Config Mode Commands

6.3.1 Hostname Command

Hostname

Description:

Set system's network name

Syntax:

Hostname [<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.

Example:

To set system's network name:

```
WGSW-28040(config)# hostname test_switch
test_switch(config)#
```

6.3.2 History Command

History

Description:

Set the number of history commands

Syntax:

history

Parameters:

<1-256> : Number of commands, range is 1-256

Example:

To set number of history:

```
WGSW-28040(config)# history 200
WGSW-28040(config)#
```

6.3.3 No Command

No History

Description:

Disable command history

Syntax:

no history

Example:

Disable command history:

```
WGSW-28040(config)# no history
WGSW-28040(config)#
```

No More

Description:

Show XMORE page on cli

Syntax:

no more

Example:

Disable XMORE page on cli:

```
WGSW-28040(config)# no more
WGSW-28040(config)#
```

No ACL

Description:

ACL configuration

Syntax:

no acl [<acl_index>] [apply]

Parameters:

<1-16000> :ACL index

apply :Apply ACL configuration to interface

Example:

Disable ACL configuration:

```
WGSW-28040(config)# no acl 1
WGSW-28040(config)#
```

No ACL Range

Description:

ACL range configuration

Syntax:

no acl-range <index_range>

Parameters:

< index_range >	:1-1000	Index 1-1000
	1001-2000	Index 1001-2000
	2001-3000	Index 2001-3000
	3001-4000	Index 3001-4000
	4001-5000	Index 4001-5000

5001-6000	Index 5001-6000
6001-7000	Index 6001-7000
7001-8000	Index 7001-8000
8001-9000	Index 8001-9000
9001-10000	Index 9001-10000
10001-11000	Index 10001-11000
11001-12000	Index 11001-12000
12001-13000	Index 12001-13000
13001-14000	Index 13001-14000
14001-15000	Index 14001-15000
15001-16000	Index 15001-16000

Example:

Disable ACL range configuration:

```
WGSW-28040(config)# no acl-range 3
WGSW-28040(config)#
```

No ACL Policy

Description:

ACL policy configuration

Syntax:

no acl-policy <policy_index>

Parameters:

< policy_index > :1-16

Example:

Disable ACL policy configuration:

```
WGSW-28040(config)# no acl-policy 1
WGSW-28040(config)#
```

No Dot1x Re-authentication

Description:

Disabel dot1x re-authentication function

Syntax:

no dot1x <reauth| reauth-period>

Parameters:

reauth :Enable/Disabel re-authentication function

reauth-period : re-authentication period

Example:

Disabel re-authentication function:

```
WGSW-28040(config)# no dot1x reauth
WGSW-28040(config)#
```

No IGMP Snooping Fastleave

Description:

Disabel IGMP-snooping fastleave function

Syntax:

no igmp-snooping fastleave

Example:

Disabel IGMP-snooping fastleave function:

```
WGSW-28040(config)# no igmp-snooping fastleave
WGSW-28040(config)#
```

No IGMP Snooping Debug

Description:

Disabel IGMP-snooping debug function

Syntax:

no igmp-snooping debug

Example:

Disabel IGMP-snooping debug function:

```
WGSW-28040(config)# no igmp-snooping debug
WGSW-28040(config)#
```

No IGMP Snooping Router Timeout

Description:

Disabel IGMP-snooping router timeout function

Syntax:

no igmp-snooping router-timeout

Example:

Disabel IGMP-snooping router-timeout function:

```
WGSW-28040(config)# no igmp-snooping router-timeout
WGSW-28040(config)#
```

No IGMP Snooping Robustness Variable

Description:

Disabel IGMP-snooping robustness-variablet function

Syntax:

no igmp-snooping robustness-variable

Example:

Disabel IGMP-snooping robustness-variable function:

```
WGSW-28040(config)# no igmp-snooping robustness-variable
WGSW-28040(config)#
```

No IGMP Snooping Response Time

Description:

Disabel IGMP-snooping response-time function

Syntax:

no igmp-snooping response-time

Example:

Disabel IGMP-snooping response-time function:

```
WGSW-28040(config)# no igmp-snooping response-time
WGSW-28040(config)#
```

No IGMP Snooping Query Interval

Description:

Disabel IGMP-snooping query-interval function

Syntax:

no igmp-snooping query-interval

Example:

Disabel IGMP-snooping query-interval function:

```
WGSW-28040(config)# no igmp-snooping query-interval
WGSW-28040(config)#
```

No IGMP Snooping Last Member Query Interval

Description:

Disabel IGMP-snooping last-member-query-interval function

Syntax:

no igmp-snooping last-member-query-interval

Example:

Disabel IGMP-snooping last-member-query-interval function:

```
WGSW-28040(config)# no igmp-snooping last-member-query-interval
WGSW-28040(config)#
```

No IGMP Snooping VLAN

Description:

Disabel IGMP-snooping vlan function

Syntax:

no igmp-snooping vlan <vid>

Parameters:

<vid> : VLAN ID (1-4094)

Example:

Disabel IGMP-snooping vlan function:

```
WGSW-28040(config)# no igmp-snooping vlan 1
WGSW-28040(config)#
```

No IGMP Snooping Querier

Description:

Disabel IGMP-snooping querier function

Syntax:

no igmp-snooping querier <vid>

Parameters:

<vid> : VLAN ID (1-4094)

Example:

Disabel IGMP-snooping querier function:

```
WGSW-28040(config)# no igmp-snooping querier 1
WGSW-28040(config)#
```

No MAC Address Table Static

Description:

Disabel special statics MAC address function

Syntax:

no mac-address-table static <A:B:C:D:E:F>

Parameters:

A:B:C:D:E:F :MAC address xx:xx:xx:xx:xx:xx

Example:

Disabel statics MAC address:

```
WGSW-28040(config)# no mac-address-table static 00:30:4f:11:22:33
WGSW-28040(config)#
```

No MAC Address Table Filter

Description:

Disabel MAC address filter function

Syntax:

no mac-address-table filter <A:B:C:D:E:F>

Parameters:

A:B:C:D:E:F :MAC address xx:xx:xx:xx:xx:xx

Example:

Disabel MAC address filter function:

```
WGSW-28040(config)# no mac-address-table filter 00:30:4f:11:22:33
WGSW-28040(config)#
```

No LACP

Description:

Disabel LACP function

Syntax:

no lacp

Example:

Disabel LACP function:

```
WGSW-28040(config)# no lacp
WGSW-28040(config)#
```

No Mirror

Description:

Disabel port mirror function

Syntax:

no mirror

Example:

Disabel port mirror function:

```
WGSW-28040(config)# no mirror
WGSW-28040(config)#
```

No Port Flow Control

Description:

Disabel flow control function

Syntax:

no port <port-list> flow-control

Parameters:

<port_list>: Port list or 'all'

Example:

Disabel flow control function:

```
WGSW-28040(config)# no port 1 flow-control
WGSW-28040(config)#
```

No Port Security

Description:

Disabel port security function

Syntax:

no port-security port <port-list> address-limit

Parameters:

<port_list>: Port list or 'all'

Example:

Disabel port security function:

```
WGSW-28040(config)# no port-security port 1 address-limit
WGSW-28040(config)#
```

No Protected Port

Description:

Disabel protected port function

Syntax:

no protected-ports port <port-list>

Parameters:

<port_list>: Port list or 'all'

Example:

Disabel protected port function:

```
WGSW-28040(config)# no protected-ports port 1
WGSW-28040(config)#
```

No QoS

Description:

Disabel QoS function

Syntax:

no qos remark port <port-list> <1p|dscp>

Parameters:

<port_list>: Port list or 'all'

1p: 802.1p

dscp: DCSP'

Example:

Disabel protected port function:

```
WGSW-28040(config)# no protected-ports port 1
WGSW-28040(config)#
```

No SNMP Community

Description:

Delete SNMP community function

Syntax:

no snmp community <name>

Parameters:

<name>: community name

Example:

Delete SNMP community function:

```
WGSW-28040(config)# no snmp community public
WGSW-28040(config)#
```

No SNMP Host

Description:

Delete SNMP host function

Syntax:

no snmp host <A.B.C.D>

Parameters:

<A.B.C.D>: IP Address format is A.B.C.D where (A/B/C/D = 0 ~ 254)

Example:

Delete SNMP host function:

```
WGSW-28040(config)# no snmp host 192.168.0.20
WGSW-28040(config)#
```

No Storm Control

Description:

Disable storm control function

Syntax:

no storm-control [<port_list>] [broadcast|multicast|unknown-unicast|unknown-multicast]

Parameters:

<port_list>: Port list or 'all'

broadcast :Broadcast storm control

multicast :Multicast storm control

unknown-unicast :Unknown-unicast storm control

unknown-multicast :Unknown-multicast storm control

Example:

Disable storm control function:

```
WGSW-28040(config)# no storm-control port 1 broadcast
WGSW-28040(config)#
```

No Spanning Tree

Description:

Disable spanning tree function

Syntax:

no spanning-tree [<force-version>] [<hello-time>] [<max-hops>] [<forward-delay >] [<maximum-age>] [<tx-hold-count>] [<port>] [port_list] [<mst>] [<config-name>] [<config-revision>]

Parameters:

force-version :Sets the force-protocol-version parameter

hello-time :Sets the hello-time parameter

max-hops :Sets the max-hops parameter

forward-delay :Sets the forward-delay parameter

maximum-age :Sets the maximum-age parameter

tx-hold-count :Sets the tx-hold-count parameter

port :Port configuration

mst :MST config

config-name :Sets the bridge name

config-revision :All ports

Example:

Disable spanning tree function:

```
WGSW-28040(config)# no spanning-tree force-version
WGSW-28040(config)#
```

No SVLAN

Description:

Delete SVLAN function

Syntax:

no svlan [<port>] [port_list] [<S-VLAN ID>]

Parameters:

<port> : port configuration

port_list : Port list or 'all'

<S-VLAN ID> : SVLAN ID

Example:

Delete SVLAN function:

```
WGSW-28040(config)# no svlan 1
WGSW-28040(config)#
```

No Jumbo Frame

Description:

Disable jumbo frame function

Syntax:

no jumbo-frame

Example:

Disable jumbo frame function:

```
WGSW-28040(config)# no jumbo-frame
WGSW-28040(config)#
```

No IP

Description:

Disable IP configuration

Syntax:

no ip <dhcp|default-gateway>

Parameters:

dhcp : DHCP client

default-gateway : Remove default gateway address

Example:

Disable DHCP function:

```
WGSW-28040(config)# no ip dhcp
WGSW-28040(config)#
```

No SNTP

Description:

Disable Simple Network Time Protocol configuration

Syntax:

no sntp

Example:

Disable Simple Network Time Protocol configuration:

```
WGSW-28040(config)# no sntp
WGSW-28040(config)#
```

No Username

Description:

Disable local user

Syntax:

no username <name>

Parameters:

<name> : Local user name

Example:

Disable local user:

```
WGSW-28040(config)# no username 12345
WGSW-28040(config)#
```

No Enable

Description:

Disable local enable password

Syntax:

no enable

Example:

Disable local enable password:

```
WGSW-28040(config)# no enable
WGSW-28040(config)#
```

No Telnet

Description:

Disable Telent daemon configuration

Syntax:

no telnet

Example:

Disable Telent daemon configuration:

```
WGSW-28040(config)# no telnet
WGSW-28040(config)#
```

No IPv6 Auto-configuration

Description:

Disable IPv6 Auto-configuration

Syntax:

no ipv6 auto-configuration

Example:

Disable IPv6 Auto-configuration:

```
WGSW-28040(config)# no ipv6 auto-configuration
WGSW-28040(config)#
```

No Log

Description:

Delete log configuration

Syntax:

no log [<server>] [server_index] [<flash|ram>]

Parameters:

<server> : Remote server, maximum 4 servers can be configured

Server_index :Remote server index (1-4)

flash : flash

ram : ram

Example:

Delete log configuration:

```
WGSW-28040(config)# no log ram
WGSW-28040(config)#
```

No Trunk

Description:

Delete trunk configuration

Syntax:

no trunk [trunk_group] [<port>] [port_list]

Parameters:

Trunk_group : Trunk group number (1-8)

port :port configuration

port_list : Port list or 'all'

Example:

Delete trunk configuration:

```
WGSW-28040(config)# no trunk 1
WGSW-28040(config)#
```

No VLAN

Description:

Delete VLAN configuration

Syntax:

no vlan [<ingress-filter|leaky|vid>]

Parameters:

Ingress-filter : Ingress filtering configuration

leaky : VLAN leaky configuration

vid : VLAN ID (1-4094)

Example:

Delete VLAN configuration:

```
WGSW-28040(config)# no vlan 2
WGSW-28040(config)#
```

No SSH

Description:

Delete SSH (Secure Shell) configuration

Syntax:

no ssh [v1|v2|all]

Parameters:

v1 : SSH v1 host keys

v2 : SSH v2 host keys

all : Both SSH v1 and v2 host keys

Example:

Delete SSH configuration:

```
WGSW-28040(config)# no ssh v1
WGSW-28040(config)#
```

6.3.4 More Command

More

Description:

Show XMORE page on cli

Syntax:

more

Example:

Show XMORE page on cli:

```
WGSW-28040(config)# more
WGSW-28040(config)#
```

6.3.5 ACL Command

ACL

Description:

ACL configuration

Syntax:

acl <acl_index>

Parameters:

acl_index : ACL index (1-1600)

Example:

Set ACL index:

```
WGSW-28040(config)# acl 1
WGSW-28040(acl)#
```

ACL End

Description:

End current mode and change to enable mode

Syntax:

end

Example:

End current mode and change to enable mode:

```
WGSW-28040(acl)# end
WGSW-28040#
```

ACL Comment

Description:

ACL comment

Syntax:

comment <name>

Parameters:

<name> : comment name

Example:

Set ACL comment name:

```
WGSW-28040(acl)# comment test
```

```
WGSW-28040(acl)#
```

Remove ACL

Description:

Remove ACL configuration

Syntax:

no [<comment>] [<name>] [<ace>] [ace_index] [ace comment]

Parameters:

<comment> : ACL comment

<name> : ACL name

<ace> : ACE configuration

ace_index : ACE index (1-127)

ace_comment : ACE comment

Example:

Remove ACL configuration:

```
WGSW-28040(acl)# no ace 1 comment
WGSW-28040(acl)#
```

ACL Name

Description:

Configure ACL name

Syntax:

name [<name>]

Parameters:

<name> : ACL name

Example:

Configuration ACL name:

```
WGSW-28040(acl)# name deny_192.168.1.0
WGSW-28040(acl)#
```

ACE Field

Description:

Configure ACE field

Syntax:

Ace <ace_index> field [<src-mac>] [A:B:C:D:E:F] [<dst-mac>] [A:B:C:D:E:F] [<src-ip>] [A.B.C.D] [<dst-ip>] [A.B.C.D] [<ethertype>] [etype] [<ip-protocol>] [protocol] [<tos>] [tos_value] [<l4-src-port>] [sport] [<l4-dst-port>] [dport] [<tcp-flag>] [flag]

Parameters:

<ace_index> : ACE ID (1-127)

<vid> : VLAN ID (1-4094)

<src-mac> : Source MAC address

<dst-mac> : Destination MAC address

A:B:C:D:E:F :MAC address xx:xx:xx:xx:xx:xx

<src-ip> : Source IP address

<dst-ip> : Destination IP address

A.B.C.D : IP Address format is A.B.C.D where (A/B/C/D = 0 ~ 254)

<ethertype> : Ethernet type

etype : Ethernet type keyword

<ip-protocol> : IP protocol

protocol : IP protocol number

<tos> : ToS

tos_value : ToS value

<l4-src-port> : Source L4 port

Sport : Source UDP/TCP port range

<l4-dst-port> : Destination L4 port

dport : Destination UDP/TCP port range

<tcp-flags> : TCP flags

flag : flag value

Example:

Configuration ACE field:

```
WGSW-28040(acl)# ace 1 field ethertype 8100
WGSW-28040(acl)#
```

ACE Action

Description:

Configure ACE action

Syntax:

Ace <ace_index> action [permit|deny]

Parameters:

<ace_index> : ACE ID (1-127)

permit : Permit forwarding

deny : Deny forwarding

Example:

Configuration ACE action:

```
WGSW-28040(acl)# ace 1 action deny
WGSW-28040(acl)#
```

ACE Comment

Description:

Configure ACE commant

Syntax:

Ace <ace_index> comment [name]

Parameters:

<ace_index> : ACE ID (1-127)

name : ace comment name

Example:

Configuration ACE comment:

```
WGSW-28040(acl)# ace 1 comment test
WGSW-28040(acl)#
```

Show ACE

Description:

Show ACE information

Syntax:

Show ace [all|ace_index]

Parameters:

<ace_index> : ACE ID (1-127)

all : all ACE

Example:

Show ACE:

```
WGSW-28040(acl)# show ace 1
WGSW-28040(acl)#
```

6.3.6 Show Command

Show ACL

Description:

Show ACL configuration

Syntax:

Show acl <all|acl_index|acl_name>

Parameters:

all : all configuration

acl_index : ACL index (1-1600)

name : ACL name

Example:

Show ACL configuration:

```
WGSW-28040(config)# show acl 1
```

Show ACL Range

Description:

Show ACL range configuration

Syntax:

Show acl-range <all|acl_range >

Parameters:

all : all configuration

acl_range : 1-1000 Index 1-1000

1001-2000 Index 1001-2000

2001-3000 Index 2001-3000

3001-4000 Index 3001-4000

4001-5000 Index 4001-5000

5001-6000 Index 5001-6000

6001-7000 Index 6001-7000

7001-8000 Index 7001-8000

8001-9000 Index 8001-9000

9001-10000 Index 9001-10000

10001-11000 Index 10001-11000

11001-12000 Index 11001-12000

12001-13000 Index 12001-13000

13001-14000 Index 13001-14000

Example:

Show ACL range:

```
WGSW-28040(config)# show acl-range all
```

Show ACL Policy

Description:

Show ACL policy configuration

Syntax:

Show acl-policy <all|policy_index >

Parameters:

all : all configuration

policy_index : policy index (1-16)

Example:

Show ACL policy:

```
WGSW-28040(config)# show acl-policy all
```

Show ACL Template

Description:

Show ACL template configuration

Syntax:

Show acl-template <all|template_index >

Parameters:

all : all configuration

template_index : template index (1-16)

Example:

Show ACL template:

```
WGSW-28040(config)# show acl-template all
```

Show RADIUS Server

Description:

Show RADIUS server

Syntax:

Show radius-server

Example:

Show ACL template:

```
WGSW-28040(config)# show radius-server
```

Show Dot1x

Description:

Show dot1x information

Syntax:

Show dot1x [<port>] [port_list]

Parameters:

port :port configuration

port_list : Port list or 'all'

Example:

Show Dot1x:

```
WGSW-28040(config)# show dot1x
802.1x protocol: Disabled
802.1x reauthentication: Enabled
802.1x reauthentication period(sec.): 3600
WGSW-28040(config)#
```

Show IGMP Snooping

Description:

Show IGMP snooping configuration

Syntax:

Show igmp-snooping <router|table|groups|vlan|querier>

Parameters:

router : show multicast routers

table : show multicast table

groups : show IGMP groups

vlan : show VLAN configuration

querier : show Querier information

Example:

Show IGMP snooping router:

```
WGSW-28040(config)# show igmp-snooping router
  VID   |   Port   |      Expiry Time (Sec)
-----------+-----------+-------------------------------
WGSW-28040(config)#
```

Show MAC Address Table

Description:

Show MAC address table configuration

Syntax:

Show mac-address-table [<static>] [<filter>] [<multicast>] [<A:B:C:D:E:F>] [<port>] [<port_list>] [<vlan>] [vid]

Parameters:

<statics> : Static unicast and multicast entries

<filter> : MAC address filter configuration

<multicast> : Static multicast entries

A:B:C:D:E:F :MAC address xx:xx:xx:xx:xx:xx

<port> : Port configuration

port_list : Port list or 'all'

<vid> : VLAN ID (1-4094)

Example:

Show IGMP snooping router:

```
WGSW-28040(config)# show igmp-snooping router
  VID   |   Port   |      Expiry Time (Sec)
-----------+-----------+--------------------------------
WGSW-28040(config)#
```

Show LACP

Description:

Show LACP configuration

Syntax:

Show lacp

Example:

Show LACP configuration:

```
WGSW-28040(config)# show lacp
LACP is Disabled
System Priority: 32768
WGSW-28040(config)#
```

Show Mirror

Description:

Show mirror configuration

Syntax:

Show mirror

Example:

Show mirror configuration:

```
WGSW-28040(config)# show mirror
Destination port : Not Config
Source RX Port    :
Source TX Port    :
WGSW-28040(config)#
```

Show Port Security

Description:

Show port security configuration

Syntax:

Show port-security <port> <port_list>

Parameters:

<port> : Port configuration

port_list : Port list or 'all'

Example:

Show port security configuration:

```
WGSW-28040(config)# show port-security port 1
  Port   |       Security        |   Action
---------+-----------------------+----------
     1   |   Disabled            |   ---
WGSW-28040(config)#
```

Show Port

Description:

Show port configuration

Syntax:

Show port <port_list>

Parameters:

port_list : Port list or 'all'

Example:

Show port configuration:

```
WGSW-28040(config)# show port 1
            Port Number : 1
       Port Description :
```

```
                Admin State : Enabled
                Link Status : Down
                      Speed : Auto
                     Duplex : Auto
          Flow Control Admin : Disabled
        Flow Control Status : Off
              Protected Port : No
            Trunk Port Role : Normal Port
WGSW-28040(config)#
```

Show Protected Ports

Description:

Show protected port configuration

Syntax:

Show protected-ports

Example:

Show protected port configuration:

```
WGSW-28040(config)# show protected-ports
Protected-ports     :
Unprotected-ports : all
WGSW-28040(config)#
```

Show QoS Remark

Description:

Show QoS remarking ability configuration

Syntax:

Show qos remark <port> [<port_list>] <1p|dscp>

Parameters:

Port : Port configuration

<port_list> : Port list or 'all'

1p : 802.1p

Dscp : DiffServ Code Point

Example:

Show QoS remark configuration:

```
WGSW-28040(config)# show qos remark port 1 1p
Port      802.1p Remark Ability
```

```
================================================

 1          Disabled
WGSW-28040(config)#
```

Show QoS Remarking Table

Description:

Show QoS remarking table configuration

Syntax:

Show qos remarking-table <1p|dscp>

Parameters:

1p : 802.1p

Dscp : DiffServ Code Point

Example:

Show QoS remarking table configuration:

```
WGSW-28040(config)# show qos remarking-table 1p
QoS 802.1p Remarking Table


CoS      New Priority
-------------------------------
  0          1
  1          0
  2          2
  3          3
  4          4
  5          5
  6          6
  7          7
WGSW-28040(config)#
```

Show QoS Map

Description:

Show QoS remap configuration

Syntax:

Show qos map <dscp-cos|1p-cos|port-cos|cos-queue>

Parameters:

dscp-cos :dscp to cos

1p-cos :802.1p to cos

port-cos :Port-based priority

cos-queue :Cos to queue id

Example:

Show QoS remap configuration:

```
WGSW-28040(config)# show qos map 1
    QoS - 802.1p/CoS Mapping Table
    ==============================


802.1p Priority                CoS
-------------------------------------------------------
0                              1
1                              0
2                              2
3                              3
4                              4
5                              5
6                              6
7                              7
WGSW-28040(config)#
```

Show QoS Priority Selection

Description:

Show QoS priority selection configuration

Syntax:

Show qos priority selection

Example:

Show QoS priority selection configuration:

```
WGSW-28040(config)# show qos priority-selection


Priority Type                  Weight
-------------------------------------------------------
```

```
Port-based                      1
Classifier-based                1
ACL-based                       1
DSCP-based                      1
WGSW-28040(config)#
```

Show QoS Number of Queue

Description:

Show QoS number of queue configuration

Syntax:

Show qos queue-number

Example:

Show QoS number of queue configuration:

```
WGSW-28040(config)# show qos queue-number
Number Of Queue: 8
WGSW-28040(config)#
```

Show QoS Queue Weight

Description:

Show QoS queue weight configuration

Syntax:

Show qos queue-weight port <port_list>

Parameters:

<port_list> : Port list or 'all'

Example:

Show QoS queue weight configuration:

```
WGSW-28040(config)# show qos queue-weight port 1
  Port   | Queue-ID | Queue-Weight
-----------+----------+---------------
   1         1         1
   1         2         2
   1         3         3
   1         4         4
   1         5         5
   1         6         6
```

```
  1          7          7
  1          8          8
WGSW-28040(config)#
```

Show QoS Scheduling Algorithm

Description:

Show QoS scheduling algorithm configuration

Syntax:

Show qos scheduling algorithm port <port_list>

Parameters:

<port_list> : Port list or 'all'

Example:

Show QoS scheduling algorithm configuration:

```
WGSW-28040(config)# show qos scheduling-algorithm port 1

                    Scheduling Algorithm Information
                    ================================


  Port   |            Algorithm
------------+-----------------------------------------
   1                 weighted-fair-queue
WGSW-28040(config)#
```

Show SNMP

Description:

Show SNMP configuration

Syntax:

Show snmp

Example:

Show SNMP configuration:

```
WGSW-28040(config)# show snmp
SNMP is disabled.
system name        = WGSW-28040
system location = Default Location
system contact    = Default Contact
Community Name                Access Right
```

```
------------------------------------------------------------
public                          read-only
private                         read-write

Total Community Entries: 2

IP Address              Community Name
------------------------------------------------------------

Total Trap Entries: 0
WGSW-28040(config)#
```

Show Storm Control

Description:

Show storm control configuration

Syntax:

Show storm-control port <port_list>

Parameters:

<port_list> : Port list or 'all'

Example:

Show storm control configuration:

```
WGSW-28040(config)# show storm-control port 1

  Port   | Broadcast | Multicast | Unknown-Unicast | Unkonwn-Multicast
         |    (pps)  |    (pps)  |       (pps)     |         (pps)
-----------+-----------+-----------+-----------------+-----------------
     1          Off         Off             Off                 Off
WGSW-28040(config)#
```

Show Spanning Tree

Description:

Show spanning tree configuration

Syntax:

Show spanning-tree [<port>] [port_list] [<mst>] [mst_id]

Parameters:

Port : port configuration

<port_list> : Port list or 'all'

Mst : instance configruation

<mst_id> : instance ID (0~15)

Example:

Show spanning tree configuration:

```
WGSW-28040(config)# show spanning-tree port 1


 STP Port Information
==================================================


  Port Identifier : 0x8001 (128/ 1)
--------------------------------------------------
  External Path Cost : 0            /0
               Edge Port : Auto /Yes
           BPDU Filter : False
            BPDU Guard : False
  Point-to-Point MAC : Auto /Yes
--------------------------------------------------
   Pkts Counters : Rx:0/0/0   Tx:0/0/0
--------------------------------------------------
WGSW-28040(config)#
```

Show SVLAN

Description:

Show SVLAN configuration

Syntax:

Show svlan [<port>] [port_list] <pvid|service-port> [<table>] [svid]

Parameters:

Port : port configuration

<port_list> : Port list or 'all'

Pvid : pvid

Service-port : NNI Port Setting

<table> : table list

Svid :svid

Example:

Show SVLAN configuration:

```
WGSW-28040(config)# show svlan table
 SVLAN ID    | Member Port
-----------------+-----------------------------------------------------
WGSW-28040(config)#
```

Show Jumbo Frame

Description:

Show jumbo frame size

Syntax:

Show jumbo-frame

Example:

Show jumbo frame:

```
WGSW-28040(config)# show jumbo-frame
Jumbo frame size is 1522 Bytes
WGSW-28040(config)#
```

Show Info

Description:

Show basic information

Syntax:

Show info

Example:

Show basic information:

```
WGSW-28040(config)# show info
MAC Address          : 00:30:4F:88:88:88
IP Address           : 192.168.0.100
Subnet Mask          : 255.255.255.0
Loader Version       : 1.3.0
Loader Date          : Feb 10 2011 - 02:04:21
Firmware Version : 1.0
Firmware Date        : Thu Apr 14 14:19:30 CST 2011
System Object ID : 1.3.6.1.4.1.10456.1.1509
WGSW-28040(config)#
```

Show IP

Description:

Show IP information

Syntax:

Show ip [<dhcp>]

Parameters:

dhcp : dhcp configuration

Example:

Show IP information:

```
WGSW-28040(config)# show ip
IP Address: 192.168.0.100
Subnet Netmask: 255.255.255.0
Default Gateway: 0.0.0.0
IPv6 Address: fe80::230:4fff:fe88:8888/64
IPv6 Router: ::
WGSW-28040(config)#
```

Show ARP

Description:

Show the IP ARP translation table

Syntax:

Show arp

Example:

Show the IP ARP translation table:

```
WGSW-28040(config)# show arp
WGSW-28040(config)#
```

Show Time

Description:

Show time configuration

Syntax:

Show time

Example:

Show time configuration:

```
WGSW-28040(config)# show time
Time Zone: UTC+0000
2000-01-01 (Sat.) 00:02:23 UTC+0000
WGSW-28040(config)#
```

Show SNTP

Description:

Show the status of SNTP

Syntax:

Show sntp

Example:

Show the status of SNTP:

```
WGSW-28040(config)# show sntp
SNTP: Disabled
SNTP Server: 0.0.0.0
SNTP Port: 123
WGSW-28040(config)#
```

Show Startup Configuration

Description:

Show the startup configurations

Syntax:

Show startup-config

Example:

Show the startup configurations:

```
WGSW-28040(config)# show startup-config
```

Show SNTP

Description:

Show the running configurations

Syntax:

Show running-config

Example:

Show the running configurations:

```
WGSW-28040(config)# show running-config
```

Show Username

Description:

Show the local user

Syntax:

Show username

Example:

Show the local user:

```
WGSW-28040(config)# show username
 Priv   |   Type   |              User Name                |              Password
-------+--------+---------------------------------------------------+--------------------------------
 admin | secret |                admin                  | b4lXeu1GE2FGo
WGSW-28040(config)#
```

Show Privilege

Description:

Show the local user privilege level

Syntax:

Show privilege

Example:

Show the local user privilege level:

```
WGSW-28040(config)# show privilege
Current CLI Username:   admin
Current CLI Privilege: Admin
WGSW-28040(config)#
```

Show Telnet

Description:

Show the telent daemon configuration

Syntax:

Show telnet

Example:

Show the Telent daemon configuration:

```
WGSW-28040(config)# show telnet
Telnet daemon : enabled
WGSW-28040(config)#
```

Show IPv6

Description:

Show IPv6 information

Syntax:

Show ipv6

Example:

Show IPv6 information:

```
WGSW-28040(config)# show ipv6
IPv6 Auto Configuration: Enabled
IPv6 in use Address: fe80::230:4fff:fe88:8888/64
IPv6 in use Router: ::
IPv6 static Address: ::/1
IPv6 static Router: 0:1:0:1:0:1:0:1
WGSW-28040(config)#
```

Show Log

Description:

Show log information

Syntax:

Show log <flash|ram|target-info|cat-sev-table>

Parameters:

flash :log of Flash

ram :log of RAM

target-info :log table

cat-sev-table : category and severity

Example:

Show log information:

```
WGSW-28040(config)# show log flash

                    Log messages in FLASH
```

```
 NO.| Severity | Category |     Timestamp       |   Message
--------------------+------------+-------------------------+--------------------------------------
WGSW-28040(config)#
```

Show TFTP Server

Description:

Show TFTP server configurations

Syntax:

Show tftp-server

Example:

Show log information:

```
WGSW-28040(config)# show tftp-server
 FILE TYPE |     IP Address       | Remote File Name
-----------+-----------------+----------------------
  firmware |     192.168.1.111     | vmlinux.bix
     config   |     192.168.1.111    | startup-config.cfg
WGSW-28040(config)#
```

Show Trunk

Description:

Show trunk configurations

Syntax:

Show trunk

Example:

Show trunk configurations:

```
WGSW-28040(config)# show trunk
No trunk entry created.
WGSW-28040(config)#
```

Show VLAN Port

Description:

Show VLAN port configurations

Syntax:

Show vlan port <port_list> [<mode|pvid|accept-frame-type>]

Parameters:

<port_list> :Port list or 'all'

mode :Display the current VLAN mode

pvid :Port configured VLAN ID

accept-frame-type :VLAN accept frame type

Example:

Show VLAN port configurations:

```
WGSW-28040(config)# show vlan port 1 mode
   Port | Mode
----------+-------------
1         | Original
WGSW-28040(config)#
```

Show VLAN Ingress Filter

Description:

Show VLAN ingress filtering configurations

Syntax:

show vlan ingress-filter

Example:

Show VLAN ingress filtering configurations:

```
WGSW-28040(config)# show vlan ingress-filter
 VLAN Ingress Filtering: Enabled
WGSW-28040(config)#
```

Show VLAN Leaky

Description:

Show VLAN leaky configurations

Syntax:

show vlan leaky

Example:

Show VLAN leaky configurations:

```
WGSW-28040(config)# show vlan leaky
 VLAN Leaky: Disabled
WGSW-28040(config)#
```

Show VLAN

Description:

Show VLAN ID

Syntax:

show vlan <vid>

Parameters:

vid :Port configured VLAN ID

Example:

Show VLAN leaky configurations:

```
WGSW-28040(config)# show vlan 1
 VLAN ID    : 1
 VLAN Name : default

   Port   |  Member
---------+----------
01         |  Untagged
02         |  Untagged
03         |  Untagged
04         |  Untagged
05         |  Untagged
06         |  Untagged
07         |  Untagged
08         |  Untagged
09         |  Untagged
10         |  Untagged
11         |  Untagged
12         |  Untagged
13         |  Untagged
14         |  Untagged
15         |  Untagged
16         |  Untagged

--More--
17         |  Untagged
18         |  Untagged
19         |  Untagged
20         |  Untagged
21         |  Untagged
22         |  Untagged
```

```
23        |  Untagged
24        |  Untagged
25        |  Untagged
26        |  Untagged
27        |  Untagged
28        |  Untagged
WGSW-28040(config)#
```

Show SSH

Description:

Show SSH configurations

Syntax:

show ssh

Example:

Show ssh configurations:

```
WGSW-28040(config)# show ssh
SSH daemon : enabled
WGSW-28040(config)#
```

Show PoE Info

Description:

Display PoE Infomation

Syntax:

show poe info

Example:

Show PoE information:

```
WGSW-28040(config)# show poe info
System PoE Admin Mode          : Enable
Power Limit Mode               : Consumption
PoE Temperature Unit 1         : 27(C) / 80(F)
PoE Temperature Unit 2         : 27(C) / 80(F)
Maximum Available Power        : 180 Watt
PoE Power Consumption          : 0.0 Watt
WGSW-28040(config)#
```

Show PoE Status

Description:

Show per PoE port information

Syntax:

show poe status <port_list>

Parameters:

<port_list> :Port list or 'all'

Example:

Show PoE status of port 1:

```
WGSW-28040(config)# show poe status 1
Port | PoE Function | Class | Current[mA] | Consumption[W]
------+--------------------+---------+-------------------+----------------
   1  |      Enable   |  ---  |           0     |           0
--------------------------------------------------------------------------------
WGSW-28040(config)#
```

6.3.7 ACL Range Command

ACL Range

Description:

ACL range configuration

Syntax:

acl-range <index_range> template <template_index>

Parameters:

Index_range : 1-1000 Index 1-1000
1001-2000 Index 1001-2000
2001-3000 Index 2001-3000
3001-4000 Index 3001-4000
4001-5000 Index 4001-5000
5001-6000 Index 5001-6000
6001-7000 Index 6001-7000
7001-8000 Index 7001-8000
8001-9000 Index 8001-9000
9001-10000 Index 9001-10000
10001-11000 Index 10001-11000
11001-12000 Index 11001-12000
12001-13000 Index 12001-13000

13001-14000 Index 13001-14000

14001-15000 Index 14001-15000

15001-16000 Index 15001-16000

template_index : template index (1-16)

Example:

To set ACL range:

```
WGSW-28040(config)# acl-range 6001-7000 template 5
```

6.3.8 ACL Policy Command

ACL Policy

Description:

ACL policy configuration

Syntax:

acl-policy <policy_index> <action|vlan|port> [<vid|port_list>] <mirror|priority|rate-limit>

Parameters:

policy_index : policy index (1-16)

action : action configuration

vlan : VLAN configuration

port : port configuration

vid : vid

port_list : Port list or 'all'

mirror : mirror packet

priority : modify priority

rate-limit : rate limit

Example:

To set ACL policy:

```
WGSW-28040(config)# acl-policy 1 action mirror 1
```

6.3.9 ACL Template Command

ACL Template

Description:

ACL template configuration

Syntax:

acl-template <template_index> field

<src-mac|dst-mac|ethertype|src-ip|dst-ip|ip-protocol|tos|l4-src-port|l4-dst-port|tcp-flag>

Parameters:

template_index : template index (1-16)

src-mac : source MAC

dst-mac : destination MAC

ethertype : ethernet type

src-ip : source IP

dst-ip : destination IP

ip-protocol : IP protocol

tos : Type of Service

l4-src-port : L4 source port

l4-dst-port : L4 destination port

tcp-flag : TCP flag

Example:

To set ACL template:

```
WGSW-28040(config)# acl-template 1 field src-mac
```

6.3.10 Dot1x Command

Dot1x Reauthentication

Description:

Set Re-authentication function

Syntax:

dot1x reauth

Example:

To set reauthentication function:

```
WGSW-28040(config)# dot1x reauth
```

Dot1x Reauthentication Period

Description:

Set dot1x re-authentication period

Syntax:

dot1x reauthperiod <re-auth_period>

Parameters:

Re-auth_period : 30~65535, (default: 3600 seconds)

Example:

To set dot1x re-authentication period:

```
WGSW-28040(config)# dot1x reauthperiod 30
```

Dot1x Port

Description:

Set dot1x port configuration

Syntax:

dot1x port <port_list> <admin-status|control> <enable|disable|authorized|unauthorized>

Parameters:

port_list : Port list or 'all'

admin-status : Administration status

control : Port authentication control

enable : Enable authorization

disable : Disable authorization

authorized : Force authorized

unauthorized : Force unauthorized

Example:

To set dot1x port configuration:

```
WGSW-28040(config)# dot1x port 1 admin-status enable
```

6.3.11 RADIUS Server Command

RADIUS Host Server

Description:

Set IP address of the remote radius server host

Syntax:

radius-server host <A.B.C.D> auth-port <port_number>

Parameters:

A.B.C.D : IP Address format is A.B.C.D where (A/B/C/D = 0 ~ 254)

Port_number : 0~65535

Example:

To set IP address of the remote radius server host:

```
WGSW-28040(config)# radius-server host 192.168.0.20 auth-port 1812
```

RADIUS Key

Description:

Set shared key

Syntax:

radius-server key <shared_key>

Parameters:

Shared_key : Shared key (maximum 30 characters)

Example:

To set shared key:

```
WGSW-28040(config)# radius-server key 12345678
```

6.3.12 IGMP Snooping Command

IGMP Snooping Fastleave

Description:

Enable IGMP snooping fastleave

Syntax:

igmp-snooping fastleave

Example:

Enable IGMP snooping fastleave:

```
WGSW-28040(config)# igmp-snooping fastleave
```

IGMP Snooping Router Timeout

Description:

Set IGMP snooping router timeout

Syntax:

igmp-snooping router-timeout <timeout>

Parameters:

timeout : Valid timeout range is 1-600 Sec. Default is 125 Sec.

Example:

To set IGMP snooping router timeout:

```
WGSW-28040(config)# igmp-snooping router-timeout 20
```

IGMP Snooping Robustness Variable

Description:

Set IGMP snooping Robustness Variable

Syntax:

igmp-snooping robustness-variable <rnage>

Parameters:

range : Valid range is 1-255. Default is 2.

Example:

To set IGMP snooping Robustness Variable:

```
WGSW-28040(config)# igmp-snooping robustness-variable 20
```

IGMP Snooping Response Time

Description:

Set IGMP snooping response time

Syntax:

igmp-snooping response-time <time_sec>

Parameters:

Time_sec : Valid range is 10-25 Sec. Default is 10 Sec.

Example:

To set IGMP snooping response time:

```
WGSW-28040(config)# igmp-snooping response time 20
```

IGMP Snooping Query Interval

Description:

Set IGMP snooping query interval

Syntax:

igmp-snooping query-interval <time_sec>

Parameters:

time_sec : Valid range is 1-600 Sec. Default is 125 Sec.

Example:

To set IGMP snooping query interval:

```
WGSW-28040(config)# igmp-snooping query-interval 20
```

IGMP Snooping Last Member Query Interval

Description:

Set IGMP snooping last member query interval

Syntax:

igmp-snooping last-member-query-interval <time_sec>

Parameters:

time_sec : Valid range is 1-25 Sec. Default is 1 Sec.

Example:

To set IGMP snooping last member query interval:

```
WGSW-28040(config)# igmp-snooping last-member-query-interval 20
```

IGMP Snooping VLAN

Description:

Set IGMP snooping VLAN configuration

Syntax:

igmp-snooping vlan <vid>

Parameters:

vid : vid.

Example:

To set IGMP snooping VLAN:

```
WGSW-28040(config)# igmp-snooping vlan 1
```

IGMP Snooping Querier

Description:

Set IGMP snooping querier

Syntax:

igmp-snooping querier

Example:

To set IGMP snooping querier:

```
WGSW-28040(config)# igmp-snooping querier
```

6.3.13 Clear Command

Clear IGMP Snooping

Description:

Clear IGMP snooping

Syntax:

clear igmp-snooping <group|statistics>

Example:

Clear IGMP snooping:

```
WGSW-28040(config)# clear igmp-snooping statistics
```

Clear MAC Address Table

Description:

Clear MAC address table

Syntax:

clear mac-address-table <port|vlan> <port_list|vid>

Parameters:

port : port configuration

vlan : VLAN configuratio

port_list : Port list or 'all'

vid : vid.

Example:

Clear MAC address table:

```
WGSW-28040(config)# clear mac-address-table vlan 1
```

Clear Port Statistics

Description:

Clear port statistics

Syntax:

clear port <port_list> statistics

Parameters:

port_list : Port list or 'all'

Example:

Clear port statistics:

```
WGSW-28040(config)# clear port 1 statistics
```

Clear ARP

Description:

Clear entries in the ARP cache

Syntax:

clear arp <A.B.C.D>

Parameters:

A.B.C.D : IP Address format is A.B.C.D where (A/B/C/D = 0 ~ 254)

Example:

Clear entries in the ARP cache:

```
WGSW-28040(config)# clear arp 192.168.0.21
```

Clear Log

Description:

Clear log configuration

Syntax:

clear log <flash|ram>

Parameters:

flash :log from flash

ram :log from RAM

Example:

Clear log configuration:

```
WGSW-28040(config)# clear log ram
```

6.3.14 MAC Address Table Command

Static MAC Address Table

Description:

Set static MAC address

Syntax:

Mac-address-table static <A:B:C:D:E:F> vlan <vid> port <port_list>

Parameters:

A:B:C:D:E:F :MAC address xx:xx:xx:xx:xx:xx

Vid :vid

port_list : Port list or 'all'

Example:

To set static MAC address:

```
WGSW-28040(config)# mac-address-table static 00:30:4F:11:22:33 vlan 1 port 1
```

MAC Address Table Filter

Description:

Set MAC addressf ilter

Syntax:

Mac-address-table filter <source|destination|both> <A:B:C:D:E:F> vlan <vid> <name>

Parameters:

source : Source MAC address filter

destination : Destination MAC address filter

both : Source and Destination MAC address filter

A:B:C:D:E:F :MAC address xx:xx:xx:xx:xx:xx

Vid :vid

name : Entry name, maximum 32 characters

Example:

To MAC address filter:

```
WGSW-28040(config)# mac-address-table filter both 00:30:4f:11:22:33 vlan 1 123
```

6.3.15 LACP Command

LACP Port

Description:

Set LACP port configuration

Syntax:

lacp port <port_list> <active|passive>

Parameters:

port_list : Port list or 'all'

active :LACP active

passive :LACP passive

Example:

To set LACP port configuration:

```
WGSW-28040(config)# lacp port 1 active
```

LACP System Priority

Description:

Set LACP system priority

Syntax:

lacp system-priority <priority>

Parameters:

priority : Valid range is 0-65535. Default is 32768.

Example:

To set LACP system priority:

```
WGSW-28040(config)# lacp system-priority 32768
```

6.3.16 Trunk Command

Trunk Group

Description:

Set trunk configuration

Syntax:

Trunk <trunk_group> port <port_list> <lacp|static>

Parameters:

trunk_group : trunk group member (1-8)

port_list : Port list or 'all'

lacp : LACP trunk group

static : static trunk, disable LACP for this trunk group

Example:

To set trunk configuration:

```
WGSW-28040(config)# trunk 1 port 1-4 lacp
```

6.3.17 Mirror Command

Mirror Source

Description:

Set mirroring source configuration

Syntax:

Mirror source port <port_list> <both|rx|tx>

Parameters:

port_list : Port list or 'all'

both : tx & rx

tx : tx only

rx : rx only

Example:

To set mirroring source configuration:

```
WGSW-28040(config)# mirror source port 1 both
```

Mirror Destination

Description:

Set mirroring destination configuration

Syntax:

Mirror destination port <port_list>

Parameters:

port_list : Port list or 'all'

Example:

To set mirroring destination configuration:

```
WGSW-28040(config)# mirror destination port 2
```

6.3.18 Port Command

Port State

Description:

Set port forwarding state

Syntax:

port <port_list> <enable|disable>

Parameters:

port_list : Port list or 'all'

enable : enable port forwarding

disable : disable port forwarding

Example:

To set port forwarding state:

```
WGSW-28040(config)# port 1 state enable
```

Port Speed

Description:

Set port speed operation

Syntax:

port <port_list> speed [<10|100|1000|auto>] [<10|100|1000|10/100>]

Parameters:

port_list : Port list or 'all'

10 : 10Mbps

100 : 100Mbps

1000 : 1000Mbps

auto : Enable AUTO speed configuration

10 : 10Mbps

100 : 100Mbps

1000 : 1000Mbps

10/100 : 10Mbps and 100Mbps

Example:

To set port speed operation:

```
WGSW-28040(config)# port 1 speed 10
```

Port Duplex

Description:

Set port duplex operation

Syntax:

port <port_list> duplex [<auto|full|half>]

Parameters:

port_list : Port list or 'all'

auto : Enable AUTO duplex configuration

full : Full Duplex

half : Half Duplex

Example:

To set port duplex operation:

```
WGSW-28040(config)# port 1 duplex auto
```

Port Flow Control

Description:

Set port flow control ability configuration

Syntax:

port <port_list> flow-control

Parameters:

port_list : Port list or 'all'

Example:

To set port flow control ability configuration:

```
WGSW-28040(config)# port 1 flow-control
```

Port Error Disable

Description:

Set error diable port configuration

Syntax:

port <port_list> errdisable <all|bpdu|loopbackup|udld>

Parameters:

port_list : Port list or 'all'

all : All reasons

bpdu : BPDU Guard

loopbackup : Loopback

udld : UDLD

Example:

To set error diable port configuration:

```
WGSW-28040(config)# port 1 errdisable recovery all
```

Port Description

Description:

Set port description configuration

Syntax:

port <port_list> description <name>

Parameters:

port_list : Port list or 'all'

name : Description string

Example:

To set port description configuration:

```
WGSW-28040(config)# port 1 description camera_1
```

6.3.19 Port Security Command

Port Security

Description:

Set port security configuration

Syntax:

Port-security <port_list> address-limit <limit_num>

Parameters:

port_list : Port list or 'all'

limit_num : number of limitation (1-16447)

Example:

To set port security configuration:

```
WGSW-28040(config)# port-security port 1 address-limit 1
```

6.3.20 Protected Ports Command

Protected Port

Description:

Prevents the selected ports from communicating with each other

Syntax:

protected-ports port <port_list>

Parameters:

port_list : Port list or 'all'

Example:

To set protected port configuration:

```
WGSW-28040(config)# protected-ports port 1
```

6.3.21 QoS Command

QoS Remark Port

Description:

Set remarking ability for port

Syntax:

qos remark port <port_list> <1p|dscp>

Parameters:

port_list : Port list or 'all'

1p : 802.1p

dscp : DiffServ Code Point

Example:

To set remarking ability for port:

```
WGSW-28040(config)# qos remark port 1 1p
```

QoS Remark CoS

Description:

Set remarking ability for CoS

Syntax:

qos remark <cos-1p|cos-dscp> <range1> to <range2>

Parameters:

cos-1p : CoS to 802.1p

cos-dscp : CoS to DSCP

range1 : range is 0-7

range2 : 802.1p range is 0-7, DSCP range is 0-63

Example:

To set remarking ability for QoS:

```
WGSW-28040(config)# qos remark cos-1p 0 to 1
```

QoS Map

Description:

Set QoS remap configuration

Syntax:

qos map <dscp-cos|1p-cos|port-cos|cos-queue> <range1|port_list> to <range2>

Parameters:

dscp-cos : DSCP to CoS

1p-cos : 802.1p to CoS

port-cos : Port-based priority

cos-queue: CoS to queue mapping

range1 : DSCP range is 0-63, 802.1p priority range is 0-7,

port_list : Port list or 'all'

range2 : CoS range is 0-7,

Example:

To set remarking ability for QoS:

```
WGSW-28040(config)# qos map cos-queue 1 2 1 1 1 1 1 1
```

QoS Priority Selection

Description:

Set QoS priority selection

Syntax:

qos priority-selection port-based <weight> classifier-based <weight > acl-based <weight> dscp-based <weight>

Parameters:

weight : range is 1-4

Example:

To set QoS priority selection:

```
WGSW-28040(config)# qos priority-selection port-based 1 classifier-based 1 acl-based 1
dscp-based 1
```

QoS Queue Number

Description:

Set QoS number of queue

Syntax:

qos queue-number <range>

Parameters:

range : range is 1-8

Example:

To set QoS number of queue:

```
WGSW-28040(config)# qos queue-number 1
```

QoS Queue Weight

Description:

Set QoS queue weight

Syntax:

qos queue-number port <port_list> <range>

Parameters:

port_list : Port list or 'all'

range : range is 1-8

Example:

To set QoS queue weight:

```
WGSW-28040(config)# qos queue-weight port 1 1 1 1 1 1 1 1
```

QoS Scheduling Algorithm

Description:

Set QoS scheduling algorithm

Syntax:

qos scheduling-algorithm port <port_list> <wrr|wfq>

Parameters:

port_list : Port list or 'all'

wrr : weighted round robin

wfq : weighted fair queue

Example:

To set QoS scheduling algorithm:

```
WGSW-28040(config)# qos scheduling-algorithm port 1 wrr
```

6.3.22 SNMP Command

SNMP Community

Description:

Set community string configuration

Syntax:

snmp community <name> <ro|rw>

Parameters:

name : Community name (length 1~16)

ro : Read all objects only

rw : Read write all objects

Example:

To set community string configuration:

```
WGSW-28040(config)# snmp community public rw
```

SNMP Host

Description:

Set trap receiver IP address

Syntax:

snmp host <A.B.C.D> <name>

Parameters:

A.B.C.D : IP Address format is A.B.C.D where (A/B/C/D = 0 ~ 254)

name : Community name (length 1~16)

Example:

To set trap receiver IP address:

```
WGSW-28040(config)# snmp host 192.168.0.99 public
```

6.3.23 Storm Control Command

Storm Control

Description:

Set storm control configuration

Syntax:

storm-control port <port_list> <broadcast|multicast|unknown-unicast|unknown-multicast>

Parameters:

Port_list : Port list or 'all'

broadcast :Broadcast storm control

multicast :Multicast storm control

unknown-unicast :Unknown-unicast storm control

unknown-multicast :Unknown-multicast storm control

Example:

To set storm control configuration:

```
WGSW-28040(config)# storm-control port 1 unknown-multicast 100
```

6.3.24 Bandwidth Control Command

Port Bandwidth Control

Description:

Set port bandwidth control configuration

Syntax:

bandwidth-control port <port_list> <ingress|egress> <rate>

Parameters:

Port_list : Port list or 'all'

Ingress : Port effective ingress rate

egress : Port effective egress rate

rate : Rate (unit: Kbps), must be a multiple of 16 (0~1048544)

Example:

To set port bandwidth control configuration:

```
WGSW-28040(config)# bandwidth-control port 1 ingress 16
```

Ingress & Egress Bandwidth Control

Description:

Set ingress or egress bandwidth control configuration

Syntax:

bandwidth-control <ingress|egress> <include|exclude>

Parameters:

Ingress : Port effective ingress rate

egress : Port effective egress rate

include :Include preamble and IFG

exclude :Exclude preamble and IFG

Example:

To set ingress bandwidth control configuration:

```
WGSW-28040(config)# bandwidth-control ingress include
```

6.3.25 Spanning Tree Command

Force Version

Description:

Sets the force-protocol-version parameter

Syntax:

spanning-tree force-version <stp-compatible|rstp-operation|mstp-operation>

Parameters:

stp-compatible :Spanning-tree protocol compatible

rstp-operation :Rapid spanning-tree protocol (802.1w)

mstp-operation :Multiple spanning-tree protocol (802.1s)

Example:

To set the force-protocol-version parameter:

```
WGSW-28040(config)# spanning-tree force-version stp-compatible
```

Hello Time

Description:

Sets the hello-time parameter

Syntax:

spanning-tree hello-time <time>

Parameters:

time : specifies hello time of Spanning-tree (1-10 sec)

Example:

To set the hello-time parameter:

```
WGSW-28040(config)# spanning-tree hello-time 1
```

MAX Hops

Description:

Sets the max-hops parameter

Syntax:

spanning-tree max-hops <number>

Parameters:

number: hop number (1-40)

Example:

To set the max-hops parameter:

```
WGSW-28040(config)# spanning-tree max-hops 1
```

Forward Delay

Description:

Sets the forward-delay parameter

Syntax:

spanning-tree forward-delay <time>

Parameters:

time: Forward-delay interval (4-30 sec)

Example:

To set the forward-delay parameter:

```
WGSW-28040(config)# spanning-tree forward-delay 20
```

Maximum Age

Description:

Changes the interval between messages the spanning tree receives from the root switch

Syntax:

spanning-tree maximum-age <time>

Parameters:

time: Interval the switch waits between receiving BPDUs from the root switch (6-40 sec)

Example:

To set the maximum age parameter:

```
WGSW-28040(config)# spanning-tree maximum-age 20
```

Tx Hold Count

Description:

Set spanning-tree tx hold count, in seconds

Syntax:

spanning-tree tx-hold-count <time>

Parameters:

time: Specifies the tx hold count (1-10 sec)

Example:

To set the tx hold count:

```
WGSW-28040(config)# spanning-tree tx-hold-count 10
```

Path Cost

Description:

Sets the path cost for specified port

Syntax:

spanning-tree port <port_list> path-cost <cost>

Parameters:

Port_list : Port list or 'all'

Cost : The value of path cost (0~ 200000000, 0 = Auto)

Example:

To set the path cost:

```
WGSW-28040(config)# spanning-tree port 1 path-cost 2000
```

Edge Port

Description:

Sets the edge port for specified port

Syntax:

spanning-tree port <port_list> edge-port <enable|disable|auto>

Parameters:

Port_list : Port list or 'all'

enable :Force enable

disable :Force disable

auto :Auto mode

Example:

To set the edge port:

```
WGSW-28040(config)# spanning-tree port 1 edge-port enable
```

BPDU Filter

Description:

Sets the BPDU-Filter for specified port

Syntax:

spanning-tree port <port_list> bpdu-filter <enable|disable>

Parameters:

Port_list : Port list or 'all'

enable :Force enable

disable :Force disable

Example:

To set the BPDU filter:

```
WGSW-28040(config)# spanning-tree port 1 bpdu-filter enable
```

BPDU Guard

Description:

Sets the BPDU-Guard for specified port

Syntax:

spanning-tree port <port_list> bpdu-guard <enable|disable>

Parameters:

Port_list : Port list or 'all'

enable :Force enable

disable :Force disable

Example:

To set the BPDU guard:

```
WGSW-28040(config)# spanning-tree port 1 bpdu-guard enable
```

Point to Point MAC

Description:

Sets the point-to-point mac for specified port

Syntax:

spanning-tree port <port_list> point-to-point-mac <enable|disable|auto>

Parameters:

Port_list : Port list or 'all'

enable :Force enable

disable :Force disable

auto :Auto mode

Example:

To set the point-to-point mac:

```
WGSW-28040(config)# spanning-tree port 1 point-to-point-mac auto
```

Mcheck

Description:

Set the mcheck for specified port to migrate

Syntax:

spanning-tree port <port_list> mcheck

Parameters:

Port_list : Port list or 'all'

Example:

To set the mcheck:

```
WGSW-28040(config)# spanning-tree port 1 mcheck
```

MST Configuration Name

Description:

Set the MST configuration name

Syntax:

spanning-tree mst config-name <name>

Parameters:

name : Bridge name (Max.32 charactor)

Example:

To set the MST configuration name:

```
WGSW-28040(config)# spanning-tree mst config-name test
```

MST Configuration Revision

Description:

Sets the revision level

Syntax:

spanning-tree mst config-revision <level>

Parameters:

level : Revision level (0-65535)

Example:

To set the MST revision level:

```
WGSW-28040(config)# spanning-tree mst config-revision 100
```

MSTI VLAN

Description:

Add the MSTI-to-VLAN mapping

Syntax:

spanning-tree mst <msti> vlan <vid>

Parameters:

msti : Instance ID (0~15)

vid : vid

Example:

To add the MSTI-to-VLAN mapping:

```
WGSW-28040(config)# spanning-tree mst 1 vlan 1
```

MSTI Priority

Description:

Sets the priority for specified instance

Syntax:

spanning-tree mst <msti> priority <priority>

Parameters:

Msti : Instance ID (0~15)

priority : Priority (0~61440)

Example:

To add the priority for specified instance:

```
WGSW-28040(config)# spanning-tree mst 1 priority 0
```

MSTI Port Path Cost

Description:

Sets the path cost for specified instance

Syntax:

spanning-tree mst <msti> port <port_list> path-cost <cost>

Parameters:

Msti : Instance ID (0~15)

Port_list : Port list or 'all'

Cost : Path Cost (0~2000000)

Example:

To sets the path cost for specified instance:

```
WGSW-28040(config)# spanning-tree mst 1 port 1 path-cost 2000
```

MSTI Port Priority

Description:

Sets the priority for specified instance

Syntax:

spanning-tree mst <msti> port <port_list> priority <priority>

Parameters:

Msti : Instance ID (0~15)

Port_list : Port list or 'all'

priority : priority (0~240)

Example:

To sets the path cost for specified instance:

```
WGSW-28040(config)# spanning-tree mst 1 port 1 priority 1
```

6.3.26 SVLAN Command

TPID

Description:

Sets the TPID

Syntax:

svlan tpid <id>

Parameters:

ID :Tag-protocol-id (0x0000 ~ 0xFFFF)

Example:

To set the TPID:

```
WGSW-28040(config)# svlan tpid 0000
```

Port

Description:

Sets the SVLAN port

Syntax:

svlan port <port_list> <pvid|service-port> [<vid>]

Parameters:

Port_list : Port list or 'all'

pvid : Pvid

service-port : NNI Port Setting

vid :vid

Example:

To set the TPID:

```
WGSW-28040(config)# svlan tpid 0000
```

S-VLAN ID

Description:

Assign port for SVLAN

Syntax:

svlan <svlan_id> port <port_list>

Parameters:

Svlan_id : S-VLAN ID (1-4094)

Port_list : Port list or 'all'

Example:

To assign port for SVLAN:

```
WGSW-28040(config)# svlan 1 port 1
```

6.3.27 Jumbo Frame Command

Jumbo Frame

Description:

Sets the jumbo frame configuration

Syntax:

Jumbo-frame <frame_size>

Parameters:

Frame_size : 1522 1522 Bytes

1536 1536 Bytes

1552 1552 Bytes

9216 9216 Bytes

Example:

To set jumbo frame size:

```
WGSW-28040(config)# jumbo-frame 9216
```

6.3.28 System Command

System Name

Description:

Set host name

Syntax:

system name <name>

Parameters:

name : System name (length 1~256). If string has blank, use "" to quote it.

Example:

To set host name:

```
WGSW-28040(config)# system name test
```

System Location

Description:

Set host location

Syntax:

system location <name>

Parameters:

name : Location (length 1~256). If string has blank, use "" to quote it.

Example:

To set host name:

```
WGSW-28040(config)# system location 9F
```

System Contact

Description:

Set host contact

Syntax:

system contact <name>

Parameters:

name : System contact (length 1~256). If string has blank, use "" to quote it.

Example:

To set host name:

```
WGSW-28040(config)# system contact test
```

6.3.29 IP Command

DHCP

Description:

Enable DHCP client

Syntax:

ip dhcp

Example:

To enable DHCP client:

```
WGSW-28040(config)# ip dhcp
```

IP Address

Description:

Set IP address

Syntax:

ip address <ip_address> <subnet_mask>

Parameters:

Ip_address : IP Address format is A.B.C.D where (A/B/C/D = 0 ~ 254)

Subnet_mask : subnet mask format is A.B.C.D where (A/B/C/D = 0 ~ 255)

Example:

To set IP address:

```
WGSW-28040(config)# ip address 192.168.0.20 255.255.255.0
```

IP Default Gateway

Description:

Set IP default gateway

Syntax:

ip default-gateway <A.B.C.D>

Parameters:

A.B.C.D : IP default gateway format is A.B.C.D where (A/B/C/D = 0 ~ 254)

Example:

To set IP default-gateway:

```
WGSW-28040(config)# ip default-gateway 192.168.0.254
```

6.3.30 Ping Command

Ping

Description:

Send ICMP ECHO_REQUEST to network hosts

Syntax:

Ping <ipv4_address|ipv6_address> <times>

Parameters:

Ipv4_address : The IP address to PING

Ipv6_address : The IPv6 address to PING

times : The number of repetitions (1- 999999999)

Example:

To send ICMP ECHO_REQUEST to network hosts:

```
WGSW-28040(config)# ping 192.168.0.21 999999999
```

6.3.31 Time Command

Timezone

Description:

Set the time zone of system

Syntax:

time timezone <before-utc|after-utc> <hour> <min>

Parameters:

Before-utc : Time zone before UTC

After-utc : Time zone after UTC

hour : Time zone hour (0-12)

min : Time zone min (0-59)

Example:

To set the time zone of system:

```
WGSW-28040(config)# time timezone before-utc 12 0
```

Date

Description:

Set the date of system

Syntax:

time date <year> <month> <day> <hour> <min> <sec>

Parameters:

year : Year (Format: YYYY) (1990-2037)

month : Month (Format: MM) (1-12)

day : Day (Format: DD) (1-31)

hour : Hour (Format: hh) (0-23)

min : Min (Format: mm) (0-59)

sec : Sec (Format: ss) (0-59)

Example:

To set the time zone of system:

```
WGSW-28040(config)# time date 2011 4 25 15 50 50
```

6.3.32 SNTP Command

Timezone

Description:

Set theSimple Network Time Protocol

Syntax:

sntp server <A.B.C.D> port <tcp_udp_port>

Parameters:

A.B.C.D : IP default gateway format is A.B.C.D where (A/B/C/D = 0 ~ 254)

Tcp_udp_port : TCP/UDP port (1-65535)

Example:

To set the Simple Network Time Protocol:

```
WGSW-28040(config)# sntp server 192.168.0.50 port 111
```

6.3.33 Copy Command

Copy Running-config

Description:

Copy the running-config configurations

Syntax:

copy running-config <startup-config|tftp> [<file_name|A.B.C.D>] [<remote_file>]

Parameters:

Startup-config : Backup the switch configurations

tftp : Send configuration to TFTP server

file_name : Config file name

A.B.C.D : IP default gateway format is A.B.C.D where (A/B/C/D = 0 ~ 254)

Remote_file : Remote file name on TFTP server

Example:

To copy the running-config to TFTP server:

```
WGSW-28040(config)# copy running-config tftp 192.168.0.21 config
```

Copy TFTP

Description:

Retrieve configuration from TFTP server

Syntax:

copy <running-config|startup-config|firmware> [<A.B.C.D|local_file>] [<remote_file>]

Parameters:

running-config : Running configurations

startup-config : Startup config configurations

firmware : Run time firmware image

A.B.C.D : IP default gateway format is A.B.C.D where (A/B/C/D = 0 ~ 254)

local_file : Local startup-config file name

Remote_file : Remote file name on TFTP server

Example:

To copy the running-config to TFTP server:

```
WGSW-28040(config)# copy running-config tftp 192.168.0.21 config
```

Copy Startup-config

Description:

Copy the startup-config configurations

Syntax:

copy startup-config tftp <A.B.C.D|local_file> [<remote_file>] [<local_file>]

Parameters:

A.B.C.D : IP default gateway format is A.B.C.D where (A/B/C/D = 0 ~ 254)

local_file : Local startup-config file name

Remote_file : Remote file name on TFTP server

Example:

To copy the startup-config configurations:

```
WGSW-28040(config)# copy startup-config tftp 192.168.0.21 config test
```

Copy Firmware

Description:

Copy the run time firmware image

Syntax:

copy firmware tftp <A.B.C.D> <remote_file>

Parameters:

A.B.C.D : IP default gateway format is A.B.C.D where (A/B/C/D = 0 ~ 254)

Remote_file : Remote file name on TFTP server

Example:

To copy the run time firmware image:

```
WGSW-28040(config)# copy firmware tftp 192.168.0.21 config
```

Copy Authentication Key

Description:

Copy the SSH Authenticate Private key

Syntax:

copy <rsa1|rsa2|dsa2|ssl_cert> tftp <A.B.C.D> <remote_file>

Parameters:

A.B.C.D : IP default gateway format is A.B.C.D where (A/B/C/D = 0 ~ 254)

Remote_file : Remote file name on TFTP server

Example:

To copy the SSH Authenticate Private key:

```
WGSW-28040(config)# copy rsa1 tftp 192.168.0.21 key
```

6.3.34 Reboot Command

Reboot

Description:

Reboot the switch

Syntax:

reboot

Example:

To reboot the switch:

```
WGSW-28040(config)# reboot
```

6.3.35 Restore Default Command

Restore Default

Description:

Restore to default

Syntax:

restore-defaults

Example:

To restore defaults the switch:

```
WGSW-28040(config)# restore-defaults
```

6.3.36 Username Command

Username

Description:

Set the local username and password

Syntax:

Username <name> privilege <admin|user> <password|secret|nopassword> <password>

Parameters:

name : Local user name

admin : Admin privilege

user : User privilege

password : Use clear text password

secret : Use encrypted password

nopassword : No password for this user

Example:

To restore defaults the switch:

```
WGSW-28040(config)# username test privilege admin password test
```

6.3.37 Enable Command

Enable

Description:

Change the local password

Syntax:

enable <admin|user> <password|secret> <password>

Parameters:

password : Use clear text password

secret : Use encrypted password

Example:

To change the local password:

```
WGSW-28040(config)# enable password security
```

6.3.38 SSL Command

SSL

Description:

Setup SSL host keys

Syntax:

ssl

Generating a 1024 bit RSA private key

.....++++++

.....++++++

writing new private key to '/mnt/ssl_key.pem'

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:

State or Province Name (full name) [Some-State]:

Locality Name (eg, city) []:

Organization Name (eg, company) [Internet Widgits Pty Ltd]:

Organizational Unit Name (eg, section) []:

Common Name (eg, YOUR name) []:

Email Address []:

Parameters:

Country Name (2 letter code) [AU]: Country name

State or Province Name (full name) [Some-State] :State or Province Name

Locality Name (eg, city) [] :Locality Name

Organization Name (eg, company) [Internet Widgits Pty Ltd] :Organization Name

Organizational Unit Name (eg, section) [] :Organizational Unit Name

Common Name (eg, YOUR name) [] :Common Name

Email Address [] :Email Address

Example:

To setup SSL host keys:

```
WGSW-28040(config)# ssl
Generating a 1024 bit RSA private key
.............++++++
.............................++++++
writing new private key to '/mnt/ssl_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:planet
Organizational Unit Name (eg, section) []:switch
Common Name (eg, YOUR name) []:Neo
Email Address []:neot@planet.com.tw
```

6.3.39 Boot Command

Boot

Description:

Set Booting Operations

Syntax:

Boot config-file <name>

Parameters:

name : Local file name

Example:

To set Booting Operations:

```
WGSW-28040(config)# boot config-file config1
```

6.3.40 Delete Command

Delete

Description:

Delete Operations

Syntax:

delete config-file <name>

Parameters:

name : Local file name

Example:

To delete Operations:

```
WGSW-28040(config)# delete config-file config1
```

6.3.41 Telnet Command

Telnet

Description:

Enable Telent daemon configuration

Syntax:

telnet

Example:

To enable Telent daemon configuration:

```
WGSW-28040(config)# telnet
```

6.3.42 IPv6 Command

Auto Configuration

Description:

Enable IPv6 auto-configuration

Syntax:

ipv6 auto-configuration

Example:

To enable IPv6 auto-configuration:

```
WGSW-28040(config)# ipv6 auto-configuration
```

IPv6 Address

Description:

Set IPv6 address

Syntax:

ipv6 address <ipv6_address> prefix <prefix>

Parameters:

Ipv6_address : IPv6 host address.

IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

Prefix : IPv6 subnet mask , default: Show IPv6 prefix

Example:

To set IPv6 address:

```
WGSW-28040(config)# ipv6 address 2001::0001 prefix 64
```

IPv6 Gateway

Description:

Set IPv6 gateway

Syntax:

ipv6 gateway <ipv6_address>

Parameters:

gateway: IPv6 router , default: Show IPv6 router.

IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

Example:

To set IPv6 gateway:

```
WGSW-28040(config)# ipv6 gateway 2001::0002
```

6.3.43 Log Command

Log Restart

Description:

Restart syslog daemon

Syntax:

log restart

Example:

To restart syslog daemon:

```
WGSW-28040(config)# log restart
```

Log Server

Description:

Set the remote server, maximum 4 servers can be configured

Syntax:

log server <server_index> <A.B.C.D> <server_port> <severity>

Parameters:

Server_index :Remote server index (1-4)

A.B.C.D :IP default gateway format is A.B.C.D where (A/B/C/D = 0 ~ 254)

Server_port : Remote server Port, default 514 (1~65535)

Severity : Log severity 0-7 (EMEGR->DEBUG) (e.g. 0,5-7) Use "show log cat-sev-table" to see mapping index.

Example:

To set the remote server:

```
WGSW-28040(config)# log server 1 192.168.0.21 514 0
```

Log Flash & RAM

Description:

Set the flash or RAM log

Syntax:

log <flash|ram> <severity>

Parameters:

Flash|ram :target side

Severity : Log severity 0-7 (EMEGR->DEBUG) (e.g. 0,5-7) Use "show log cat-sev-table" to see mapping index.

Example:

To set flash log:

```
WGSW-28040(config)# log flash 1
```

6.3.44 TFTP Server Command

TFTP Server

Description:

Set the TFTP server configurations

Syntax:

tftp-server <firmware|config> <ip|filename> <A.B.C.D|file_name>

Parameters:

firmware : Run time firmware image

config : Startup config configurations

ip : tftp server ip address

filename :tftp server remote file name

A.B.C.D : IP Address format is A.B.C.D where (A/B/C/D = 0 ~ 254)

File_name :file name

Example:

To set the TFTP server configurations:

```
WGSW-28040(config)# tftp-server config filename config
```

6.3.45 VLAN Command

VLAN Port Mode

Description:

Set VLAN mode

Syntax:

vlan port <port_list> mode <original|keep-format|priority-tag>

Parameters:

Port_list :Port list or 'all'

original :original mode

keep-format : keep format mode

priority-tag :priority tag mode

Example:

To set VLAN mode:

```
WGSW-28040(config)# vlan port 1 mode original
```

VLAN Port PVID

Description:

Set port configured VLAN ID

Syntax:

vlan port <port_list> pvid <pvid>

Parameters:

Port_list :Port list or 'all'

pvid : pvid

Example:

To set port configured VLAN ID:

```
WGSW-28040(config)# vlan port 1 pvid 1
```

VLAN Port Accept Frame Type

Description:

Set VLAN accept frame type

Syntax:

vlan port <port_list> accept-frame-type <all|tag-only|untag-only>

Parameters:

Port_list :Port list or 'all'

all : pvid

tag-only : pvid

untag-only : pvid

Example:

To set VLAN accept frame type:

```
WGSW-28040(config)# vlan port 1 accept-frame-type all
```

VLAN Ingress Filter

Description:

Set VLAN ingress filtering configuration

Syntax:

vlan ingress-filter

Example:

To set VLAN ingress filtering configuration:

```
WGSW-28040(config)# vlan ingress-filter
```

VLAN Leaky

Description:

Set VLAN leaky configuration

Syntax:

vlan leaky

Example:

To set VLAN leaky configuration:

```
WGSW-28040(config)# vlan leaky
```

VLAN Name

Description:

Set VLAN name configuration

Syntax:

vlan <vid> name <name>

Parameters:

vid :vid

name : VLAN name, maximum 16 characters

Example:

To set VLAN name configuration:

```
WGSW-28040(config)# vlan1 name vlan1
```

VLAN Tagged

Description:

Set VLAN tagged or untagged port

Syntax:

vlan <vid> <tagged|untagged> port <port_list>

Parameters:

vid :vid

tagged|untagged : tagged or untagged ports

Port_list :Port list or 'all'

Example:

To set VLAN tagged port:

```
WGSW-28040(config)# vlan1 tagged port 1
```

6.3.46 SSH Command

SSH

Description:

Set SSH (Secure Shell) configuration

Syntax:

Ssh [<v1|v2|all>]

Parameters:

V1 : SSH v1 host keys

V2 : SSH v2 host keys

all : Both SSH v1 and v2 host keys

Example:

To set SSH (Secure Shell) configuration:

```
WGSW-28040(config)#ssh
```

6.3.47 PoE Command

PoE Admin-mode

Description:

Configure System PoE Admin mode information

Syntax:

poe admin-mode <enable|disable>

Parameters:

enable Enable POE

disable Disable POE

Example:

To enable PoE admin mode:

```
WGSW-28040(config)#poe admin-mode enable
```

PoE Limit-mode

Description:

Configure System PoE power limit mode information

Syntax:

poe limit-mode <consumption>

Parameters:

consumption Power is allocated according to the actual need of each PD

Example:

To use consumption mode for PoE limit mode:

```
WGSW-28040(config)#poe limit-mode consumption
```

PoE Port

Description:

Enable/Disable the port POE injects funtion

Syntax:

poe port <enable|disable> <port-list>

Parameters:

enable Enable POE

disable Disable POE

Port_list :Port list or 'all'

Example:

To disable port 1 PoE function:

```
WGSW-28040(config)#poe didsable port 1
```

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. TROUBLE SHOOTING

This chapter contains information to help you solve issue. If the Managed Switch is not functioning properly, make sure the Managed Switch was set up according to instructions in this manual.

■ **The Link LED is not lit**

Solution:

Check the cable connection and remove duplex mode of the Managed Switch

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

Solution:

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

■ **Performance is bad**

Solution:

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

■ **Why the Switch doesn't connect to the network**

Solution:

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

■ **100Base-TX port link LED is lit, but the traffic is irregular**

Solution:

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

■ **Switch does not power up**

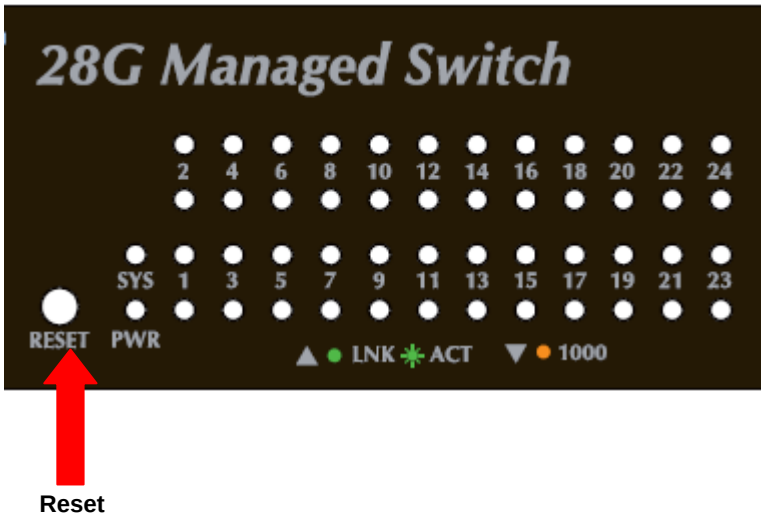
Solution:

1. AC power cord not inserted or faulty
2. Check 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

■ **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.



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-

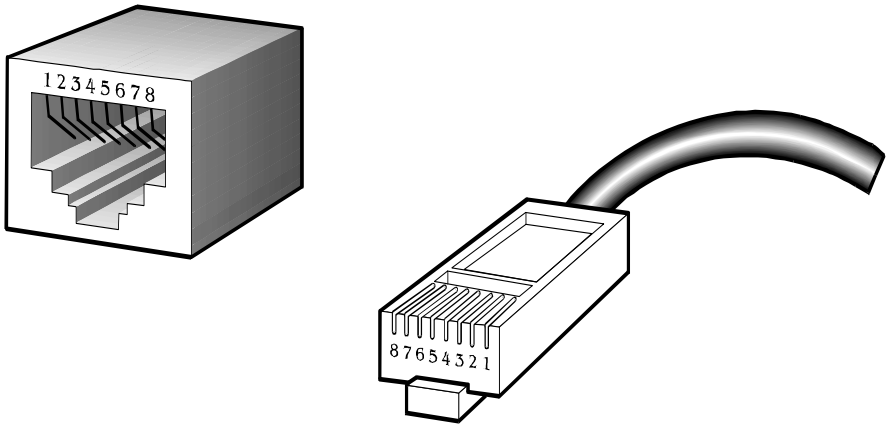
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

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:

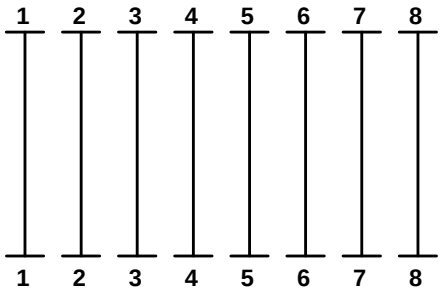
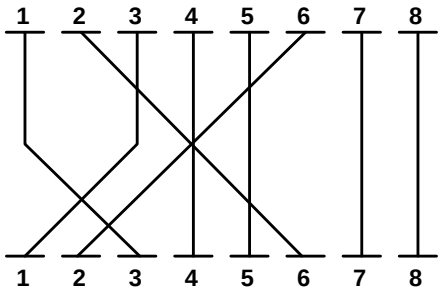
Straight Cable		**SIDE 1**	**SIDE2**
	**SIDE 1**	**1 = White / Orange**	**1 = White / Orange**
		2 = Orange	**2 = Orange**
		3 = White / Green	**3 = White / Green**
		4 = Blue	**4 = Blue**
		5 = White / Blue	**5 = White / Blue**
		6 = Green	**6 = Green**
		7 = White / Brown	**7 = White / Brown**
	SIDE 2	**8 = Brown**	**8 = Brown**
Crossover Cable		**SIDE 1**	**SIDE2**
	**SIDE 1**	**1 = White / Orange**	**1 = White / Green**
		2 = Orange	**2 = Green**
		3 = White / Green	**3 = White / Orange**
		4 = Blue	**4 = Blue**
		5 = White / Blue	**5 = White / Blue**
		6 = Green	**6 = Orange**
		7 = White / Brown	**7 = White / Brown**
	SIDE 2	**8 = Brown**	**8 = Brown**

Figure A-1: Straight-Through and Crossover Cable

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

2080-A93230-000

EC Declaration of Conformity

For the following equipment:

*Type of Product: 28-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch
*Model Number: WGSW-28040

* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address: 10F., No.96, Minquan Rd., Xindian Dist.,
New Taipei City 231, Taiwan (R.O.C.)

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC).
For the evaluation regarding the EMC, the following standards were applied:

EN 55022	(Class A:2006)
EN 61000-3-2	(2006)
EN 61000-3-3	(1995/A1: 2001/A2:2005)
EN 55024	(1998/A1: 2001/A2:2003)
IEC 61000-4-2	(2001)
IEC 61000-4-3	(2008)
IEC 61000-4-4	(2004)
IEC 61000-4-5	(2005)
IEC 61000-4-6	(2008)
IEC 61000-4-8	(2001)
IEC 61000-4-11	(2004)

Responsible for marking this declaration if the:

☒ **Manufacturer** ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

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

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Taiwan	**9th May., 2011**	Kent Kang
Place	*Date*	*Legal Signature*

PLANET TECHNOLOGY CORPORATION

e-mail: sales@planet.com.tw http://www.planet.com.tw
10F., No.96, Minquan Rd., Xindian Dist., New Taipei City, Taiwan, R.O.C. Tel:886-2-2219-9518 Fax:886-2-2219-9528

EC Declaration of Conformity

For the following equipment:

*Type of Product: 24-Port 10/100/1000Mbps PoE + 4-Port Gigabit TP/SFP Combo Managed Switch
*Model Number: WGSW-28040P

* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address: 10F., No.96, Minquan Rd., Xindian Dist.,
New Taipei City 231, Taiwan (R.O.C.)

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC).
For the evaluation regarding the EMC, the following standards were applied:

EN 55022	(Class A:2006)
EN 61000-3-2	(2006)
EN 61000-3-3	(1995/A1: 2001/A2:2005)
EN 55024	(1998/A1: 2001/A2:2003)
IEC 61000-4-2	(2001)
IEC 61000-4-3	(2008)
IEC 61000-4-4	(2004)
IEC 61000-4-5	(2005)
IEC 61000-4-6	(2008)
IEC 61000-4-8	(2001)
IEC 61000-4-11	(2004)

Responsible for marking this declaration if the:

☒ **Manufacturer** ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

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

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Taiwan	**14th Oct., 2011**	Kent Kang
Place	*Date*	*Legal Signature*

PLANET TECHNOLOGY CORPORATION

e-mail: sales@planet.com.tw http://www.planet.com.tw
10F., No.96, Minquan Rd., Xindian Dist., New Taipei City, Taiwan, R.O.C. Tel:886-2-2219-9518 Fax:886-2-2219-9528