PLANET
Networking & Communication

User's Manual

WGSW-24040
WGSW-24040R

24-Port 10/100/1000Mbps

Layer 2 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 24-Port 10/100/1000Mbps with 4 Shared SFP Combo Managed Switch User's Manual

FOR MODELS: WGSW-24040 / WGSW-24040R

REVISION: 1.5 (June.2010)

Part No: EM-WGSW-24040_24040R (2080-A93070-003)

TABLE OF CONETNTS

1. INTRODUTION

The PLANET Layer 2 Managed Gigabit Switch series – WGSW-24040/24040R are all multiple ports Gigabit Ethernet Switches with SFP fiber optical connective ability and robust layer 2 features; the description of these models as below:

WGSW-24040 : 24-Port 10/100/1000Base-T with 4 Shared SFP Managed Gigabit Switch

WGSW-24040R : 24-Port 10/100/1000Base-T with 4 Shared SFP Managed Gigabit Switch / Redundant Power

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

1.1 Packet Contents

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

Check the contents of your package for following parts:

- ☑ **The Managed Switch** x1
- ☑ **User's manual CD** x1
- ☑ **Quick installation guide** x1
- ☑ **19" Rack mount accessory kit** x1
- ☑ **Power cord** x1
- ☑ **Rubber feet** X4
- ☑ **RS-232 DB9 male Console cable** x1

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**, WGSD-8020. 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 WGSD-8020 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 / Telecom class Gigabit solution for Enterprise backbone and Data Center Networking

The PLANET Managed Switch is a L2/L4 Managed Gigabit Switch. Since Gigabit network interface had become the basic

equipment and requirement of Enterprise and Network Servers, with 48Gbps switching fabric, the MANAGED SWITCH can handle extremely large amounts of data in a secure topology linking to a backbone or high capacity servers. The powerful QoS and Network Security features make it to meets the needs of effective data traffic control for both Campus and Enterprise, such VoIP, video streaming and multicast application.

High Performance

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

Robust Layer 2 Features

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

Excellent Traffic Control

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

Efficient Management

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

Powerful Security

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

Flexibility and Extension solution

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

WDM fiber). They are well suited for using within the enterprise data centers and distributions.

AC / DC Power Redundant to ensure continuous operation

The WGSW-24040R Managed Switch equip with one 100~240V AC power supply unit and one DC -48V power supply unit on its standard package, it provides redundant power supply installation. A redundant power system is also provided to enhance the reliability with either 100~240V AC power supply unit or DC -48V power supply unit. The continuous power systems are specifically designed to handle the demands of high tech facilities requiring the highest power integrity available.

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

Model		WGSW-24040	WGSW-24040R
Interface	10/100/1000 T	24	24
	1000SX/LX	4	4
Redundant Power		-	-48V DC (-30V~-60V)

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**
  - **24-Port 10/100/1000Base-T** Gigabit Ethernet RJ-45
  - **4 mini-GBIC/SFP slots**, shared with Port-21 to Port-24
  - **RS-232** DB9 console interface for Switch basic management and setup

- **Layer 2 Features**
  - Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standard
  - Supports Auto-negotiation and half duplex/full duplex modes for all 10Base-T/100Base-TX and 1000Base-T ports.
  - Auto-MDI/MDI-X detection for each RJ-45 port
  - Prevents packet loss with back pressure (Half-Duplex) and IEEE 802.3x PAUSE frame flow control (Full-Duplex)
  - High performance of Store-and-Forward architecture, broadcast storm control and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
  - 8K MAC address table, automatic source address learning and ageing
  - 1392Kbytes embedded memory for packet buffers
  - Storm Control support:
    - Broadcast / Multicast / Unknown-Unicast
  - Support **VLAN**
    - IEEE 802.1Q Tagged VLAN
    - Up to 255 VLANs groups, out of 4094 VLAN IDs
    - Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
    - Private VLAN Edge (PVE)
    - Voice VLAN
  - Support **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
    - BPDU Guard
  - Support **Link Aggregation**
    - 802.3ad Link Aggregation Control Protocol (LACP)
    - Cisco ether-channel (Static Trunk)
    - Maximum 12 trunk groups, up to 16 ports per trunk group
    - Up to 16Gbps bandwidth(Duplex Mode)
  - Provide Port Mirror (many-to-1)
  - Port Mirroring to monitor the incoming or outgoing traffic on a particular port

- **Quality of Service**
  - Ingress Shaper and Egress Rate Limit per port bandwidth control
  - 4 priority queues on all switch ports

- Traffic classification:
  - IEEE 802.1p CoS
  - TOS / DSCP / IP Precedence of IPv4/IPv6 packets
  - IP TCP/UDP port number
  - Typical network application
- Strict priority and Weighted Round Robin (WRR) CoS policies
- Supports QoS and In/Out bandwidth control on each port
- Traffic-policing policies on the switch port
- QoS Control List Wizard makes QoS creation and configuration easier and more quickly
- DSCP remarking

➢ **Multicast**

- Supports IGMP Snooping v1, v2 and v3
- Querier mode support
- IGMP Snooping port filtering
- Multicast VLAN Registration (MVR) support

➢ **Security**

- IEEE 802.1x Port-Based / MAC-Based network access authentication
- Built-in RADIUS client to co-operate with the RADIUS servers
- TACACS+ login users access authentication
- RADIUS / TACACS+ users access authentication
- IP-Based Access Control List (ACL)
- MAC-Based Access Control List
- Source MAC / IP address binding
- **DHCP Snooping** to filter un-trusted DHCP messages
- **Dynamic ARP Inspection** discards ARP packets with invalid MAC address to IP address binding
- **IP Source Guard** prevents IP spoofing attacks
- Auto DoS rule to defend DoS attack
- IP address access management to prevent unauthorized intruder

➢ **Management**

- Switch Management Interfaces
  - Console / Telnet Command Line Interface
  - Web switch management
  - SNMP v1, v2c, and v3 switch management
  - SSH / SSL secure access
- Four RMON groups (history, statistics, alarms, and events)
- **IPv6** IP Address / NTP / DNS management
- Built-in Trivial File Transfer Protocol (TFTP) client

- BOOTP and DHCP for IP address assignment
- Firmware upload/download via HTTP / TFTP
- DHCP Relay
- User Privilege levels control
- NTP (Network Time Protocol)
- Link Layer Discovery Protocol (LLDP) Protocol
- Cable Diagnostic technology provides the mechanism to detect and report potential cabling issues
- Reset button for system reboot or reset to factory default
- PLANET Smart Discovery Utility for deploy management
- ICMPv6

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

- 100~240V AC / 48V DC Dual power redundant
- Active-active redundant power failure protection
- Backup of catastrophic power failure on one supply
- Fault tolerance and resilience.

1.5 Product Specification

■ **WGSW Standalone models**

Product	WGSW-24040	WGSW-24040R
Hardware Specification		
Copper Ports	24 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports	
SFP/mini-GBIC Slots	4 SFP interfaces, shared with Port-21 to Port-24	
Console Port	1 x RS-232 DB9 serial port (115200, 8, N, 1)	
Switch Fabric	48Gbps / non-blocking	
Address Table	8K entries, automatic source address learning and ageing	
Share data Buffer	1392 kilobytes	
Switch Processing Scheme	Store-and-Forward	
Flow Control	IEEE 802.3x Pause Frame for Full-Duplex Back pressure for Half-Duplex	
Jumbo Frame	10Kbytes	
Reset Button	< 5 sec: System reboot > 5 sec: Factory Default	
Dimension (W x D x H)	440 x 200 x 44.5 mm, 1U high	
Weight	WGSW-24040: 3.3kg WGSW-24040R: 3.4kg	
LED	Power, Link/Act and speed per Gigabit port	
Power Consumption	Max. 30 watts / 102 BTU	

Power Requirement – AC	AC 100~240V, 50/60Hz	AC : 100~240V, 50/60Hz
Power Requirement – DC	---	-48V DC @ 0.6A Range: -30 ~ -60V
ESD Protection	6KV DC	
Layer 2 Function		
Basic Management Interfaces	Console, Telnet, Web Browser, SNMPv1, v2c and v3	
Secure Management Interface	SSH, SSL, SNMP v3	
Port configuration	Port disable/enable. Auto-negotiation 10/100/1000Mbps full and half duplex mode selection. Flow Control disable / enable. Bandwidth control on each port. Power saving mode control	
Port Status	Display each port's speed duplex mode, link status, Flow control status. Auto negotiation status, trunk status.	
VLAN	802.1Q Tagged Based VLAN ,up to 255 VLAN groups Q-in-Q Private VLAN Voice VLAN	
Port trunking	IEEE 802.3ad LACP / Static Trunk Support 12 groups of 16-Port trunk support	
QoS	Traffic classification based, Strict priority and WRR 4-level priority for switching - Port Number - 802.1p priority - DS/TOS field in IP Packet	
IGMP Snooping	IGMP (v1/v2) Snooping, up to 255 multicast Groups IGMP Querier mode support	
Access Control List	IP-Based ACL / MAC-Based ACL Up to 256 entries	
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-1643 Ethernet MIB RFC-2863 Interface MIB RFC-2665 Ether-Like MIB RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC-2933 IGMP-STD-MIB RFC3411 SNMP-Frameworks-MIB IEEE802.1X PAE LLDP	

	MAU-MIB
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX/100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1d Spanning Tree protocol IEEE 802.1w Rapid Spanning Tree protocol IEEE 802.1s Multiple Spanning Tree IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab Link Layer Discovery Protocol (LLDP)

2. INSTALLATION

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

2.1 Hardware Description

2.1.1 Switch Front Panel

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

WGSW-24040 / WGSW-24040R Front Panel

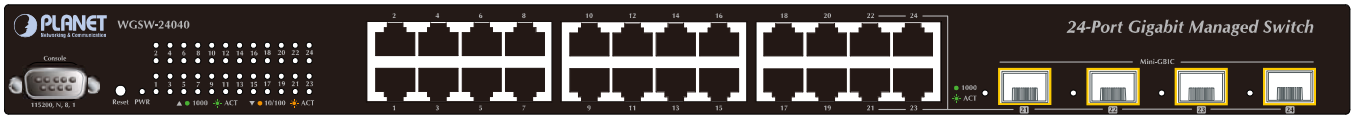


Figure 2-1 WGSW-24040 / WGSW-24040R front panel.

■ **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.

■ **Reset button**

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

Reset Button Pressed and Released	Function
< 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.

WGSW-24040 / WGSW-24040R LED indication

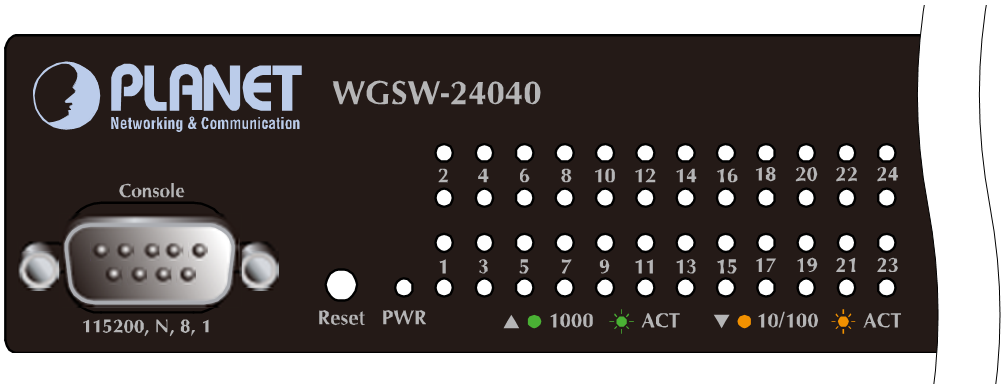


Figure 2-2 WGSW-24040 / WGSW-24040R LED panel

■ **System**

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

■ **10/100/1000Base-T interfaces**

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

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

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

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

2.1.3 Switch Rear Panel

The rear panel of the Managed Switch indicates an AC inlet power socket, which accept input power from 100 to 240V AC, 50-60Hz. Figure 2-3 & Figure 2-4 shows the rear panel of these Managed Switches

WGSW-24040 Rear Panel

Figure 2-3 Rear panel of **WGSW-24040**

WGSW-24040R Rear Panel

Figure 2-4 Rear panel of **WGSW-24040R**

■ **AC Power Receptacle**

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

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

Power Notice:

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

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

■ **DC Power Connector**

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

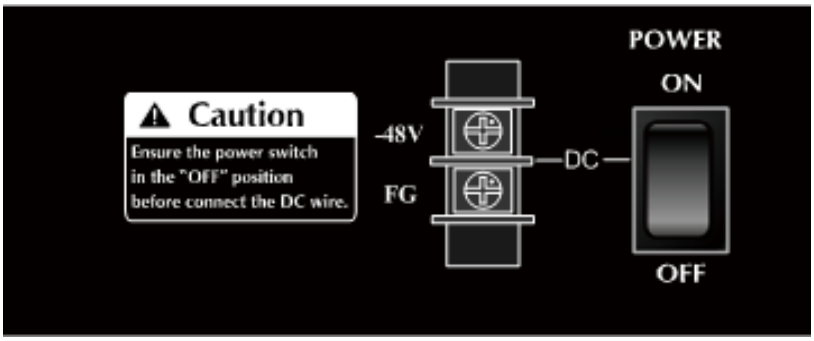


Figure 2-5 Rear Panel of WGSW-24040R

Warning:

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

2.2 Install the Switch

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

2.2.1 Desktop Installation

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

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

Step2: Place the Managed Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-6.

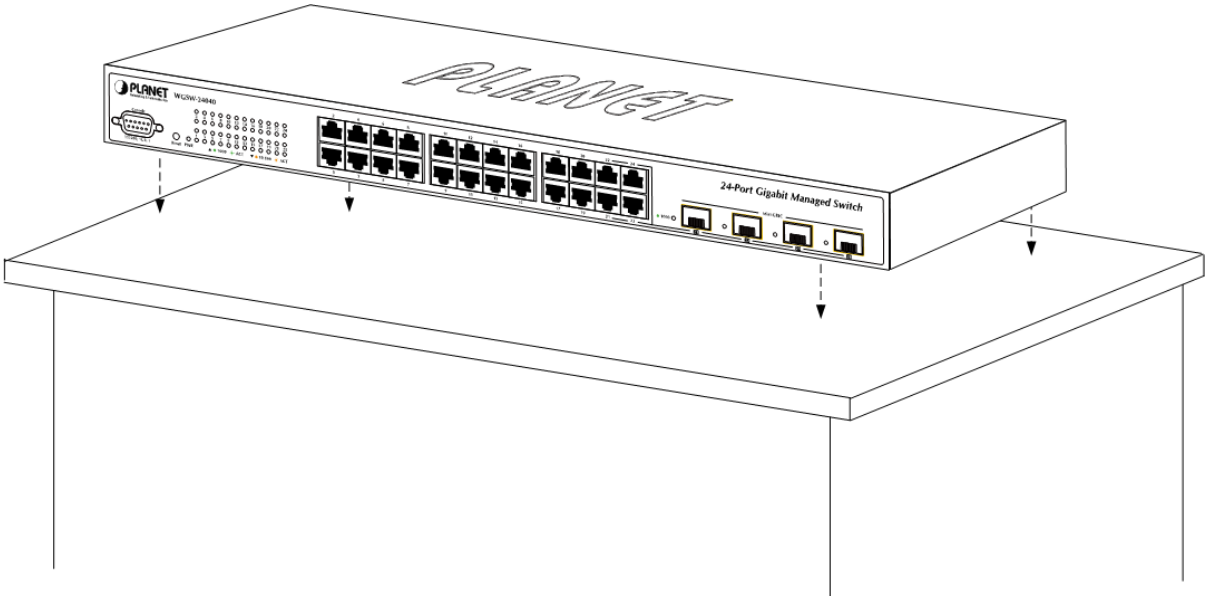


Figure 2-6 Place the Managed Switch on the desktop

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 2-7 shows how to attach brackets to one side of the Managed Switch.

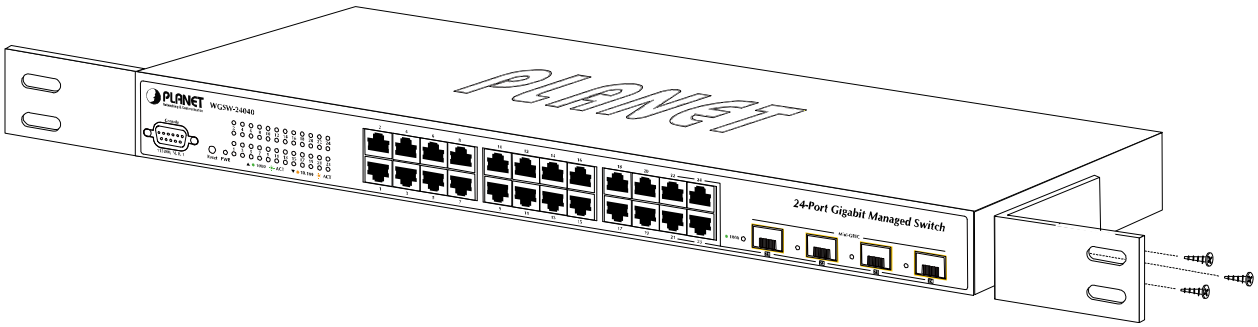


Figure 2-7 Attach brackets to the Managed Switch.

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 2-8.

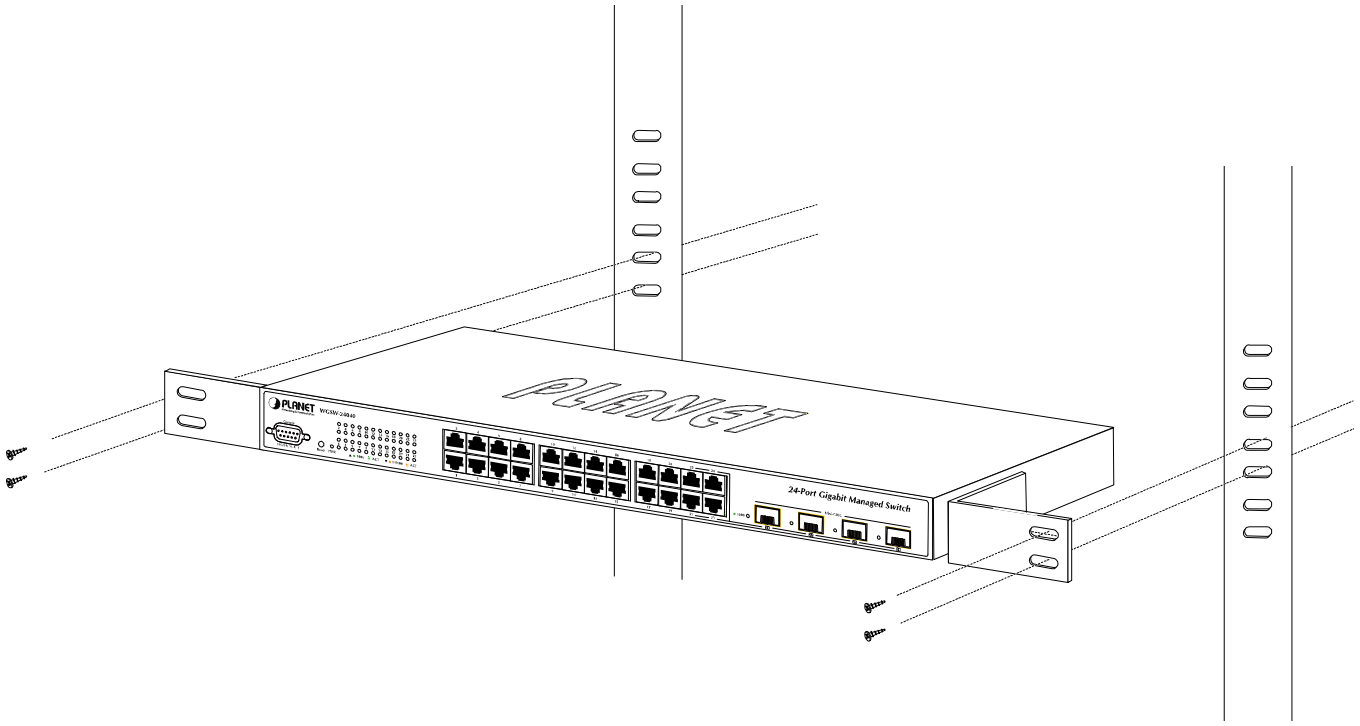


Figure 2-8 Mounting WGSW-24040 in a Rack

Step6: Proceeds with the steps 4 and steps 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Managed Switch.

2.2.3 Installing the SFP transceiver

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

The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Managed Switch. As the Figure 2-9 appears.

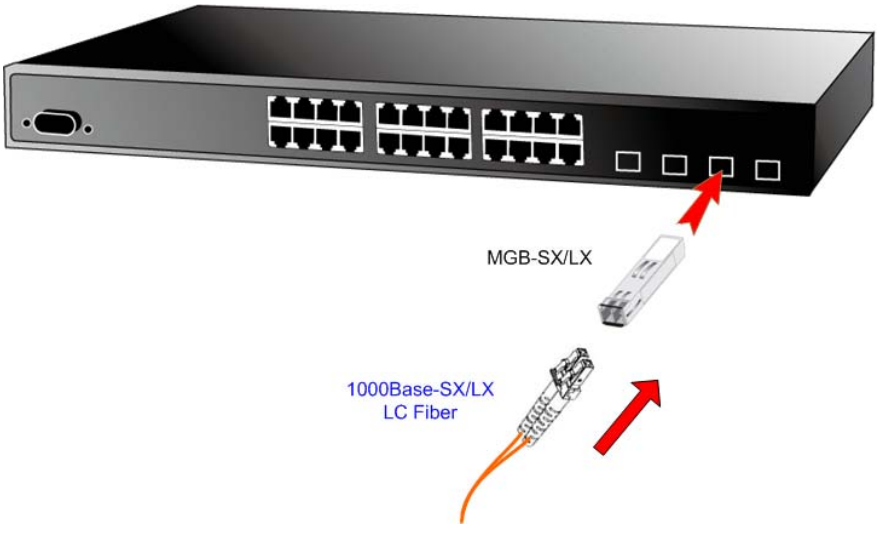


Figure 2-9 Plug-in the SFP transceiver

■ Approved PLANET SFP Transceivers

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

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

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.

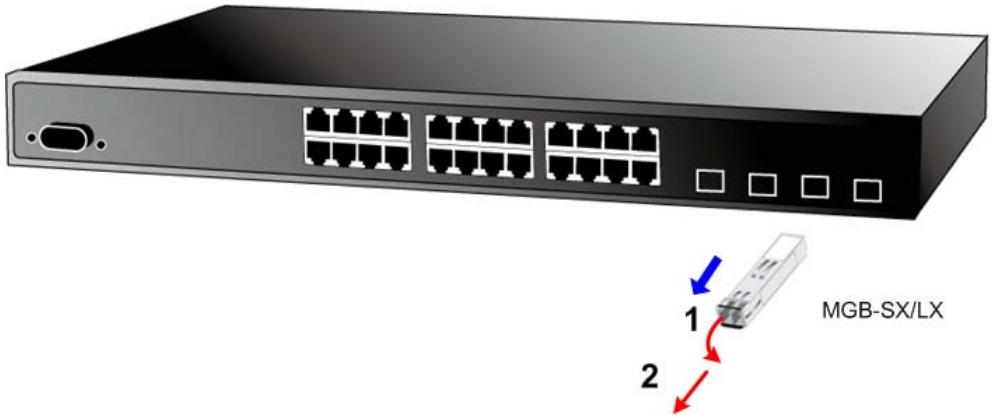


Figure 2-10 Pull out the SFP transceiver

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

2.2.4 Connecting DC Power Supply – WGSW-24040R

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

1. The size of the two screws in the terminal block is M3.5.
2. The terminals are marked "-48V", "FG".
3. Loosen the two screws so you can slide the DC cable beneath it. Insert the DC cable into the connector first, and screw it down tight.
4. Connect the power cable to the DC power supply. After power up or reset, the Managed Switch performs a cold start procedure.

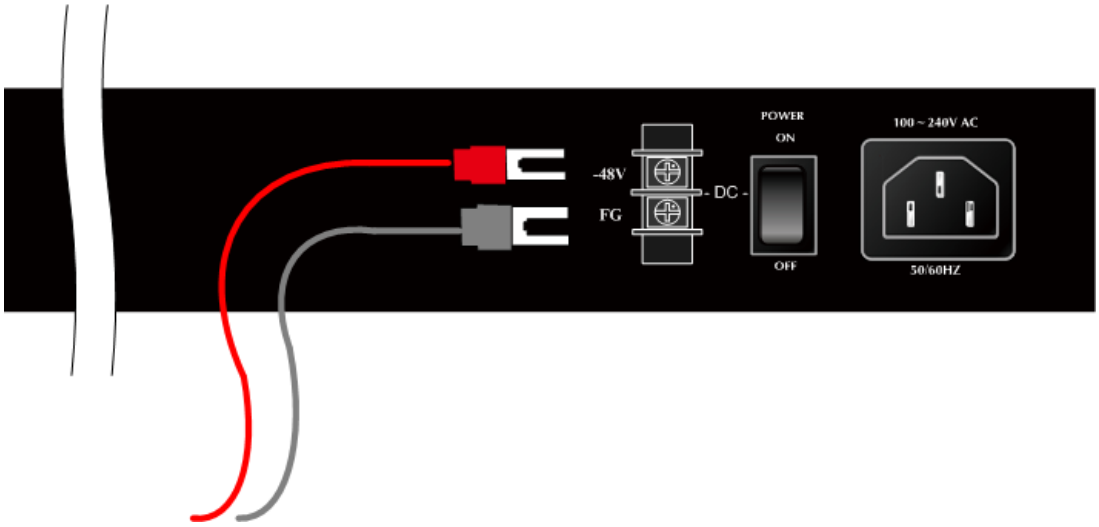


Figure 2-11 -48VDC connector

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

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**

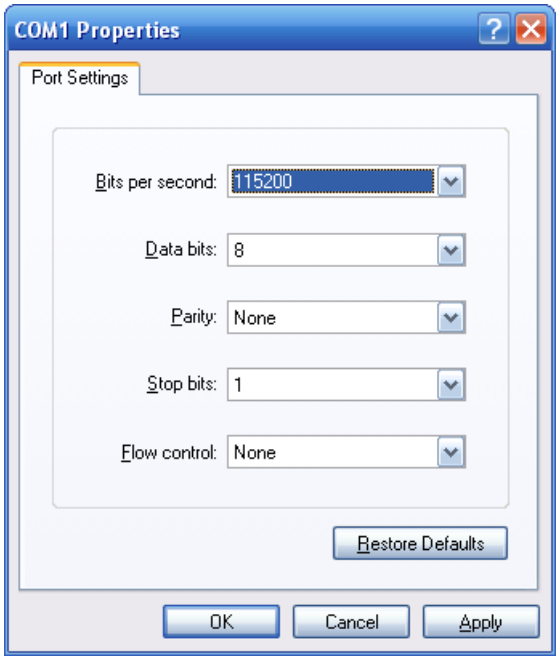


Figure 3-2 Terminal parameter settings

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.

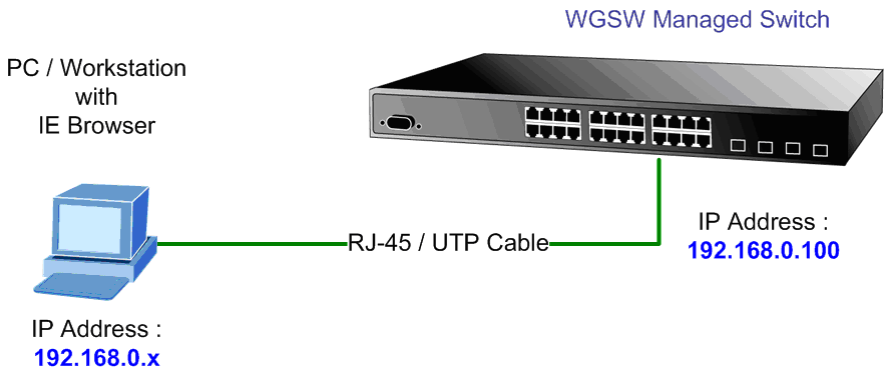


Figure 3-3 Web management

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

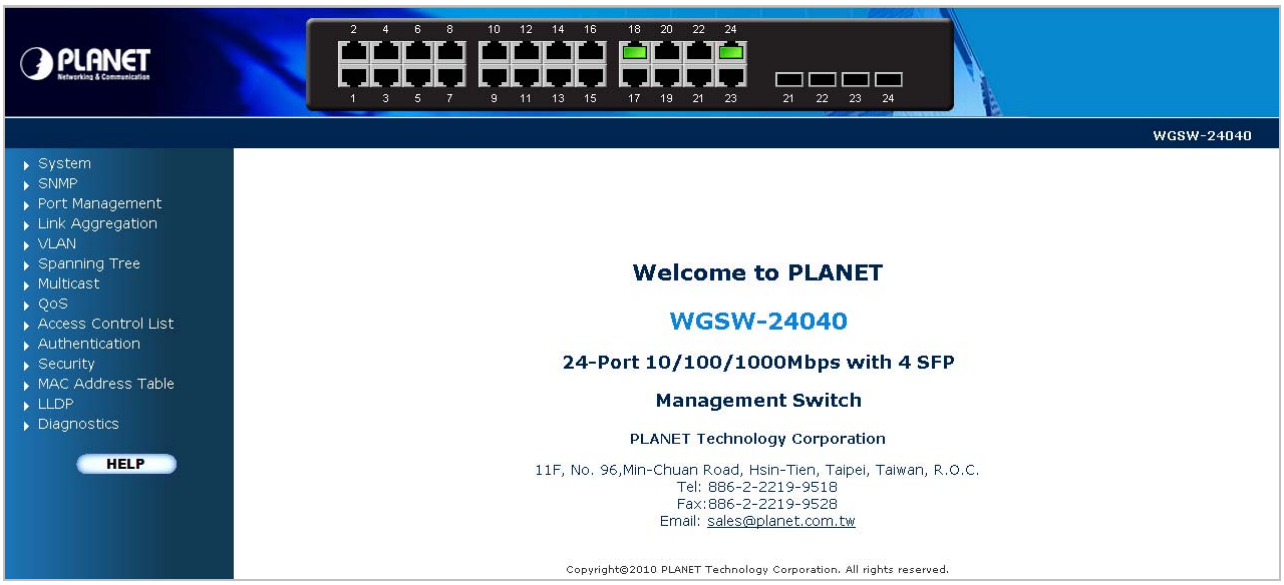


Figure 3-4 Web main screen of Managed Switch

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.

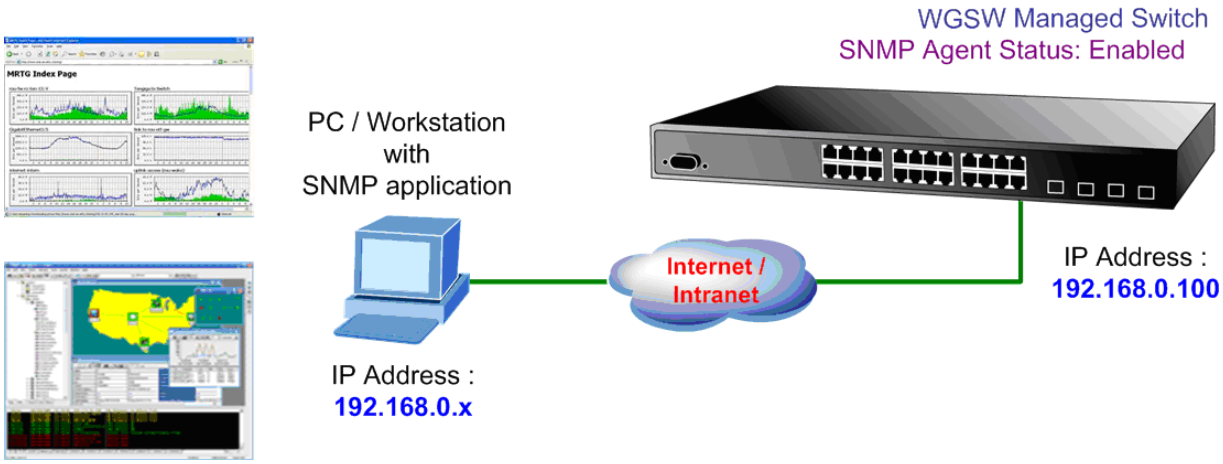


Figure 3-5 SNMP management

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 WGSW 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.

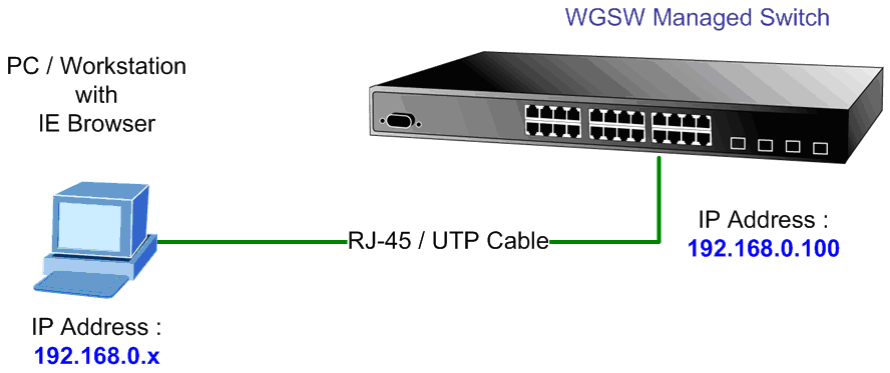


Figure 4-1-1 Web Management

- **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.

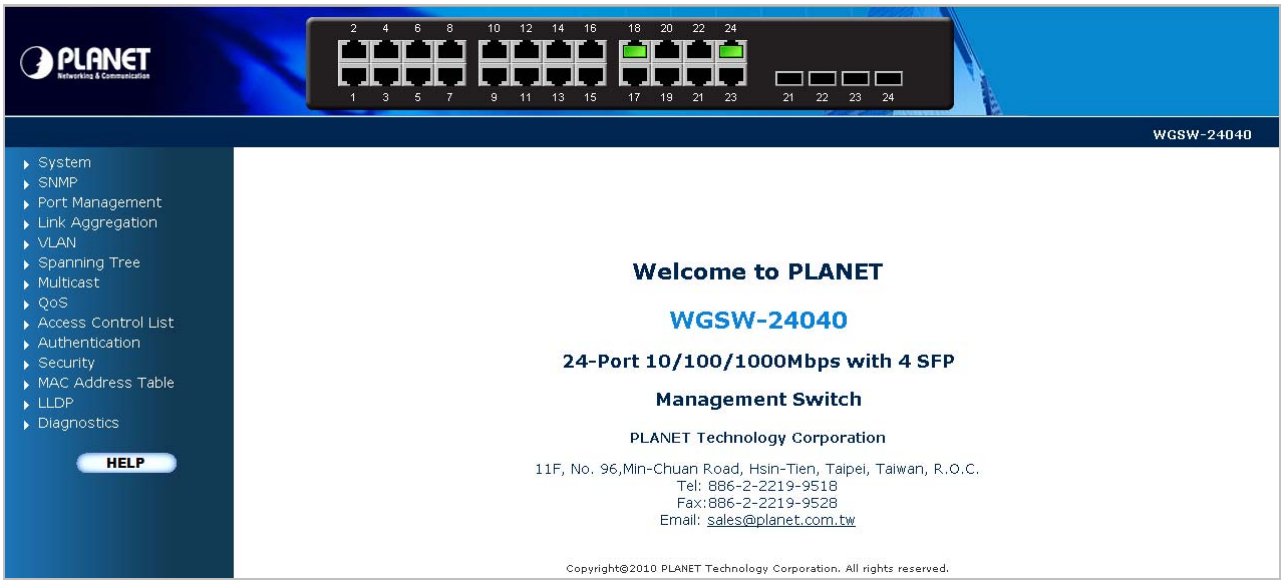


Figure 4-1-3 Default main page

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.

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 WGSW Managed Switch provide 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.

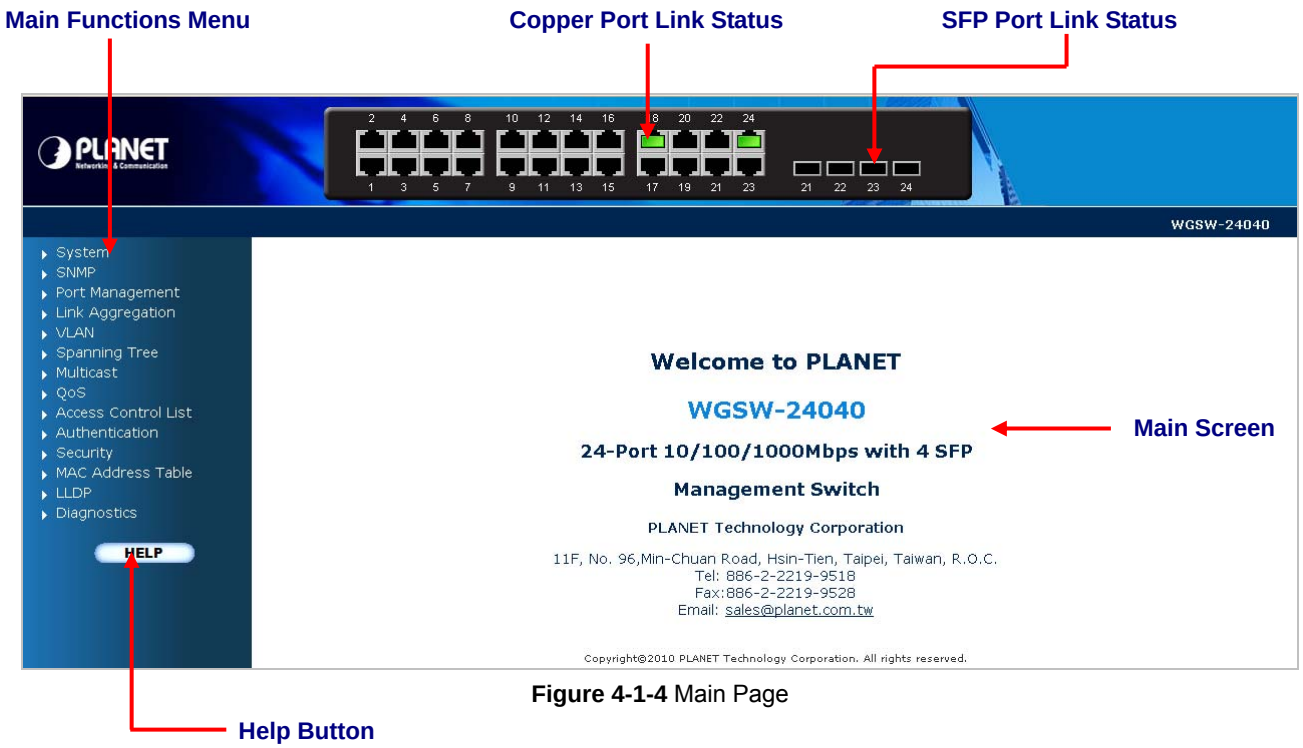


Figure 4-1-4 Main Page

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.

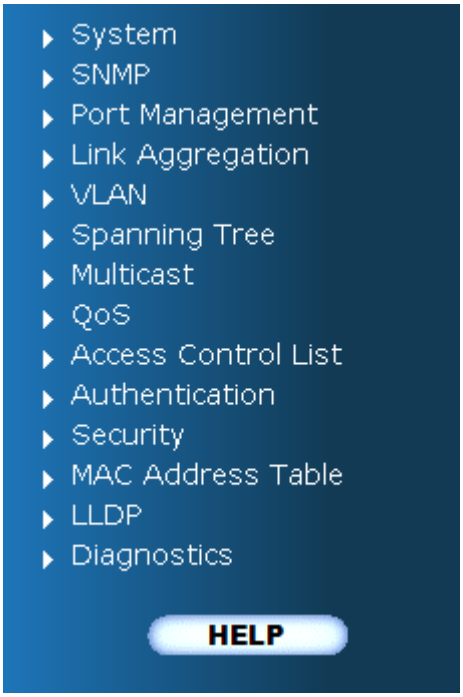


Figure 4-1-5 WGSW Managed Switch Main Functions Menu

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.
Users Configuration	This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.
Users Privilege Levels	This page provides an overview of the privilege levels.
NTP Configuration	Configure NTP on this page.
UPnP	Configure UPnP on this page.
DHCP Relay	Configure DHCP Relay on this page.
DHCP Relay Statistics	This page provides statistics for DHCP relay.
CPU Load	This page displays the CPU load, using a SVG graph.
System Log	The switch system log information is provided here.
Detailed Log	The switch system detailed log information is provided here.
Web Firmware Upgrade	This page facilitates an update of the firmware controlling the switch.
TFTP Firmware Upgrade	Upgrade the firmware via TFTP server
Configuration Save	You can save the switch configuration. The configuration file is in XML format with a hierarchy of tags.
Configuration Upload	You can load the switch configuration. The configuration file is in XML format with a hierarchy of tags.
Factory Default	You can reset the configuration of the stack switch on this page. Only the IP configuration is retained.
System Reboot	You can restart the stack switch on this page. After restart, the stack switch will boot normally.

4.2.1 System Information

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

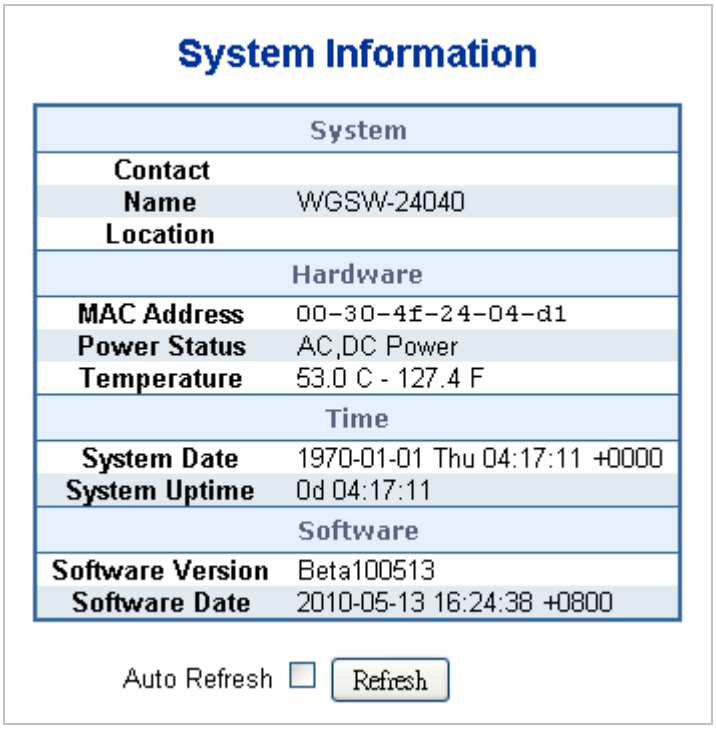


Figure 4-2-1 System Information page screenshot

The page includes the following fields:

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

Buttons

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

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

4.2.2 IP Configuration

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

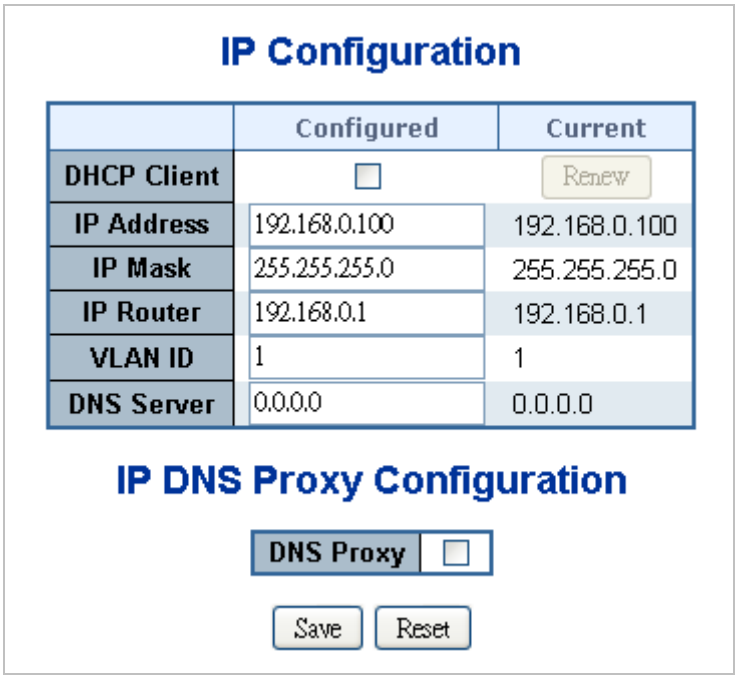


Figure 4-2-2 IP Configuration page screenshot

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

Object	Description
• **DHCP Client**	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
• **IP Address**	Provide the IP address of this switch in dotted decimal notation.
• **IP Mask**	Provide the IP mask of this switch dotted decimal notation.
• **IP Router**	Provide the IP address of the router in dotted decimal notation.

• **DNS Server**	Provide the IP address of the DNS Server in dotted decimal notation.
• **VLAN ID**	Provide the managed VLAN ID. The allowed range is **1** through **4095**.
• **DNS Proxy**	When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.

Buttons

Save: Click to save changes.

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

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

4.2.3 IPv6 Configuration

Configure the switch-managed IPv6 information on this page.

The Configured column is used to view or change the IPv6 configuration. The Current column is used to show the active IPv6 configuration. The screen in Figure 4-2-3 appears.

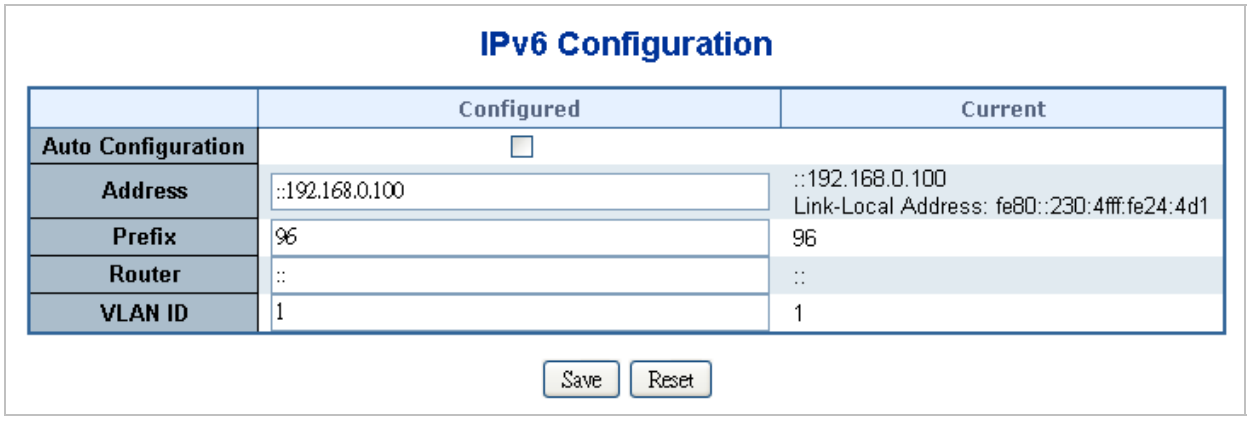


Figure 4-2-3 IPv6 Configuration page screenshot

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.
• **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'.
• **Prefix**	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'. Provide the IPv6 SNTP Server 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'.
• **VLAN ID**	Provide the managed VLAN ID. The allowed range is 1 through 4095

Buttons

Save: Click to save changes.

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

4.2.4 Users Configuration

This page provides an overview of the current users. 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 **"Save"** button to take effect. Please login web interface with new user name and password, the screen in Figure 4-2-4 appears.

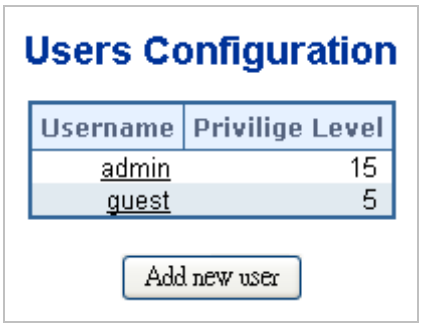


Figure 4-2-4 Users Configuration page screenshot

The page includes the following fields:

Object	Description
• **Username**	The name identifying the user. This is also a link to Add/Edit User.
• **Privilege Level**	The privilgeg level for the user.

Buttons

Add new user: Click to add a new user.

Add / Edit User

This page configures a user – add, edit or delete user.

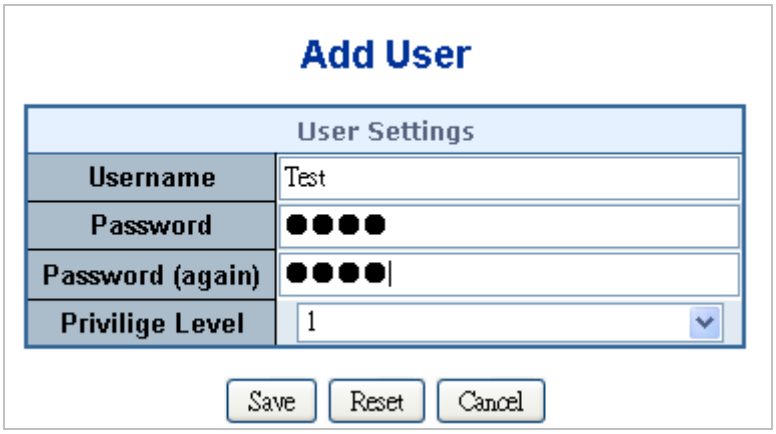


Figure 4-2-5 Add / Edit User Configuration page screenshot

The page includes the following fields:

Object	Description
• **Username**	The name identifying the user.
• **Password**	The password of the user.
• **Privilege Level**	The privilgeg level for the user.

Buttons

Save: Click to save changes.

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

Cancel: Click to undo any changes made locally and return to the Users.

Delete User: Delete the current user. This button is not available for new configurations (Add new user)

Once the new user is added, the new user entry shown in the Users Configuration page.

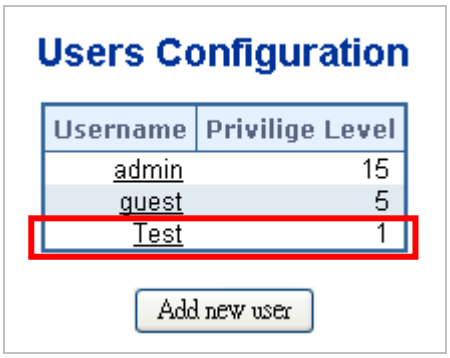


Figure 4-2-6 User Configuration page screenshot

Note

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

4.2.5 Users Privilege Levels

This page provides an overview of the privilege levels. After setup completed, please press **"Save"** button to take effect. Please login web interface with new user name and password, the screen in Figure 4-2-7 appears.

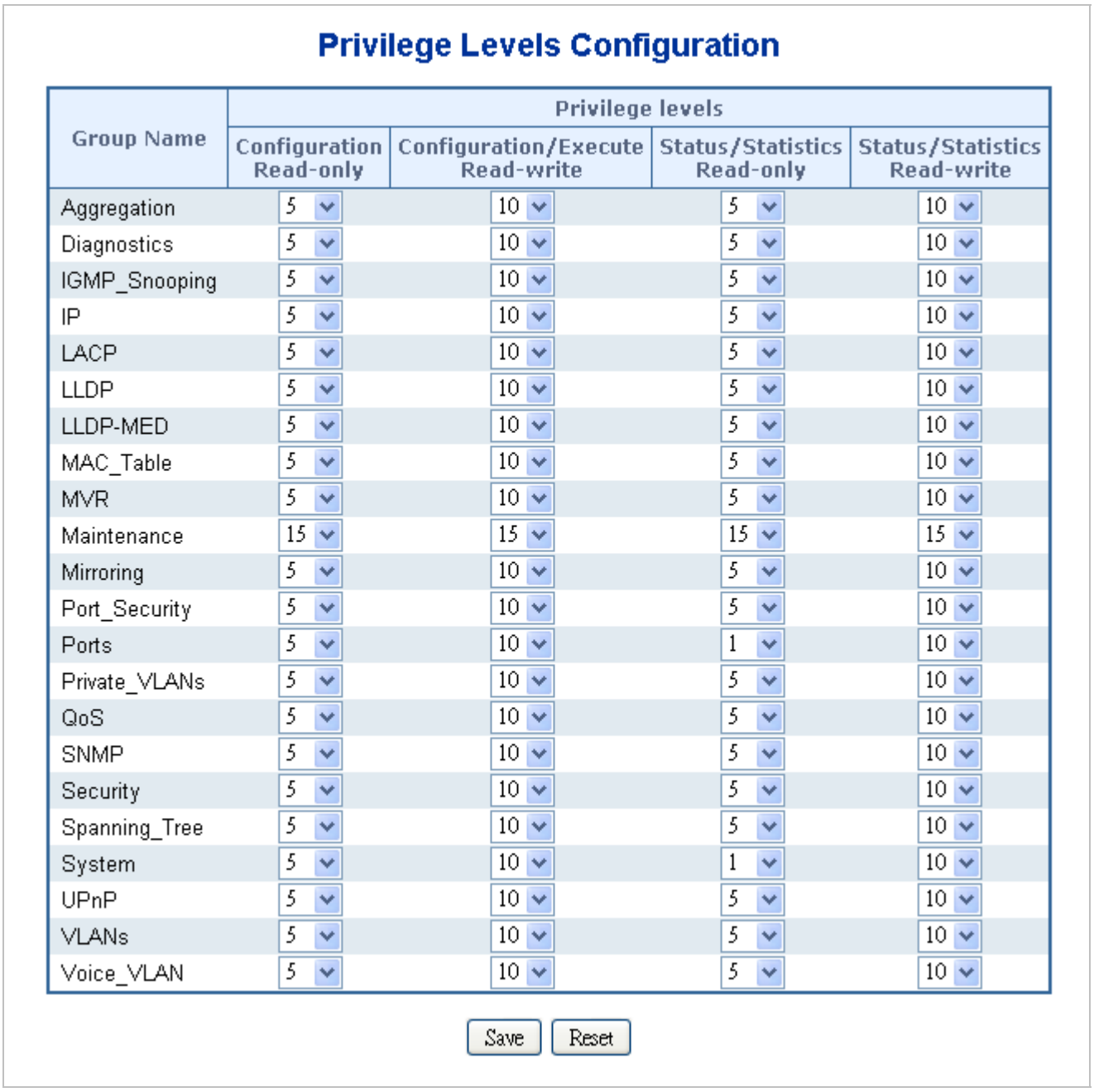


Figure 4-2-7 Privilege Levels Configuration page screenshot

The page includes the following fields:

Object	Description
• **Group Name**	The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level

	groups in details: System: Contact, Name, Location, Timezone, Log. Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard. IP: Everything except 'ping'. Port: Everything except 'VeriPHY'. Diagnostics: 'ping' and 'VeriPHY'. Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance. Debug: Only present in CLI.
• **Privilege Level**	Every privilege level group has an authorization level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics).

4.2.6 NTP Configuration

Configure NTP on this page.

NTP is an acronym for **Network Time Protocol**, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (data grams) as transport layer. You can specify NTP Servers and set GMT Time zone. The NTP Configuration screen in Figure 4-2-8 appears.

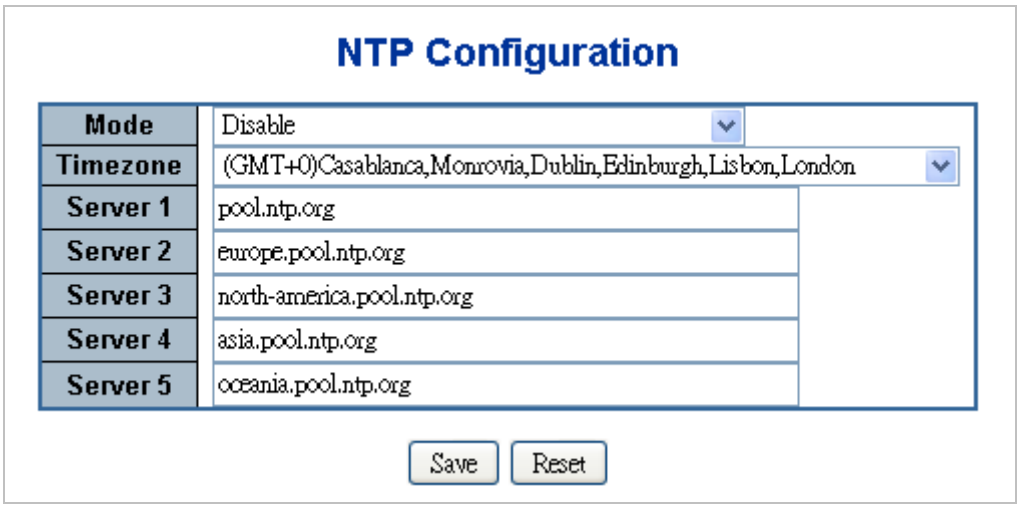


Figure 4-2-8 NTP Configuration page screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the NTP mode operation. Possible modes are: **Enabled**: 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. **Disabled**: Disable NTP mode operation.
• **Server #**	Provide the NTP IPv4 or 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'.

4.2.7 UPnP Configuration

Configure UPnP on this page.

UPnP is an acronym for **Universal Plug and Play**. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. The UPnP Configuration screen in Figure 4-2-9 appears.

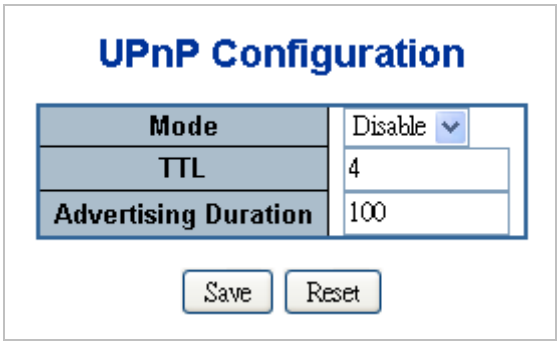


Figure 4-2-9 UPnP Configuration page screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the UPnP operation mode. Possible modes are: **Enabled**: Enable UPnP mode operation. **Disabled**: Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

• **TTL**	The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.
• **Advertising Duration**	The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive a SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

Buttons

Save: Click to save changes.

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

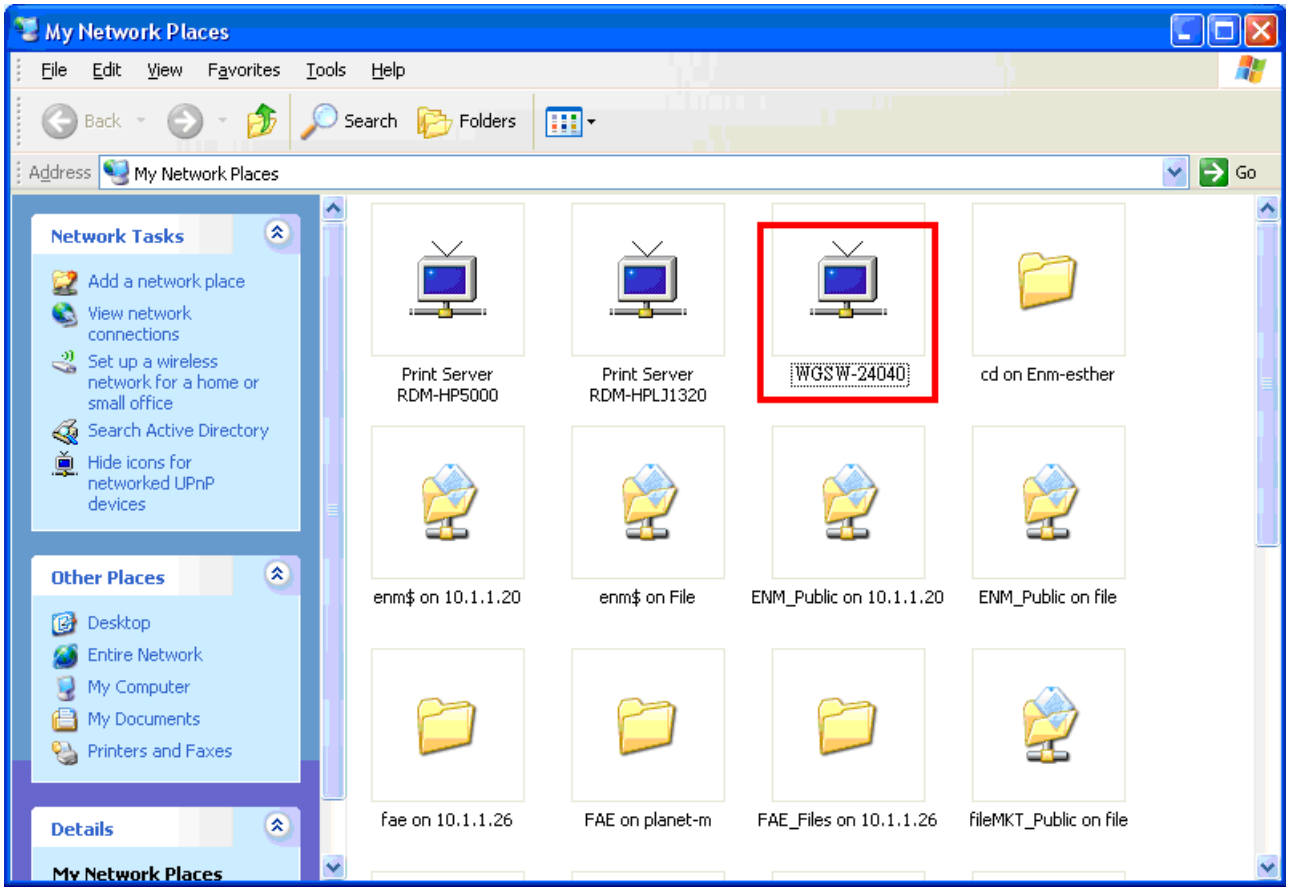


Figure 4-2-10 UPnP devices shows on Windows My Network Places

4.2.8 DHCP Relay

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

The **DHCP option 82** enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options:

- Circuit ID (option 1)
- Remote ID (option2).

The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on.
The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agent's MAC address. The DHCP Relay Configuration screen in Figure 4-2-11 appears.

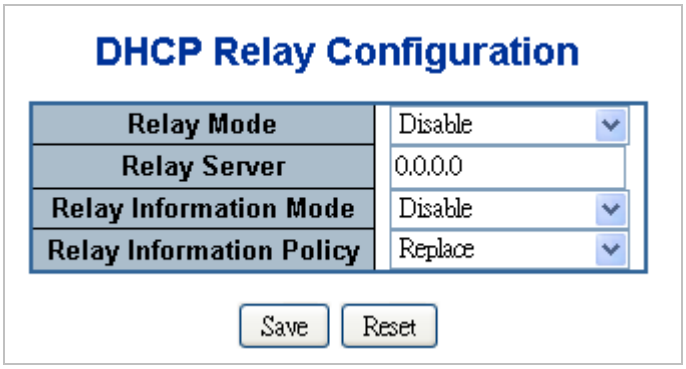


Figure 4-2-11 DHCP Relay Configuration page screenshot

The page includes the following fields:

Object	Description
• **Relay Mode**	Indicates the DHCP relay mode operation. Possible modes are: **Enabled**: Enable DHCP relay mode operation. When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered. **Disabled**: Disable DHCP relay mode operation.

• **Relay Server**	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.
• **Relay Information Mode**	Indicates the DHCP relay information mode option operation. Possible modes are: **Enabled**: Enable DHCP relay information mode operation. When enable DHCP relay information mode operation, the agent insert specific information (option 82) into a DHCP message when forwarding to DHCP server and remove it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled. **Disabled**: Disable DHCP relay information mode operation.
• **Relay Information Policy**	Indicates the DHCP relay information option policy. When enable DHCP relay information mode operation, if agent receive a DHCP message that already contains relay agent information. It will enforce the policy. And it only works under DHCP relay information operation mode enabled. Possible policies are: **Replace**: Replace the original relay information when receive a DHCP message that already contains it. **Keep**: Keep the original relay information when receive a DHCP message that already contains it. **Drop**: Drop the package when receive a DHCP message that already contains relay information.

4.2.9 DHCP Relay Statistics

This page provides statistics for DHCP relay. The DHCP Relay Statistics screen in Figure 4-2-12 appears.

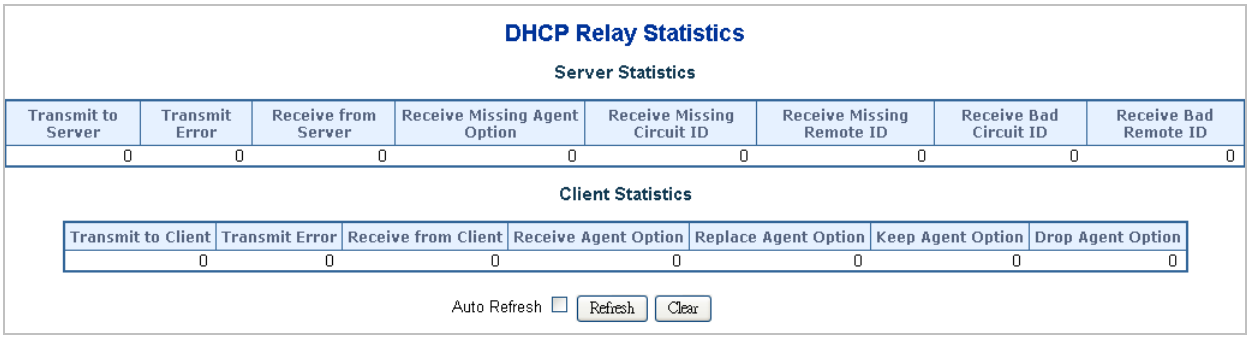


Figure 4-2-12 DHCP Relay Statistics page screenshot

The page includes the following fields:

Server Statistics

Object	Description
• **Transmit to Server**	The packets number that relayed from client to server.
• **Transmit Error**	The packets number that errors sending packets to clients.
• **Receive form Server**	The packets number that received packets from server.
• **Receive Missing Agent Option**	The packets number that received packets without agent information options.
• **Receive Missing Circuit ID**	The packets number that received packets which the Circuit ID option was missing.
• **Receive Missing Remote ID**	The packets number that received packets which Remote ID option was missing.
• **Receive Bad Circuit ID**	The packets number that the Circuit ID option did not match known circuit ID.
• **Receive Bad Remote ID**	The packets number that the Remote ID option did not match known Remote ID.

Client Statistics

Object	Description
• **Transmit to Client**	The packets number that relayed packets from server to client.
• **Transmit Error**	he packets number that error sending packets to servers.
• **Receive form Client**	The packets number that received packets from server.
• **Receive Agent Option**	The packets number that received packets with relay agent information option.
• **Replace Agent Option**	The packets number that replaced received packets with relay agent information option.
• **Keep Agent Optin**	The packets number that keepped received packets with relay agent information option.
• **Drop Agent Option**	The packets number that dropped received packets with relay agent information option.

Buttons

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

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

Clear: Clear all statistics.

4.2.10 CPU Load

This page displays the CPU load, using a SVG graph.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samles are graphed, and the last numbers are displayed as text as well.

In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG. The CPU Load screen in Figure 4-2-13 appears.

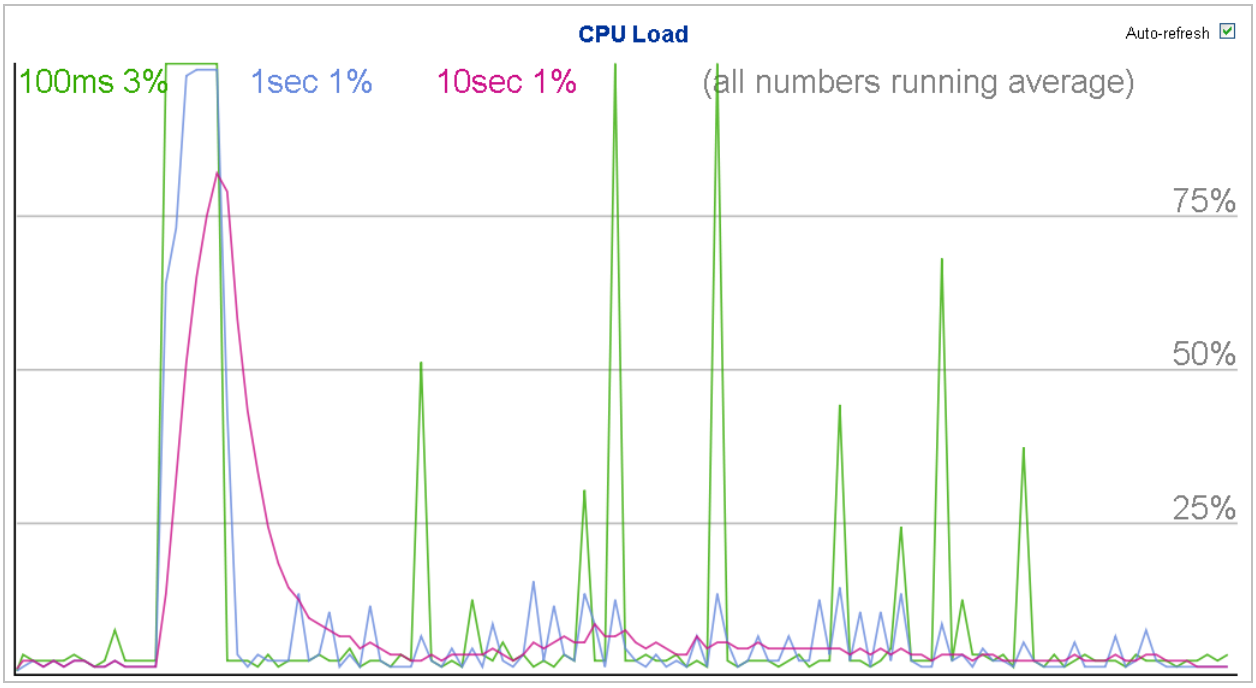


Figure 4-2-13 CPU Load page screenshot

Buttons

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

4.2.11 System Log

The switch system log information is provided here. The System Log screen in Figure 4-2-14 appears.

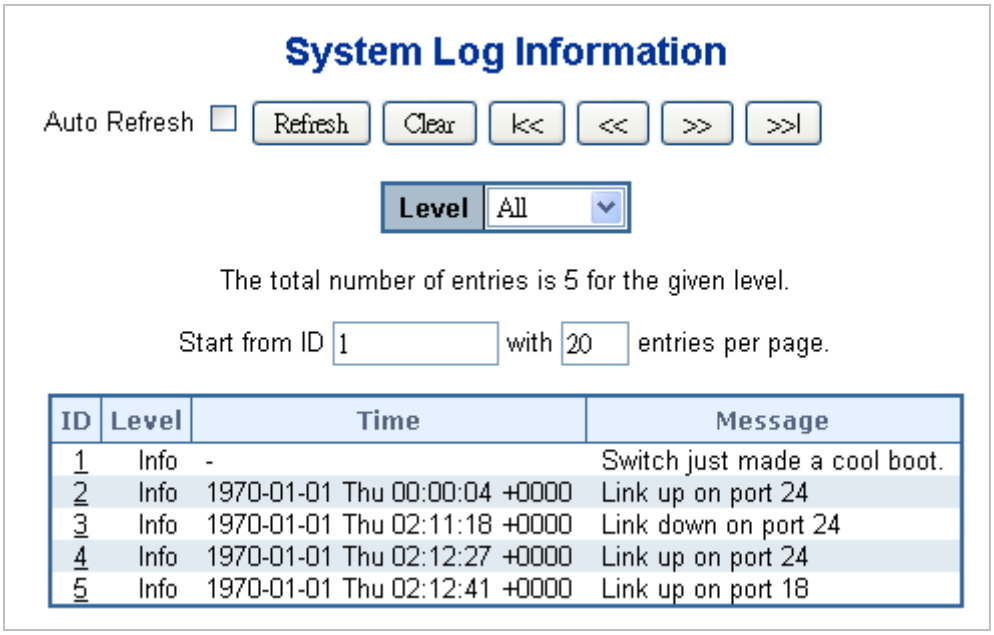


Figure 4-2-14 System Log page screenshot

The page includes the following fields:

Object	Description
• **ID**	The ID (>= 1) of the system log entry.
• **Level**	The level of the system log entry. The following level types are supported: **Info**: Information level of the system log. **Warning**: Warning level of the system log. **Error**: Error level of the system log. **All**: All levels.
• **Time**	The time of the system log entry.
• **Message**	The message of the system log entry.

Buttons

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

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

Clear: Clear all statistics.

<<: Updates the system log entries, starting from the first available entry ID.

<<: Updates the system log entries, ending at the last entry currently displayed.

>>: Updates the system log entries, starting from the last entry currently displayed.

>>|: Updates the system log entries, ending at the last available entry ID.

4.2.12 Detailed Log

The switch system detailed log information is provided here. The Detailed Log screen in Figure 4-2-15 appears.

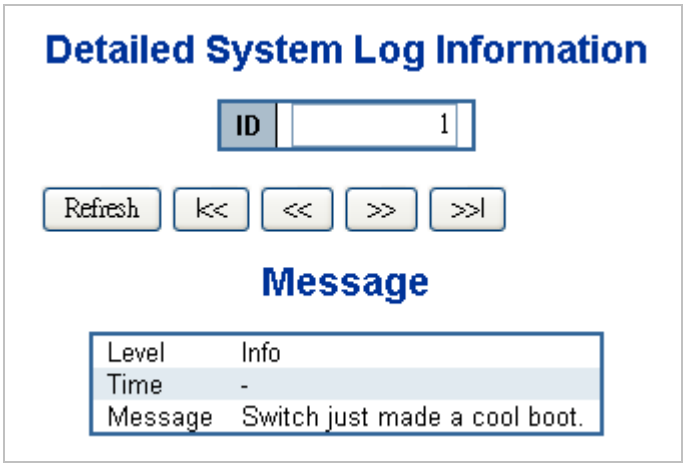


Figure 4-2-15 Detailed Log page screenshot

The page includes the following fields:

Object	Description
• **ID**	The ID (>= 1) of the system log entry.
• **Message**	The message of the system log entry.

Buttons

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

|<<: Updates the system log entries, starting from the first available entry ID.

<<: Updates the system log entries, ending at the last entry currently displayed.

>>: Updates the system log entries, starting from the last entry currently displayed.

>>|: Updates the system log entries, ending at the last available entry ID.

4.2.13 Web Firmware Upgrade

This page facilitates an update of the firmware controlling the switch. The Web Firmware Upgrade screen in Figure 4-2-16 appears.

Figure 4-2-16 Web Firmware Upgrade page screenshot

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

1. Click **System** -> Web **Firmware Upgrade**.
2. The Firmware Upgrade screen is displayed as in Figure 4-2-16.
3. Click the "Browse "button of the main page, the system would pop up the file selection menu to choose firmware.
4. Select on the firmware then click "Upload", the **Software Upload Progress** would show the file upload status.
5. Once the software be loaded to the system successfully. The following screen appears. The system will load the new software after reboot.

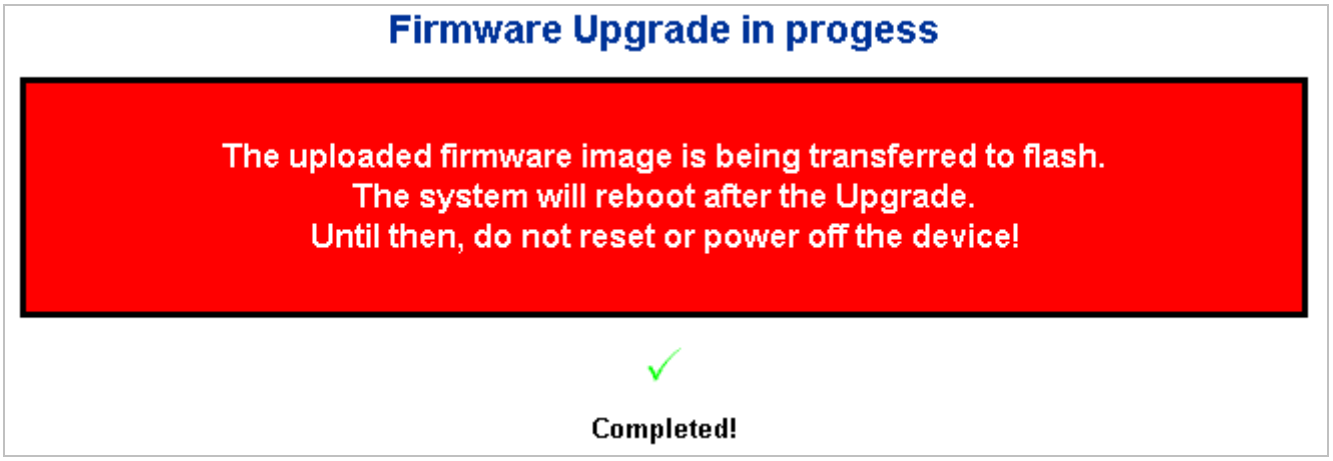


Figure 4-2-17 Software successfully loaded notice screen

Note

DO NOT Power OFF the Managed Switch until the update progress is complete.

Note

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

4.2.14 TFTP Firmware Upgrade

The **Firmware Upgrade** page provides the functions to allow a user to update the Managed Switch firmware from the TFTP server in the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. The TFTP Firmware Upgrade screen in Figure 4-2-18 appears.

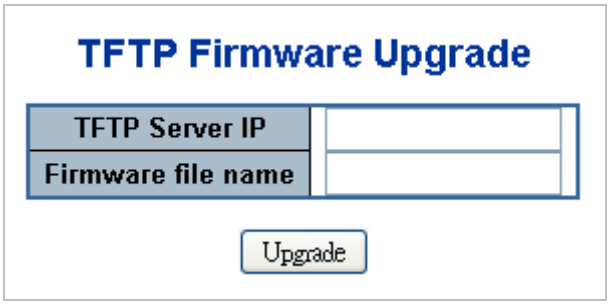


Figure 4-2-18 TFTP Firmware Update page screenshot

The page includes the following fields:

Object	Description
• **TFTP Server IP**	Fill in your TFTP server IP address.
• **Filename**	The name of firmware image. (Maximum length : 24 characters)

Buttons

Upload: Click to upgrade firmware.

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

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

4.2.15 Configuration Save

This function allows backup and reload the current configuration of the Managed Switch to the local management station. The Configuration Save screen in Figure 4-2-19 appears.

Figure 4-2-19 Configuration Save page screenshot

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

Header tags:	<?xml version="1.0"?> and <configuration>. These tags are mandatory and must be present at the beginning of the file.
Section tags:	<platform>, <global> and <switch>. The platform section must be the first section tag and this section must include the correct platform ID and version. The global section is optional and includes configuration which is not related to specific switch ports. The switch section is optional and includes configuration which is related to specific switch ports.
Module tags:	<ip>, <mac>, <port> etc. These tags identify a module controlling specific parts of the configuration.
Group tags:	<port_table>, <vlan_table> etc. These tags identify a group of parameters, typically a table.
Parameter tags:	<mode>, <entry> etc. These tags identify parameters for the specific section, module and group. The <entry> tag is used for table entries.

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

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

■ **Save Configuration**

1. Press the **"Save Configuration"** button to save the current configuration in manager workstation. The following screens in Figure 4-2-20 & 4-2-21 appear

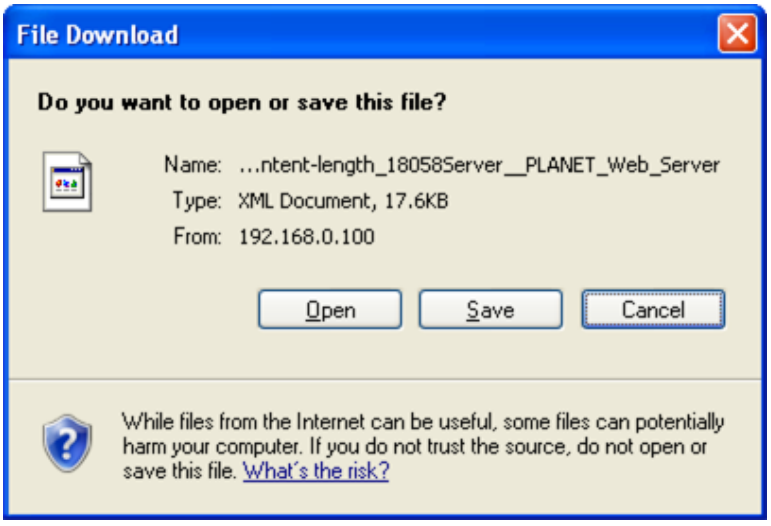


Figure 4-2-20 File Download screen

2. Chose the file save path in management workstation.

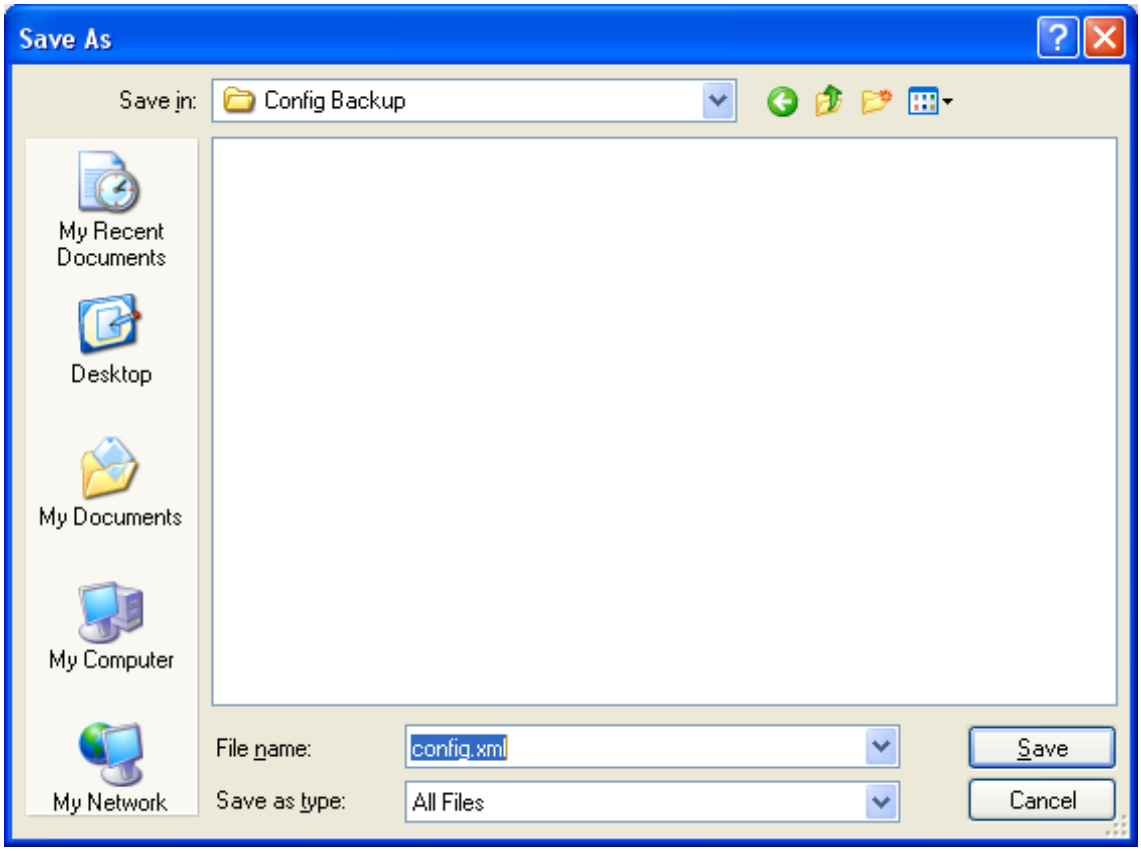


Figure 4-2-21 File save screen

4.2.16 Configuration Upload

This function allows backup and reload the current configuration of the Managed Switch to the local management station. The Configuration Upload screen in Figure 4-2-22 appears.

Figure 4-2-22 Configuration Upload page screenshot

■ **Configuration Upload**

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

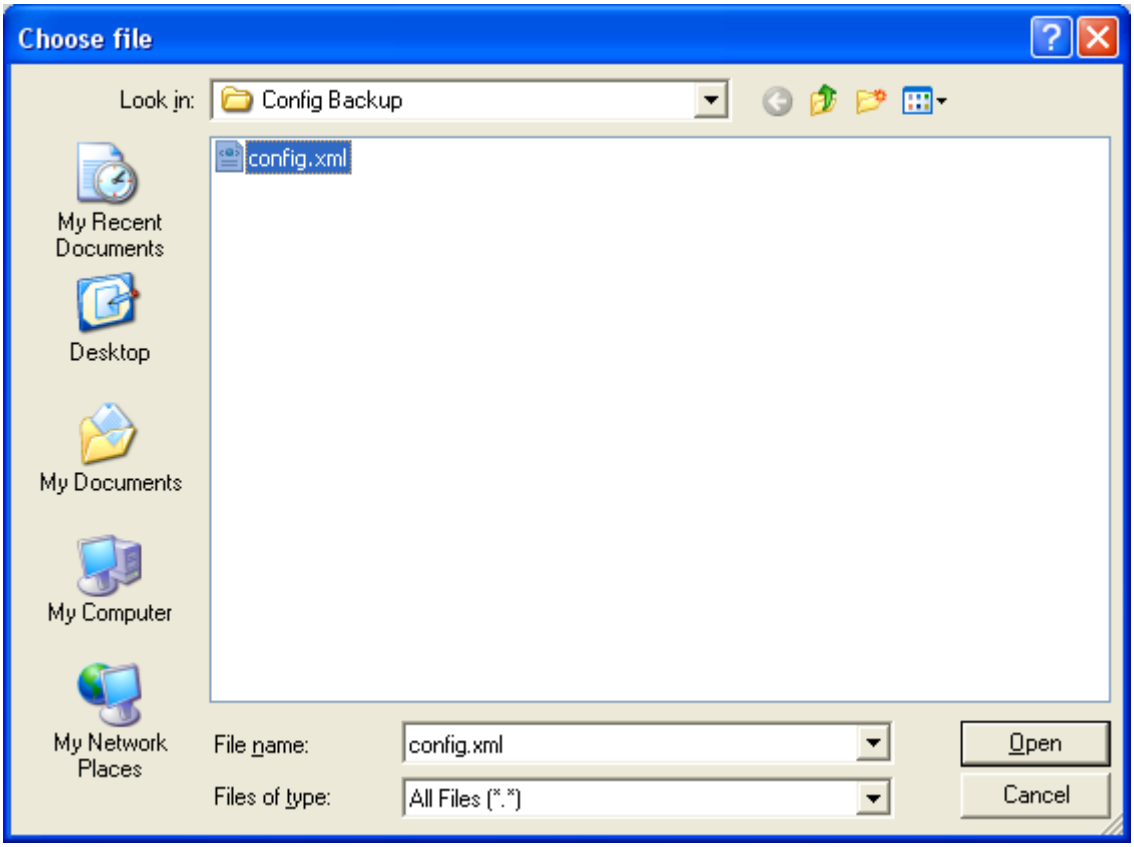


Figure 4-2-23 Windows file selection menu popup

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

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

4.2.17 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 4-2-24 appears.

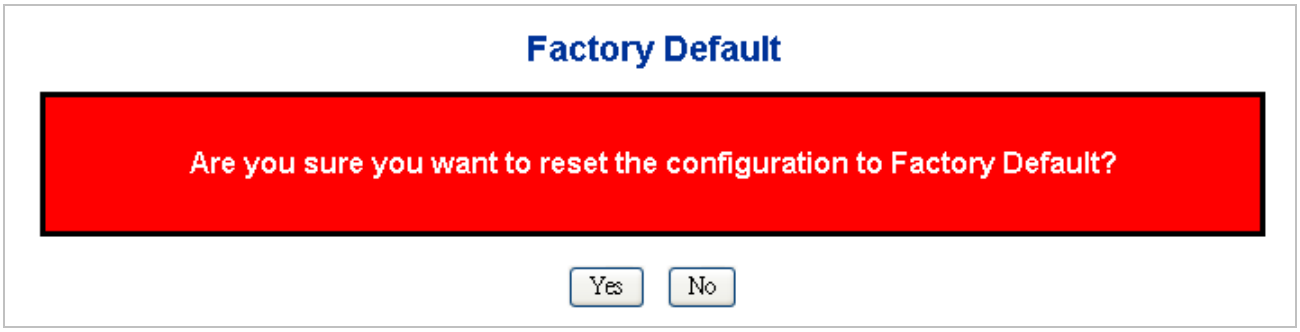


Figure 4-2-24 Factory Default page screenshot

Buttons

Yes: Click to reset the configuration to Factory Defaults.

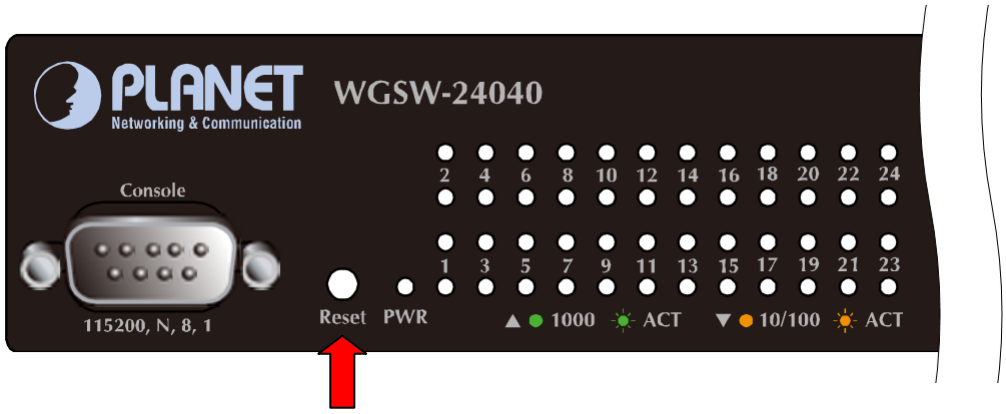
No: Click to return to the Port State page without resetting the configuration.

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

4.2.18 System Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user have to re-login the WEB interface about 60 seconds later, the System Reboot screen in Figure 4-2-25 appears.

Figure 4-2-26 System Reboot page screenshot

Buttons

Yes: Click to reboot the system.

No: Click to return to the Port State page without 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 blinking, then it is in the firmware load stage; if the SYS LED light on, you can use the WEB browser to login the Switch.

4.3 Simple Network Management Protocol

4.3.1 SNMP Overview

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

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

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

SNMP Operations

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

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

SNMP community

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

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

4.3.2 SNMP System Configuration

Configure SNMP on this page. The SNMP System Configuration screen in Figure 4-3-1 appears.

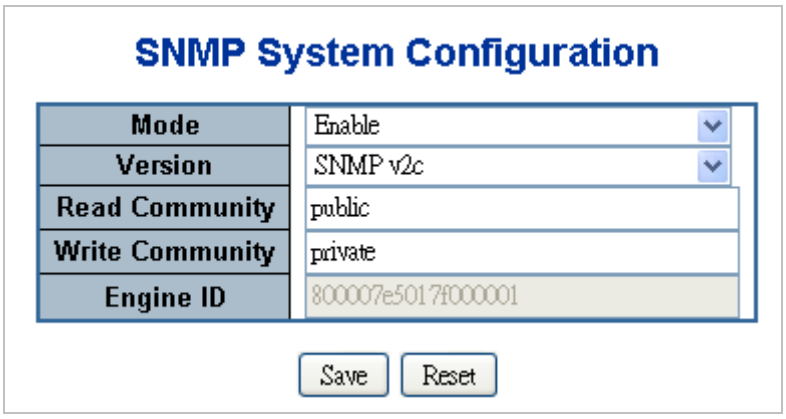


Figure 4-3-1 SNMP System Configuration page screenshot

The page includes the following fields:

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

Buttons

Save: Click to save changes.

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

4.3.3 SNMP System Information Configuration

The switch system information is provided here. The System Information Configuration screen in Figure 4-3-2 appears.

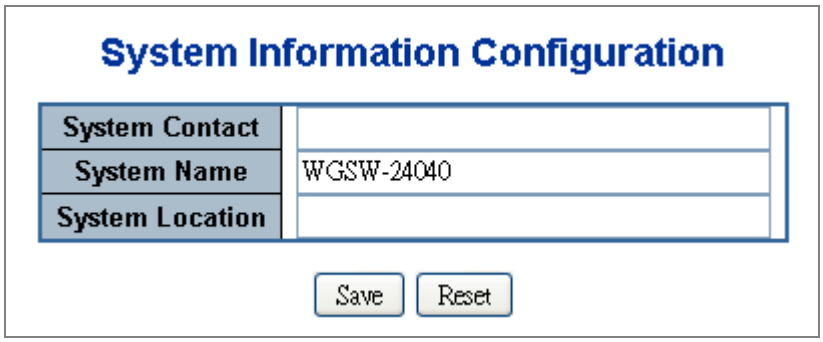


Figure 4-3-2 System Information Configuration page screenshot

The page includes the following fields:

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

Buttons

Save: Click to save changes.

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

4.3.4 SNMP Trap Configuration

Configure SNMP trap on this page. The SNMP Trap Configuration screen in Figure 4-3-3 appears.

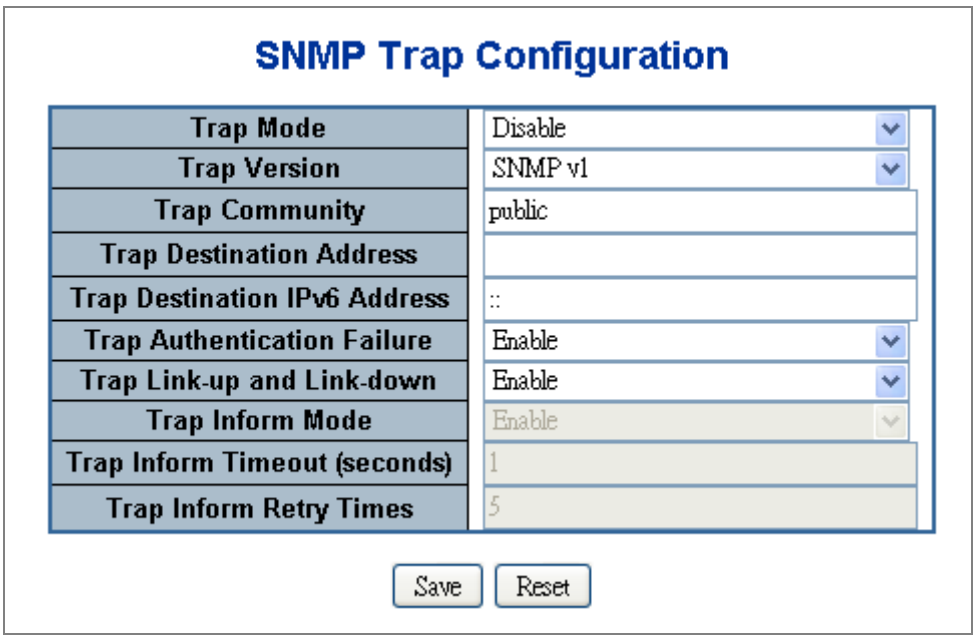


Figure 4-3-3 SNMP Trap Configuration page screenshot

The page includes the following fields:

Object	Description
• **Trap Mode**	Indicates the SNMP trap mode operation. Possible modes are: **Enabled**: Enable SNMP trap mode operation. **Disabled**: Disable SNMP trap mode operation.
• **Trap Version**	Indicates the SNMP trap supported version. Possible versions are: **SNMP v1**: Set SNMP trap supported version 1. **SNMP v2c**: Set SNMP trap supported version 2c. **SNMP v3**: Set SNMP trap supported version 3.
• **Trap Community**	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
• **Trap Destination Address**	Indicates the SNMP trap destination address.
• **Trap Destination IPv6 Address**	Provide the trap destination 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'.

• **Trap Authentication Failure**	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are: **Enabled**: Enable SNMP trap authentication failure. **Disabled**: Disable SNMP trap authentication failure.
• **Trap Link-up and Link-down**	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: **Enabled**: Enable SNMP trap link-up and link-down mode operation. **Disabled**: Disable SNMP trap link-up and link-down mode operation.
• **Trap Inform Mode**	Indicates the SNMP trap inform mode operation. Possible modes are: **Enabled**: Enable SNMP trap inform mode operation. **Disabled**: Disable SNMP trap inform mode operation.
• **Trap Inform Timeout (seconds)**	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
• **Trap Inform Retry Times**	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

Buttons

Save: Click to save changes.

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

4.3.5 SNMPv3 Configuration

4.3.5.1 SNMPv3 Communities Configuration

Configure SNMPv3 communities table on this page. The entry index key is Community. The SNMPv3 Communities Configuration screen in Figure 4-3-4 appears.

Figure 4-3-4 SNMPv3 Communities Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Community**	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Source IP**	Indicates the SNMP access source address.
• **Source Mask**	Indicates the SNMP access source address mask.

Buttons

Add new community: Click to add a new community entry.

Save: Click to save changes.

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

4.3.5.2 SNMPv3 Users Configuration

Configure SNMPv3 users table on this page. The entry index key are Engine ID and User Name. The SNMPv3 Users Configuration screen in Figure 4-3-5 appears.

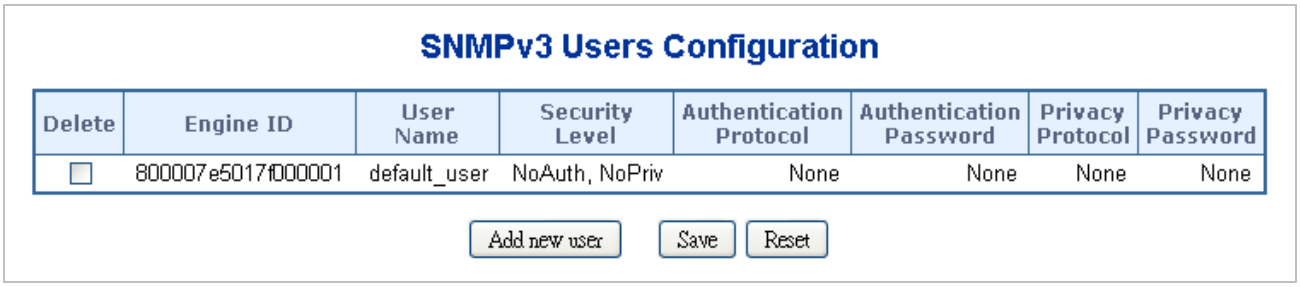


Figure 4-3-5 SNMPv3 Users Configuration page screenshot

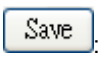
The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Engine ID**	A octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
• **User Name**	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33

	to 126.
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are: **NoAuth, NoPriv**: None authentication and none privacy. **Auth, NoPriv**: Authentication and none privacy. **Auth, Priv**: Authentication and privacy. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.
• **Authentication Protocol**	Indicates the authentication protocol that this entry should belong to. Possible authentication protocol are: **None**: None authentication protocol. **MD5**: An optional flag to indicate that this user using MD5 authentication protocol. **SHA**: An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.
• **Authentication Password**	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.
• **Privacy Protocol**	Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are: **None**: None privacy protocol. **DES**: An optional flag to indicate that this user using DES authentication protocol.
• **Privacy Password**	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

: Click to add a new user entry.



: Click to save changes.

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

4.3.5.3 SNMPv3 Groups Configuration

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

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

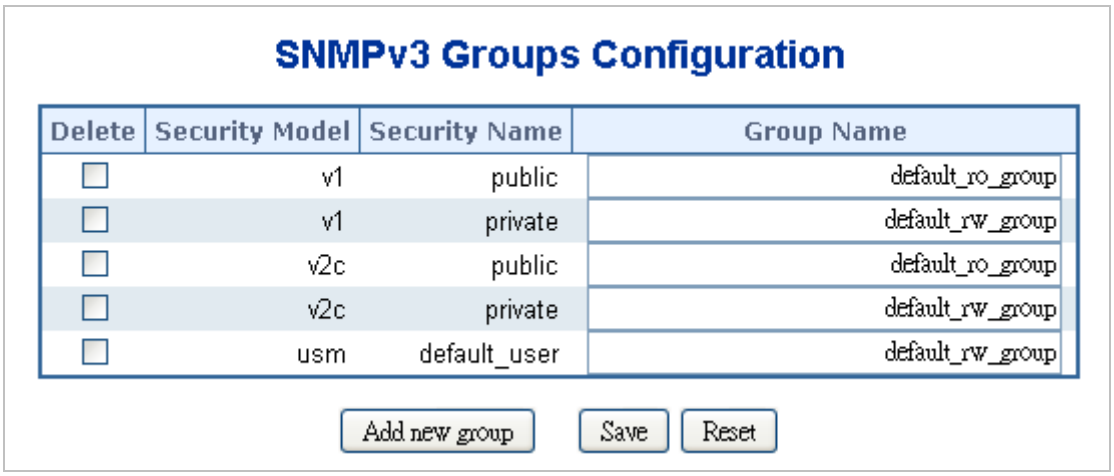


Figure 4-3-6 SNMPv3 Groups Configuration page screenshot

The page includes the following fields:

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

Buttons

Add new group: Click to add a new group entry.

Save: Click to save changes.

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

4.3.5.4 SNMPv3 Views Configuration

Configure SNMPv3 views table on this page. The entry index key are View Name and OID Subtree. The SNMPv3 Views Configuration screen in Figure 4-3-7 appears.

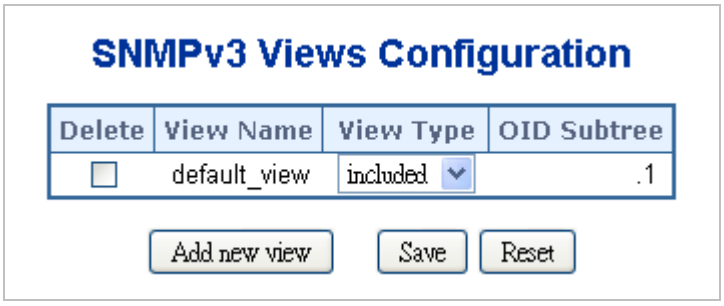


Figure 4-3-7 SNMPv3 Views Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **View Name**	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **View Type**	Indicates the view type that this entry should belong to. Possible view type are: **included**: An optional flag to indicate that this view subtree should be included. **excluded**: An optional flag to indicate that this view subtree should be excluded. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.
• **OID Subtree**	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

Add new view: Click to add a new view entry.

Save: Click to save changes.

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

4.3.5.5 SNMPv3 Accesses Configuration

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

The SNMPv3 Accesses Configuration screen in Figure 4-3-8 appears.

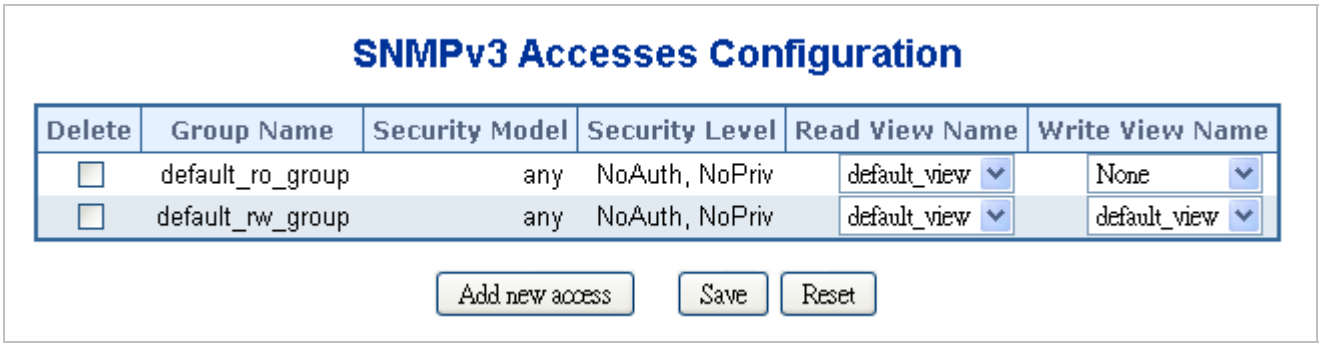


Figure 4-3-8 SNMPv3 Accesses Configuration page screenshot

The page includes the following fields:

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

Buttons

Add new access: Click to add a new access entry.

Save: Click to save changes.

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

4.4 Port Management

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

■ **Port Configuration**	Configures port connection settings
■ **Port Statistics Overview** ■ **Port Statistics Detail**	Lists Ethernet and RMON port statistics
■ **SFP Module Information**	Display SFP information
■ **Port Mirror**	Sets the source and target ports for mirroring

4.4.1 Port Configuration

This page displays current port configurations. Ports can also be configured here. The port settings relate to the currently selected stack unit, as reflected by the page header. The table has one row for each port on the selected switch in the stack and a number of columns, which are:

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

Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
1		Down	Auto	✗	✗	☐	9600	Discard	Enable
2		Down	Auto	✗	✗	☐	9600	Discard	Enable
3		Down	Auto	✗	✗	☐	9600	Discard	Enable
4		Down	Auto	✗	✗	☐	9600	Discard	Enable
5		Down	Auto	✗	✗	☐	9600	Discard	Enable
6		Down	Auto	✗	✗	☐	9600	Discard	Enable
7		Down	Auto	✗	✗	☐	9600	Discard	Enable
8		Down	Auto	✗	✗	☐	9600	Discard	Enable
9		Down	Auto	✗	✗	☐	9600	Discard	Enable
10		Down	Auto	✗	✗	☐	9600	Discard	Enable
11		Down	Auto	✗	✗	☐	9600	Discard	Enable
12		Down	Auto	✗	✗	☐	9600	Discard	Enable
13		Down	Auto	✗	✗	☐	9600	Discard	Enable
14		Down	Auto	✗	✗	☐	9600	Discard	Enable
15		Down	Auto	✗	✗	☐	9600	Discard	Enable
16		Down	Auto	✗	✗	☐	9600	Discard	Enable
17		Down	Auto	✗	✗	☐	9600	Discard	Enable
18		1Gfdx	Auto	✗	✗	☐	9600	Discard	Enable
19		Down	Auto	✗	✗	☐	9600	Discard	Enable
20		Down	Auto	✗	✗	☐	9600	Discard	Enable
21		Down	Auto	✗	✗	☐	9600	Discard	Enable
22		Down	Auto	✗	✗	☐	9600	Discard	Enable
23		Down	Auto	✗	✗	☐	9600	Discard	Enable
24		1Gfdx	Auto	✗	✗	☐	9600	Discard	Enable

Save Reset Refresh

Figure 4-4-1 Port Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	This is the logical port number for this row.
• **Link**	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
• **Current Link Speed**	Provides the current link speed of the port.
• **Configured Link Speed**	Select any available link speed for the given switch port. Draw the menu bar to select the mode. **Auto Speed** - Setup Auto negotiation. **10 Half** - Force sets 10Mbps/Half-Duplex mode. **10 Full** - Force sets 10Mbps/Full-Duplex mode. **100 Half** - Force sets 100Mbps/Half-Duplex mode. **100 Full** - Force sets 100Mbps/Full-Duplex mode. **1000 Full** - Force sets 10000Mbps/Full-Duplex mode. **Disable** - Shutdown the port manually.
• **Flow Control**	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. Current Rx column indicates whether pause frames on the port are obeyed. Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
• **Maximum Frame**	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
• **Excessive Collision Mode**	Configure port transmit collision behavior. **Discard**: Discard frame after 16 collisions (default). **Restart**: Restart back off algorithm after 16 collisions.
• **Power Control**	The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port. **Disabled**: All power savings mechanisms disabled. **ActiPHY**: Link down power savings enabled. **Dynamic**: Link up power savings enabled. **Enabled**: Link up and link down power savings enabled.

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

Buttons

Save: Click to save changes.

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

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

4.4.2 Port Statistics Overview

This page provides an overview of general traffic statistics for all switch ports. The ports belong to the currently selected stack unit, as reflected by the page header. The Port Statistics Overview screen in Figure 4-4-2 appears.

Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	6256	1990	1107870	403195	1	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	5397	14630	1169942	4244397	1	0	0	0	12

Auto Refresh ☐ Refresh Clear

Figure 4-4-2 Port Statistics Overview page screenshot

The displayed counters are:

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

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

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

4.4.3 Port Statistics Detail

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The selected port belong to the currently selected stack unit, as reflected by the page header. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. The Detailed Port Statistics screen in Figure 4-4-3 appears.

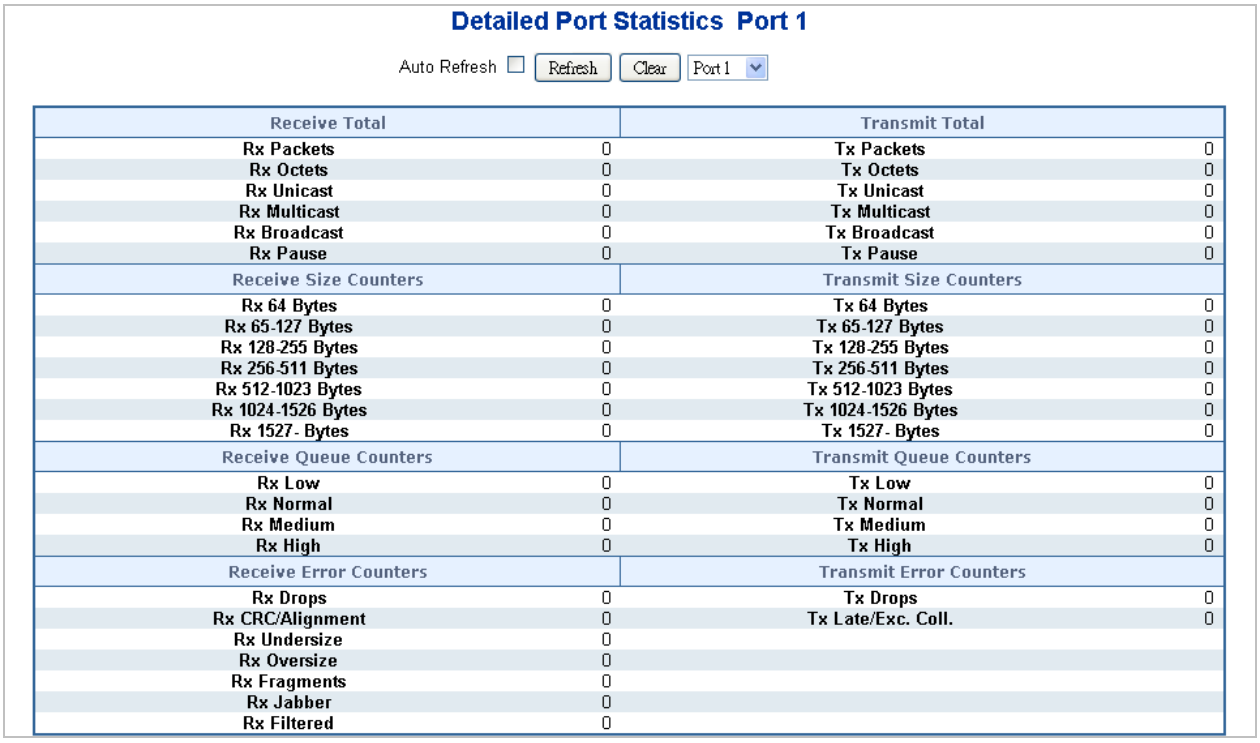


Figure 4-4-3 Detailed Port Statistics Port 1 page screenshot

The page includes the following fields:

Receive Total and Transmit Total

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

Receive and Transmit Size Counters

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

Receive and Transmit Queue Counters

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

Receive Error Counters

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

Transmit Error Counters

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

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

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

4.4.4 SFP Module Information

You can check the physical or operational status of an SFP module via the SFP Module Information page. This page shows the operational status, such as the transceiver type, speed, wavelength and supports distance of SFP module on a specific interface. You can also use the hyperlink of port no. to check the statistics on an speficic interface. The SFP Module Information screen in Figure 4-4-4 appears.

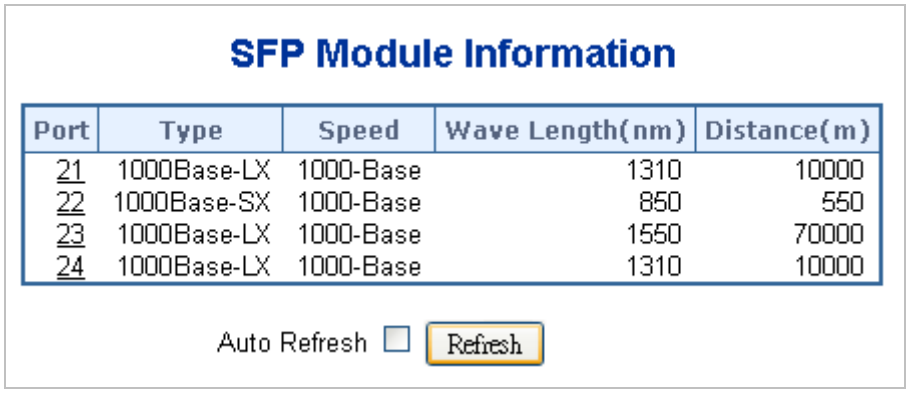


Figure 4-4-4 SFP Module Information for Switch page screenshot

The page includes the following fields:

Object	Description
• **Type**	Display the type of current SFP module, the possible types are: ■ 1000Base-SX ■ 1000Base-LX ■ 100Base-FX

• **Speed**	Display the spedd of current SFP module, the speed value or description is get from the SFP module. Different vendors SFP modules might shows different speed information.
• **Wave Length(nm)**	Display the wavelength of current SFP module, the wavelength value is get from the SFP module. Use this column to check if the wavelength values of two nodes are the matched while the fiber connection is failed.
• **Distance(m)**	Display the supports distance of current SFP module, the distance value is get from the SFP module.

Buttons

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

Refresh: Click to refresh the page immediately.

4.4.5 Port Mirroring Configuration

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

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

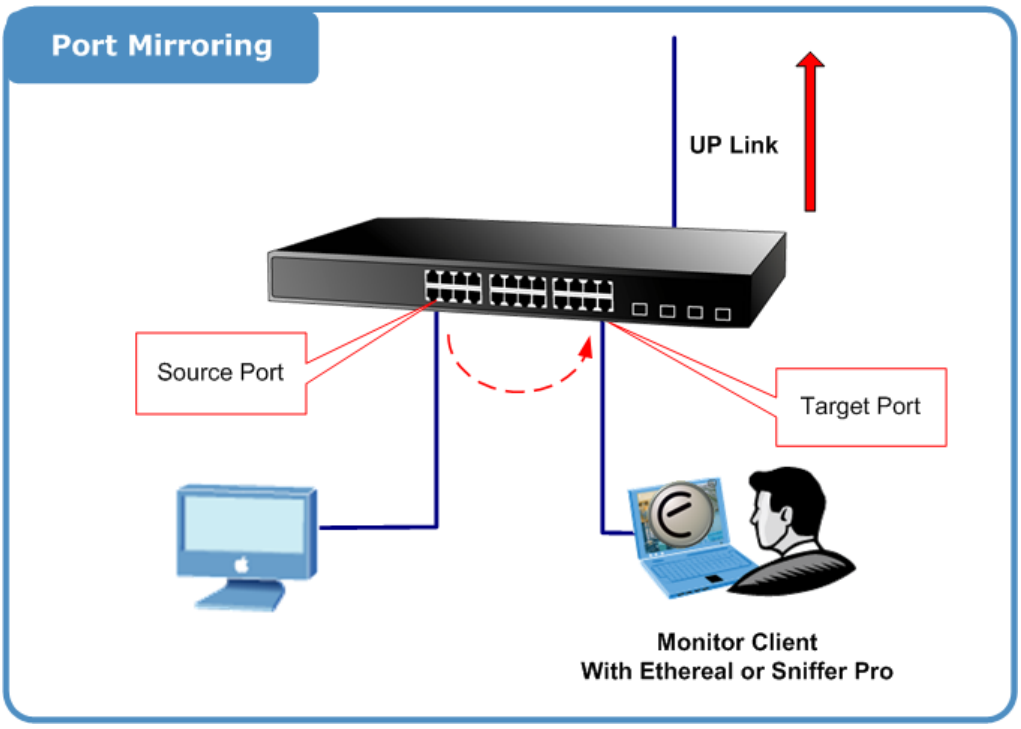


Figure 4-4-5 Port Mirror application

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

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

Mirror Port Configuration

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

Figure 4-4-6 Port Mirror Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port to mirror to**	Frames from ports that have either source or destination mirroring enabled are mirrored to this port. Disabled disables mirroring.
• **Port**	The logical port for the settings contained in the same row.
• **Mode**	Select mirror mode.

	Rx only: Frames received at this port are mirrored to the mirroring port. Frames transmitted are not mirrored.
	Tx only: Frames transmitted from this port are mirrored to the mirroring port. Frames received are not mirrored.
	Disabled: Neither frames transmitted or frames received are mirrored.
	Enabled: Frames received and frames transmitted are mirrored to the mirror port.

Buttons

Save: Click to save changes.

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

4.5 Link Aggregation

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

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

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

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

The device supports the following Aggregation links :

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

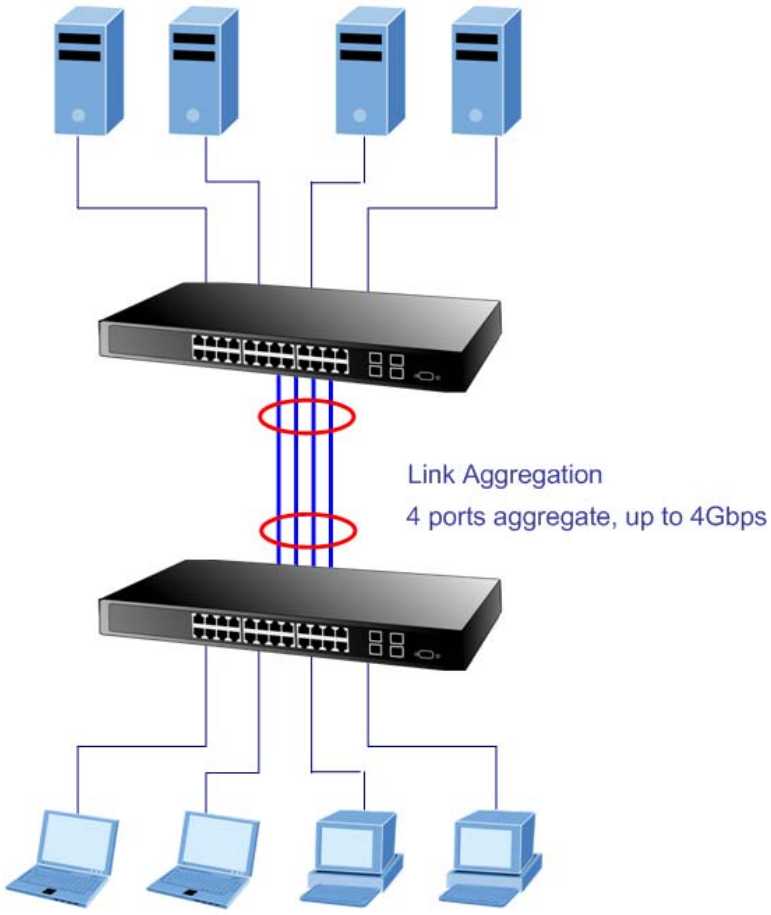


Figure 4-5-1 Link Aggregation

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

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

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

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

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

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

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

4.5.1 Static Aggregation Configuration

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

Hash Code Contributors

The Aggeration Mode COnfiguration screen in Figure 4-5-2 appears.

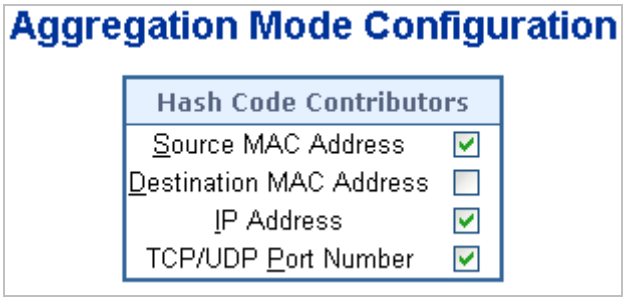


Figure 4-5-2 Aggregation Mode Configuration page screenshot

The page includes the following fields:

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

Static Aggregation Group Configuration

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

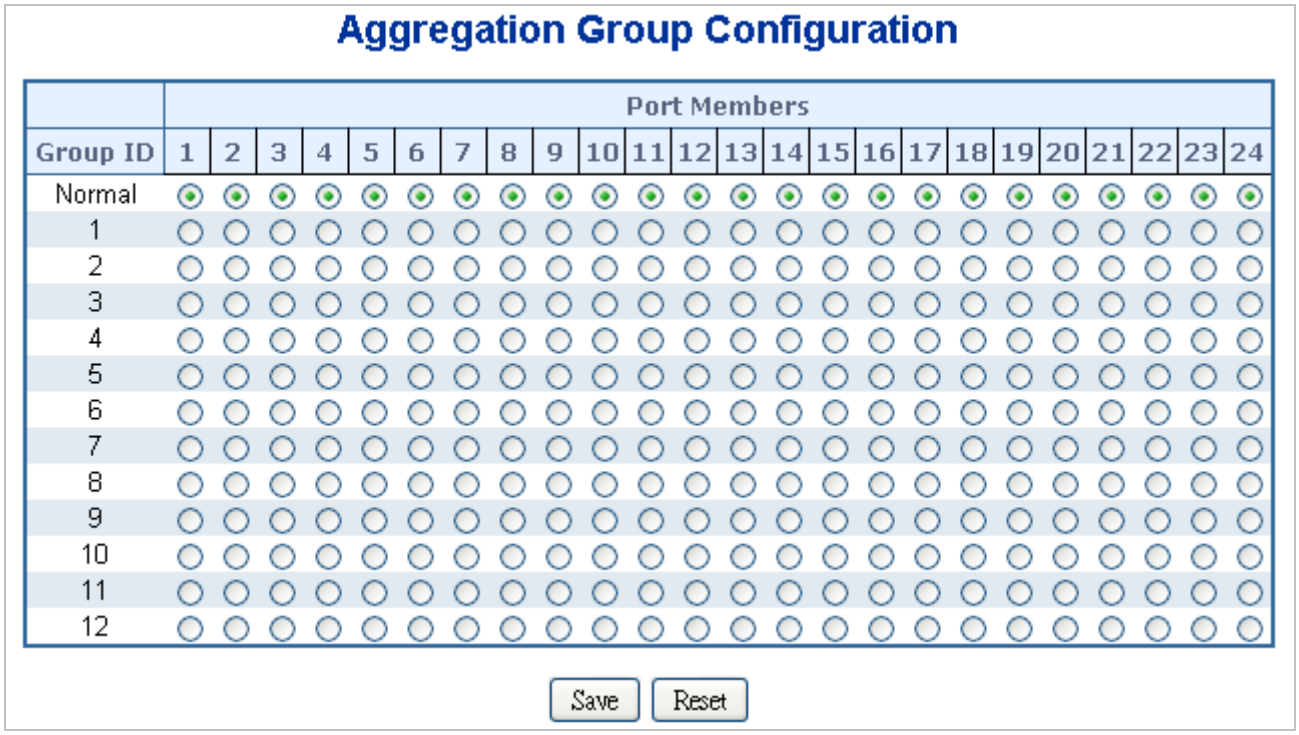


Figure 4-5-3 Aggregation Group Configuration page screenshot

The page includes the following fields:

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

Buttons

Save: Click to save changes.

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

4.5.2 LACP Configuration

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

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

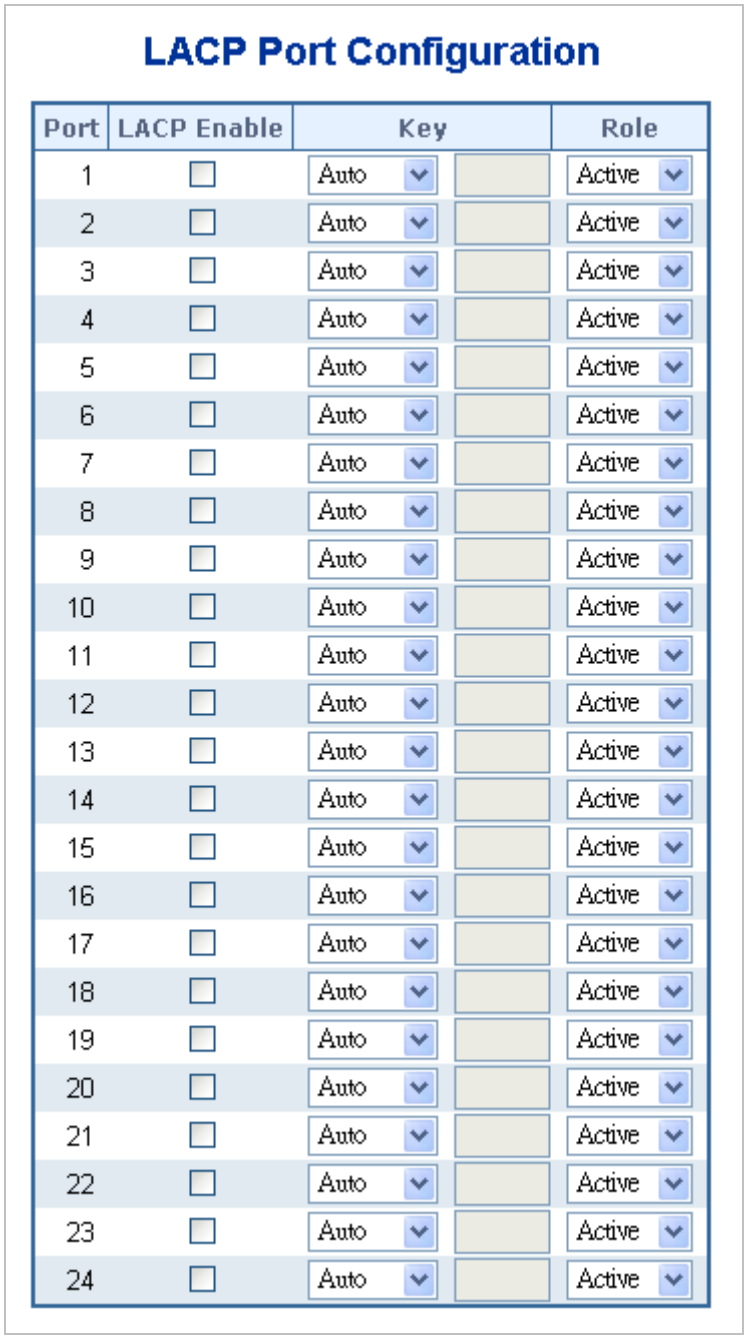


Figure 4-5-4 LACP Port Configuration page screenshot

The page includes the following fields:

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

Buttons

Save: Click to save changes.

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

4.5.3 LACP System Status

This page provides a status overview for all LACP instances. The LACP Status page display the current LACP aggregation Groups and LACP Port status . The LACP System Status screen in Figure 4-5-5 appears.

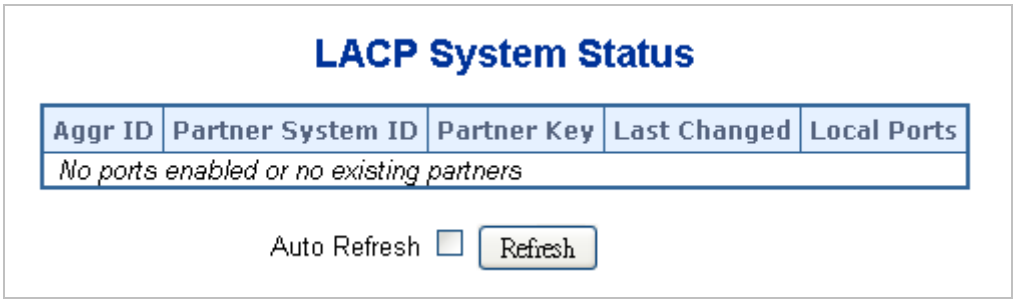


Figure 4-5-5 LACP System Status page screenshot

The page includes the following fields:

Object	Description
• **Aggr ID**	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
• **Partner System ID**	The system ID (MAC address) of the aggregation partner.

• **Partner Key**	The Key that the partner has assigned to this aggregation ID.
• **Last changed**	The time since this aggregation changed.
• **Local Ports**	Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".

4.5.4 LACP Port Status

This page provides a status overview for LACP status for all ports. The LACP Port Status screen in Figure 4-5-6 appears.

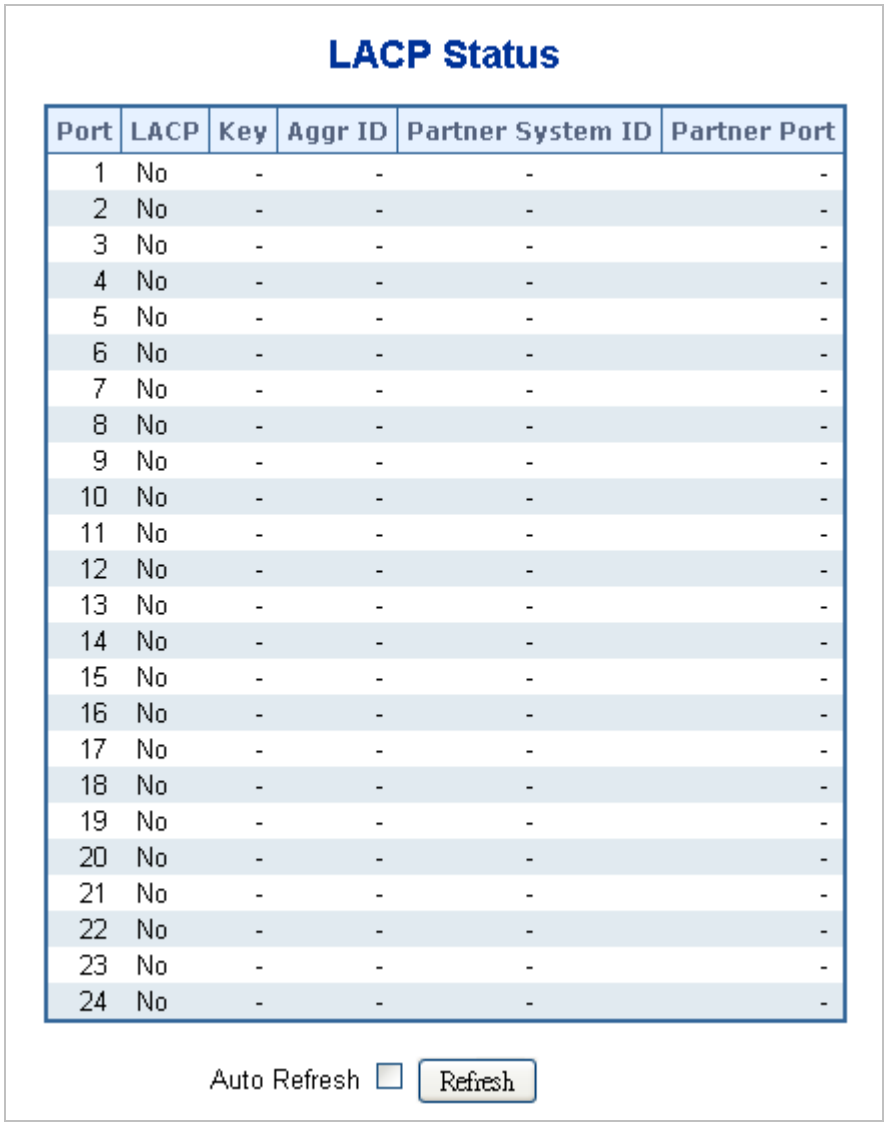


Figure 4-5-6 LACP Port Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.

• **LACP**	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
• **Key**	The key assigned to this port. Only ports with the same key can aggregate together.
• **Aggr ID**	The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
• **Partner System ID**	The partners System ID (MAC address).
• **Partner Port**	The partners port number connected to this port.

4.5.5 LACP statistics

This page provides an overview for LACP statistics for all ports. The LACP statistics screen in Figure 4-5-7 appears.

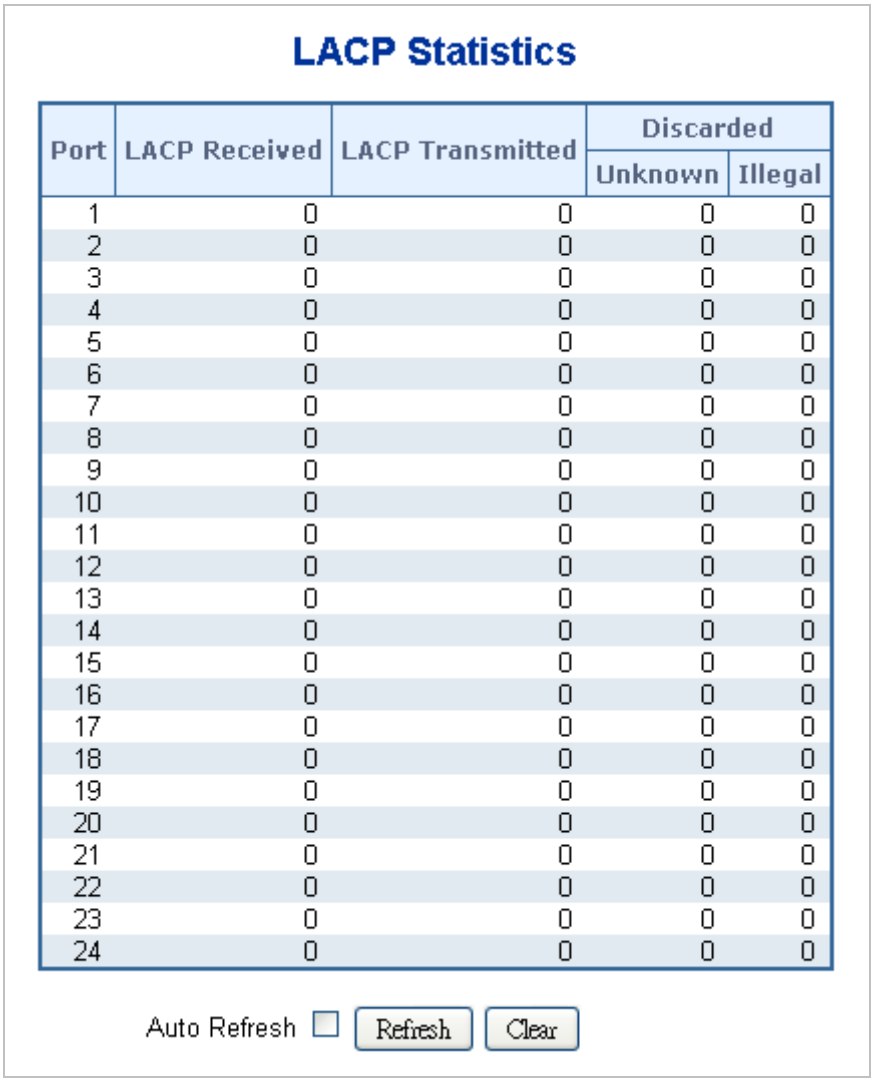


Figure 4-5-7 LACP Port statistics page screenshot

The page includes the following fields:

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

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

4.6 VLAN

4.6.1 VLAN Overview

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

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

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

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
2. The Managed Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.
3. The Switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_ VLAN port member list. The DEFAULT_VLAN has a VID = 1.

This section has the following items:

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

4.6.2 IEEE 802.1Q VLAN

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

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

to the same physical segment.

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

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

This Managed Switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

IEEE 802.1Q Standard

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

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

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

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

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.

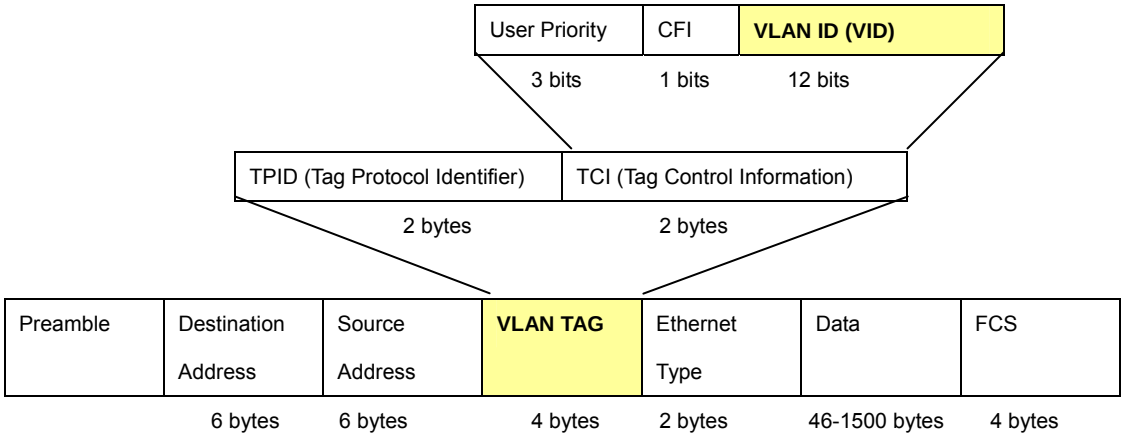
802.1Q VLAN Tags

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.

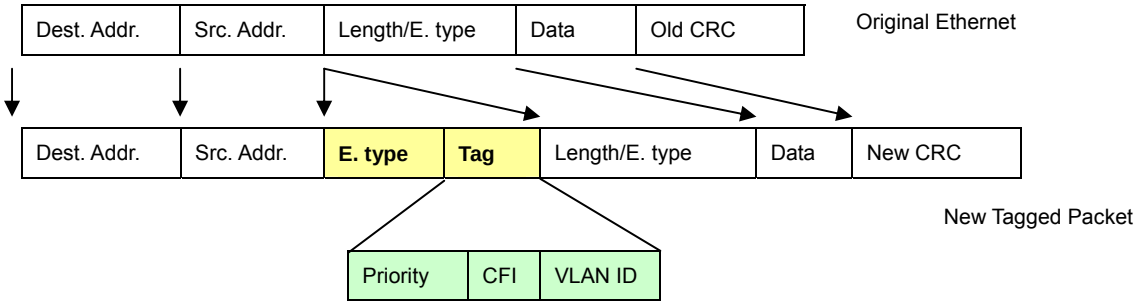
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

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.

4.6.3 VLAN Basic Information

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

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

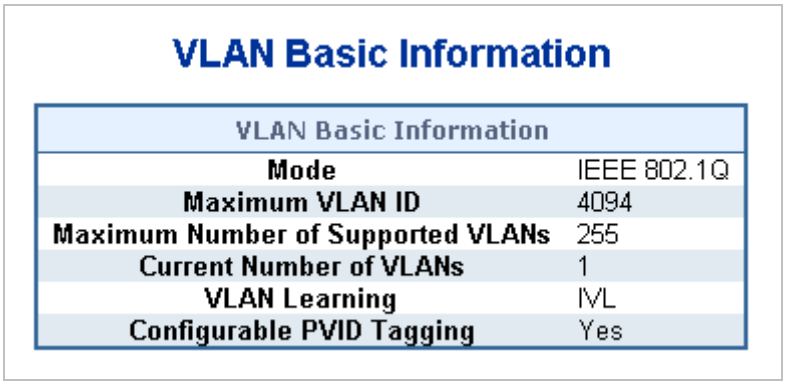


Figure 4-6-1 VLAN Basic Information page screenshot

The page includes the following fields:

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

4.6.4 VLAN Port Configuration

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

Understand nomenclature of the Switch

IEEE 802.1Q Tagged and Untagged

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

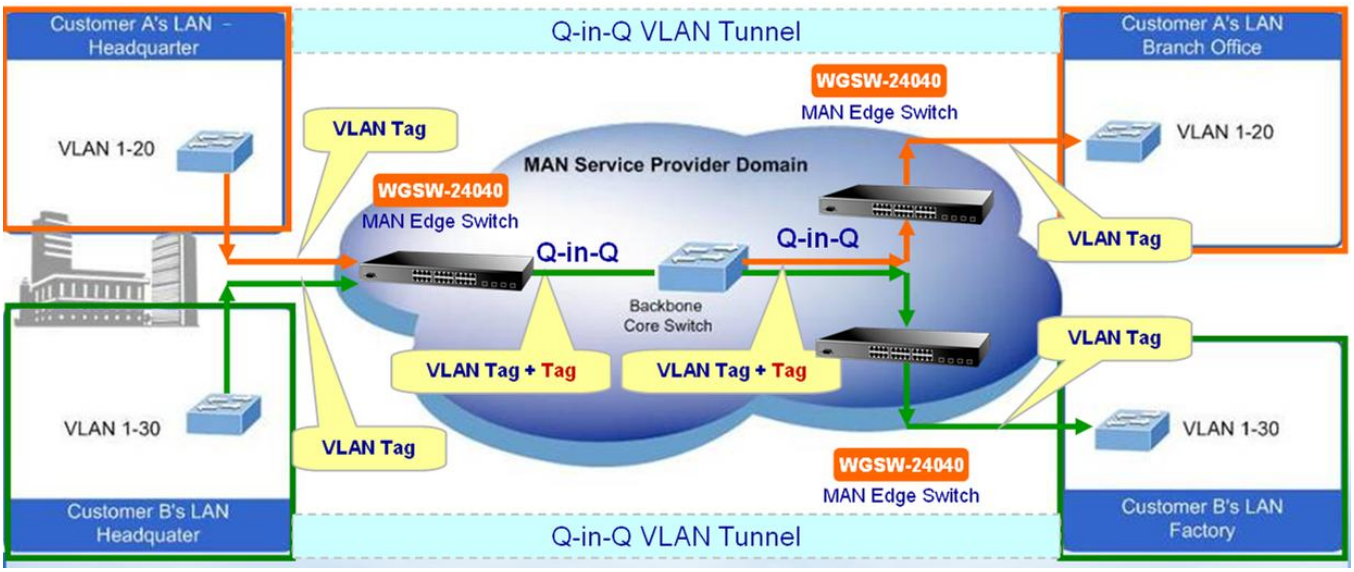
- **Tagged:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in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

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

IEEE 802.1Q Tunneling (Q-in-Q)

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

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



The Managed Switch supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

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

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

VLAN Port Configuration

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

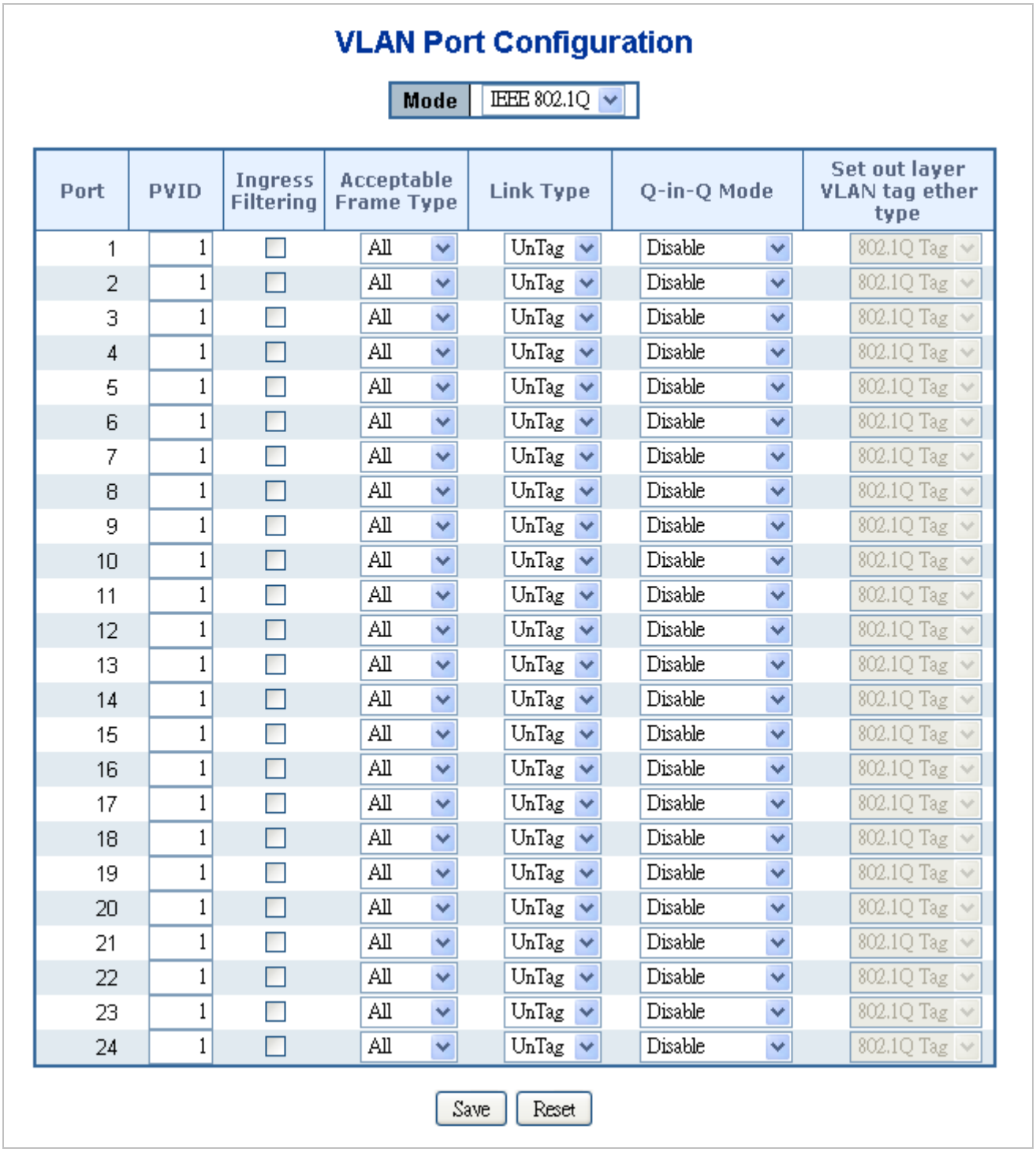


Figure 4-6-2 VLAN Port Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	This is the logical port number for this row.
• **PVID**	Allow assign PVID for selected port. The range for the PVID is 1-4094. The PVID will be inserted into all untagged frames entering the ingress port. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the

	untagged traffic will be dropped.
Ingress Filtering	Enable ingress filtering for a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).
• **Accept Frame Type**	Determines whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.
• **Link Type**	Allow 802.1Q Untagged or Tagged VLAN for selected port. When adding a VLAN to selected port, it tells the switch whether to keep or remove the tag from a frame on egress. **Untag**: outgoing frames without VLAN-Tagged. **Tagged**: outgoing frames with VLAN-Tagged.
• **Q-in-Q Mode**	Sets the Managed Switch to QinQ mode, and allows the QinQ tunnel port to be configured. The default is for the Managed Switch to function in Disable mode. **Disable**: The port operates in its normal VLAN mode. (This is the default.) **MAN Port**: Configures IEEE 802.1Q tunneling (QinQ) for an uplink port to another device within the service provider network. **Customer Port**: Configures IEEE 802.1Q tunneling (QinQ) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
Set Out layer VLAN tag ether type	The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel access port. **802.1Q Tag**: 8100 **vMAN Tag**: 88A8 Default : 802.1Q Tag

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

Buttons

Save: Click to save changes.

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

4.6.5 VLAN Membership Configuration

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

Use the VLAN Static Table to configure port members for the selected VLAN index. The VLAN membership configuration for the selected stack switch / unit switch can be monitored and modified here. Up to 255 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN. The VLAN Membership Configuration screen in Figure 4-6-3 appears.

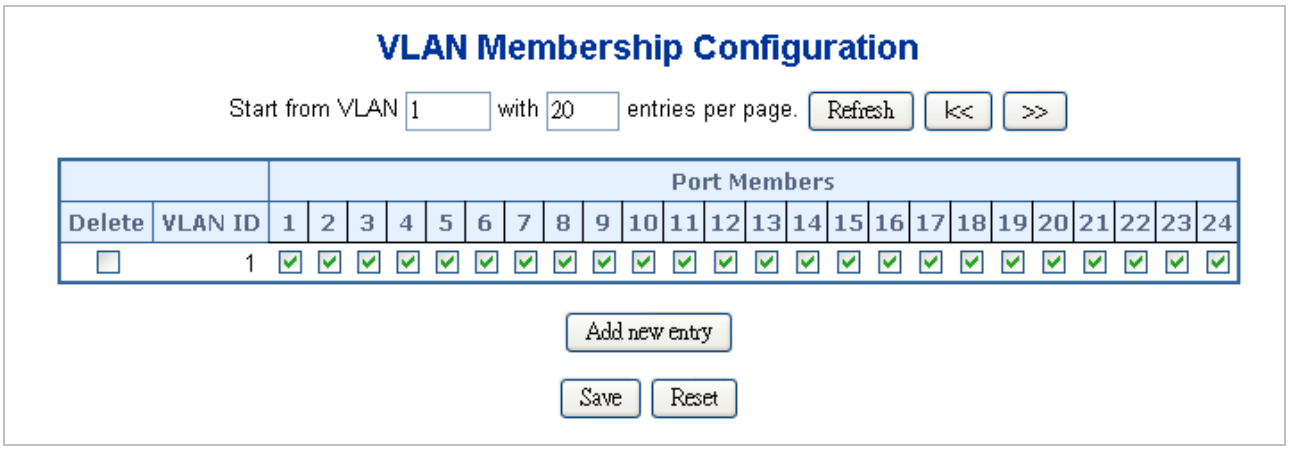


Figure 4-6-3 VLAN Membership Configuration page screenshot

The page includes the following fields:

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

Buttons

Add new entry: Click to add new VLAN.

Save: Click to save changes.

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

Refresh: Refreshes the displayed table starting from the "VLAN ID" input fields.

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

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

4.6.6 VLAN Membership Status for User Static

This page provides an overview of membership status for VLAN users. The VLAN Membership Status for User Static screen in Figure 4-6-4 appears.

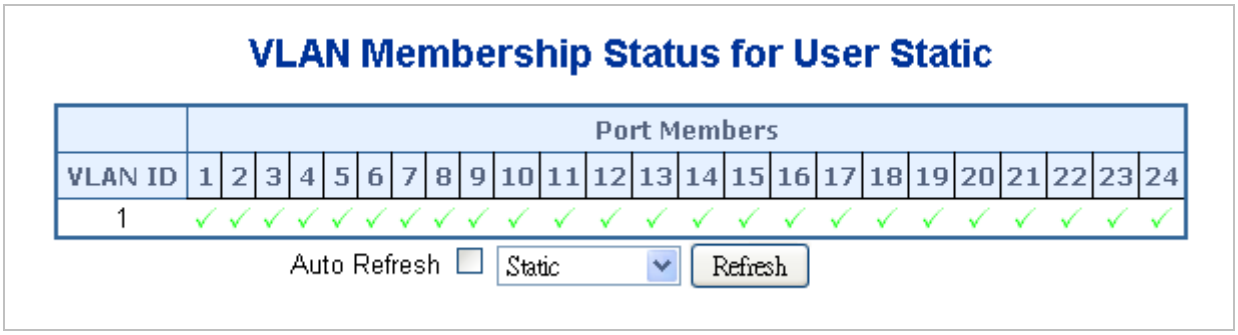


Figure 4-6-4 VLAN Membership Status for User Static page screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Indicates the ID of this particular VLAN.
• **Port Members**	The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users is selected, it shall show this information for all the VLAN Users, and this is the default. VLAN membership allows the frames Classified to the VLAN ID to be forwarded to the respective VLAN member ports.
• **VLAN User**	A VLAN User is a module that uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN : **CLI/Web/SNMP** : This are reffered as static. **NAS** : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server. **Voice VLAN** : Voice VLAN is a VLAN configured specially for voice traffic

	typically originating from IP phones. **MVR** : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN. **MSTP** : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

Buttons

Static : Select VLAN Users from this drop down list.

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

Refresh : Click to refresh the page immediately.

4.6.7 VLAN Port Status for User Static

This page provides VLAN Port Staus. The VLAN Port Status for User Static screen in Figure 4-6-5 appears.

VLAN Port Status for User Static

Port	PVID	VLAN Aware	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	Disabled	Disabled	All	Untag_this	1	No
2	1	Disabled	Disabled	All	Untag_this	1	No
3	1	Disabled	Disabled	All	Untag_this	1	No
4	1	Disabled	Disabled	All	Untag_this	1	No
5	1	Disabled	Disabled	All	Untag_this	1	No
6	1	Disabled	Disabled	All	Untag_this	1	No
7	1	Disabled	Disabled	All	Untag_this	1	No
8	1	Disabled	Disabled	All	Untag_this	1	No
9	1	Disabled	Disabled	All	Untag_this	1	No
10	1	Disabled	Disabled	All	Untag_this	1	No
11	1	Disabled	Disabled	All	Untag_this	1	No
12	1	Disabled	Disabled	All	Untag_this	1	No
13	1	Disabled	Disabled	All	Untag_this	1	No
14	1	Disabled	Disabled	All	Untag_this	1	No
15	1	Disabled	Disabled	All	Untag_this	1	No
16	1	Disabled	Disabled	All	Untag_this	1	No
17	1	Disabled	Disabled	All	Untag_this	1	No
18	1	Disabled	Disabled	All	Untag_this	1	No
19	1	Disabled	Disabled	All	Untag_this	1	No
20	1	Disabled	Disabled	All	Untag_this	1	No
21	1	Disabled	Disabled	All	Untag_this	1	No
22	1	Disabled	Disabled	All	Untag_this	1	No
23	1	Disabled	Disabled	All	Untag_this	1	No
24	1	Disabled	Disabled	All	Untag_this	1	No

Auto Refresh Static Refresh

Figure 4-6-5 VLAN Port Status for User Static page screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **PVID**	Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.
• **VLAN Aware**	Show the VLAN Awareness for the port. If VLAN awareness is enabled, the tag is removed from tagged frames received on the port. VLAN tagged frames are classified to the VLAN ID in the tag. If VLAN awareness is disabled, all frames are classified to the Port VLAN ID and tags are not removed.
• **Ingress Filtering**	Show the ingress filtering for a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded.
• **Frame Type**	Shows 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 that port are discarded.
• **Tx Tag**	Shows egress filtering frame status whether tagged or untagged.
• **UVID**	Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.
• **Conflicts**	Shows status of Conflicts whether exists or Not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur: Functional Conflicts between feature. Conflicts due to hardware limitation. Direct conflict between user modules.
• **VLAN User**	A VLAN User is a module that uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN : **CLI/Web/SNMP** : This are reffered as static. **NAS** : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server. **Voice VLAN** : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones. **MVR** : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN. **MSTP** : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network

	resource utilization while maintaining a loop-free environment.

Buttons

Static: Select VLAN Users from this drop down list.

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

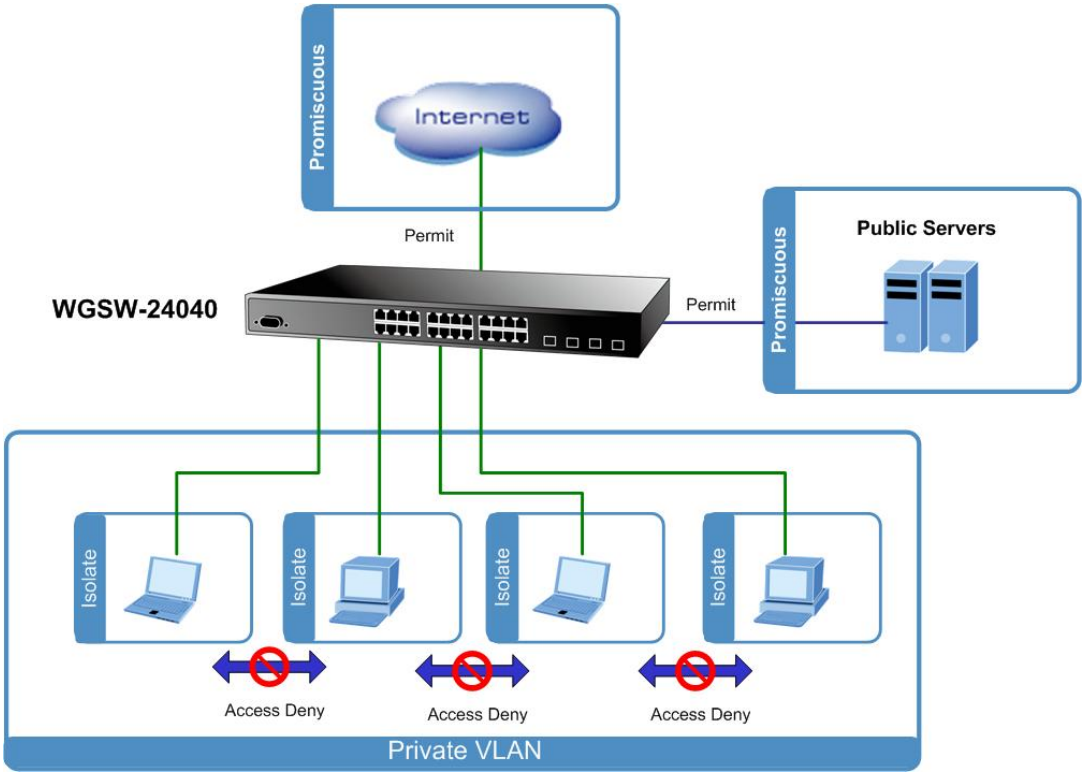
Refresh: Click to refresh the page immediately.

4.6.8 Port Isolation Configuration

Overview

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

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



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

- **Promiscuous ports**
  - — Ports from which traffic can be forwarded to all ports in the private VLAN
  - — Ports which can receive traffic from all ports in the private VLAN
- **Isolated ports**
  - — Ports from which traffic can only be forwarded to 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 4-6-6 appears.

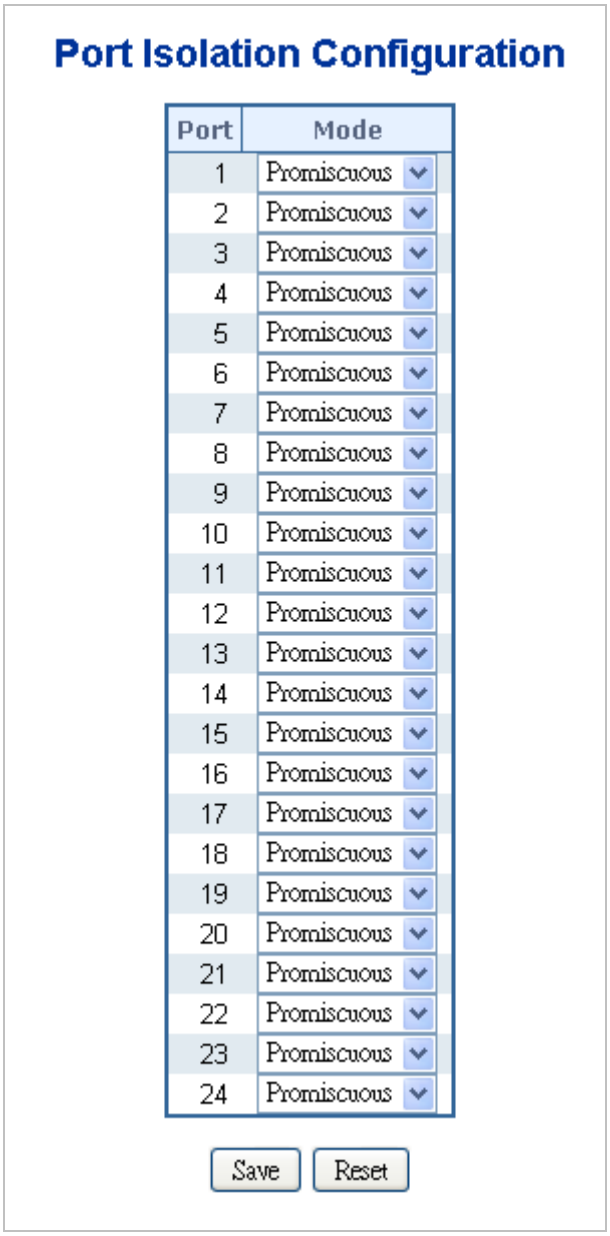


Figure 4-6-6 Port Isolation Configuration page screenshot

The page includes the following fields:

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

Buttons

Save: Click to save changes.

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

4.6.9 Private VLAN Membership Configuration

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs. The Private VLAN Membership Configuration screen in Figure 4-6-7 appears.

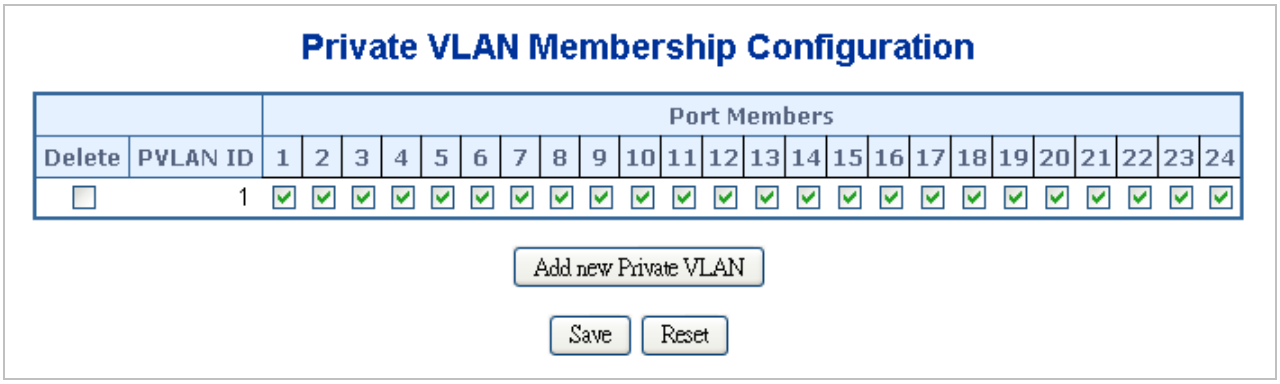


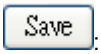
Figure 4-6-7 Private VLAN Membership Configuration page screenshot

The page includes the following fields:

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

Buttons

: Click to add new VLAN.



: Click to save changes.

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

4.7 Spanning Tree Protocol

4.7.1 Theory

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

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

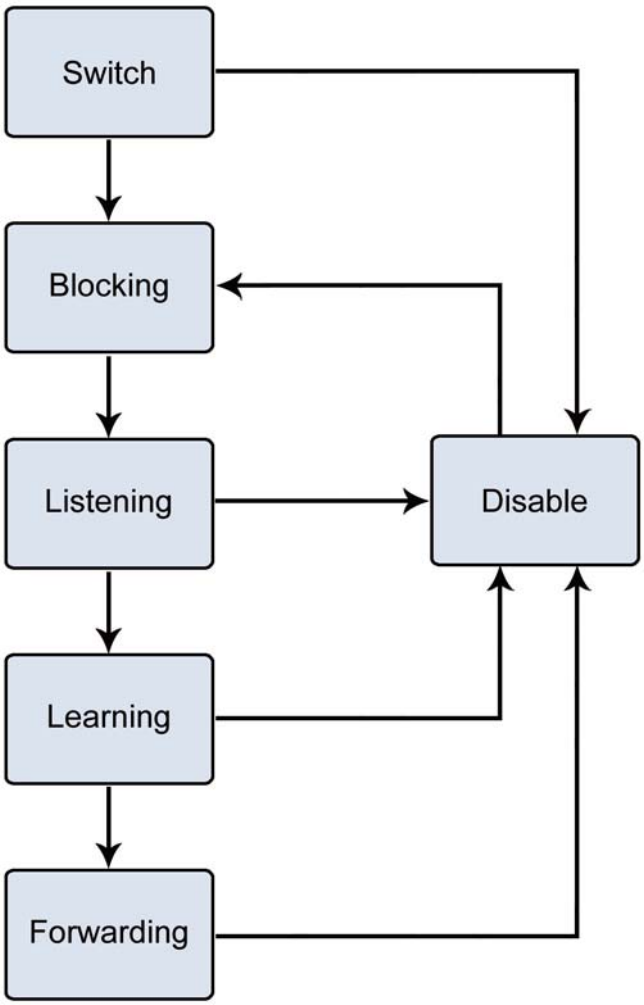


Figure 4-7-1 STP Port State Transitions

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

2. STP Parameters

STP Operation Levels

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

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

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

Parameter	Description	Default Value
Bridge Identifier(Not user configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	32768 + MAC
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

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

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

Default Spanning-Tree Configuration

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

User-Changeable STA Parameters

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

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

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

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.

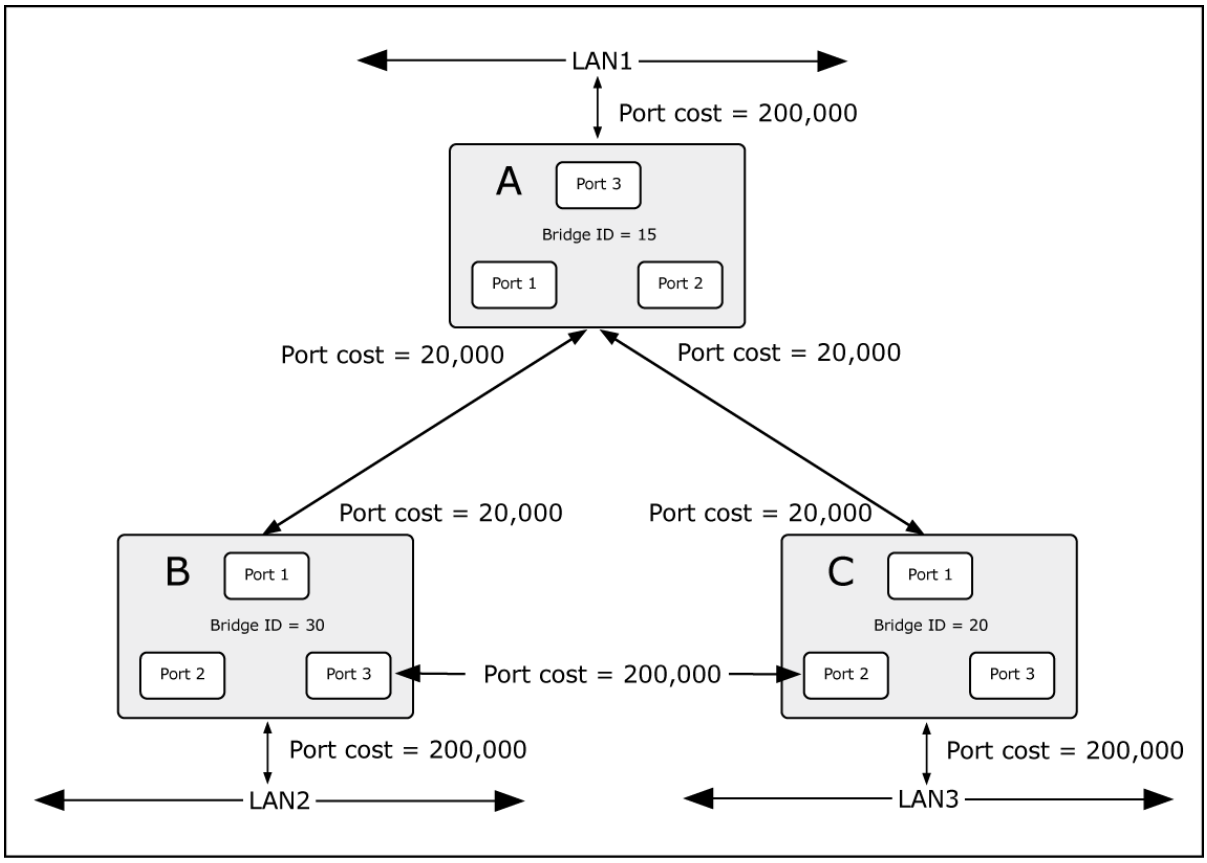


Figure 4-7-5 Before Applying the STA Rules

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

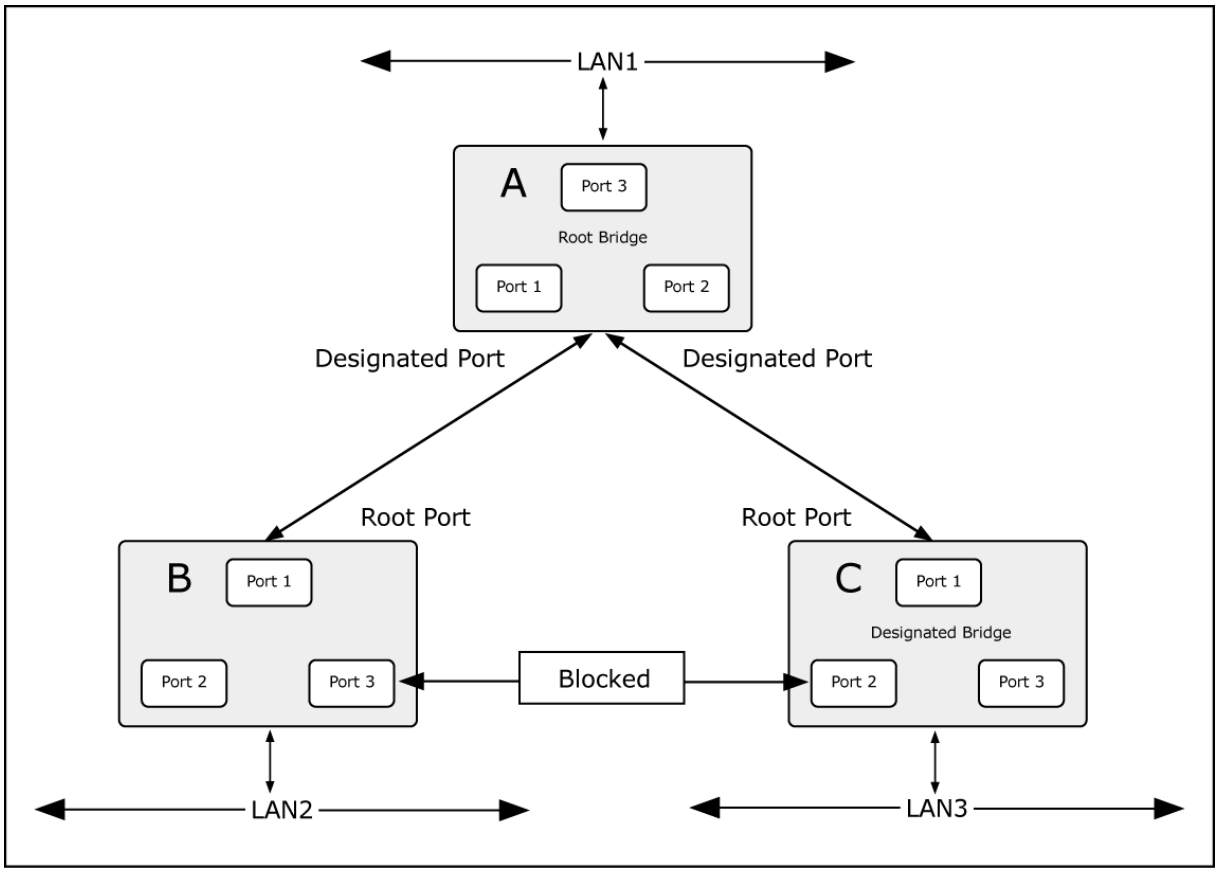


Figure 4-7-6 After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 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.

4.7.2 STP Bridge Configuration

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 Bridge Configuration screen in Figure 4-7-7 appears.

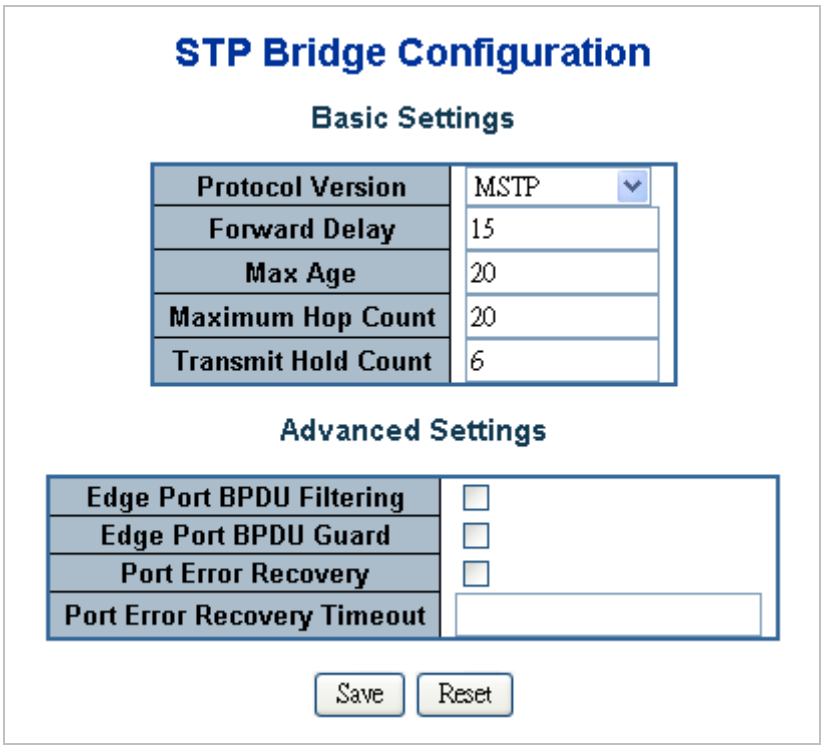


Figure 4-7-7 STP Bridge Configuration page screenshot

The page includes the following fields:

Basic Settings

Object	Description
• **Protocol Version**	The STP protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**.
• **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)]
• **Maximum Hop Count**	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.
• **Transmit 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.

Advanced Settings

Object	Description
• **Edge Port BPDU Filtering**	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
• **Edge Port 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.
• **Port Error Recovery**	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
• **Port Error Recovery Timeout**	The time that has to pass before a port in the *error-disabled* state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

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

Buttons

Save: Click to save changes.

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

4.7.3 STP Bridge Status

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

The displayed table contains a row for each STP bridge instance, where the column displays the following information: The STP Bridge Status screen in Figure 4-7-8 appears.

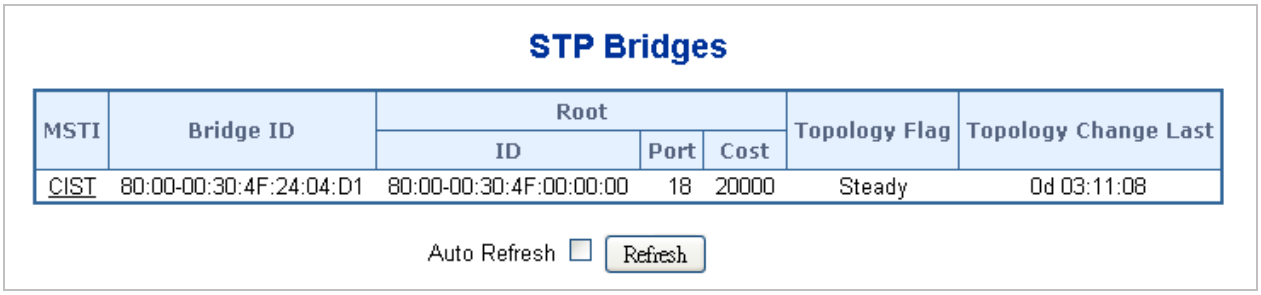


Figure 4-7-8 STP Bridge Status page screenshot

The page includes the following fields:

Object	Description
• **MSTI**	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
• **Bridge ID**	The Bridge ID of this Bridge instance.
• **Root ID**	The Bridge ID of the currently elected root bridge.
• **Root Port**	The switch port currently assigned the *root* port role.
• **Root Cost**	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
• **Topology Flag**	The current state of the Topology Change Flag for this Bridge instance.
• **Topology Change Last**	The time since last Topology Change occurred.

4.7.4 STP CIST Port Configuration

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

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

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

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

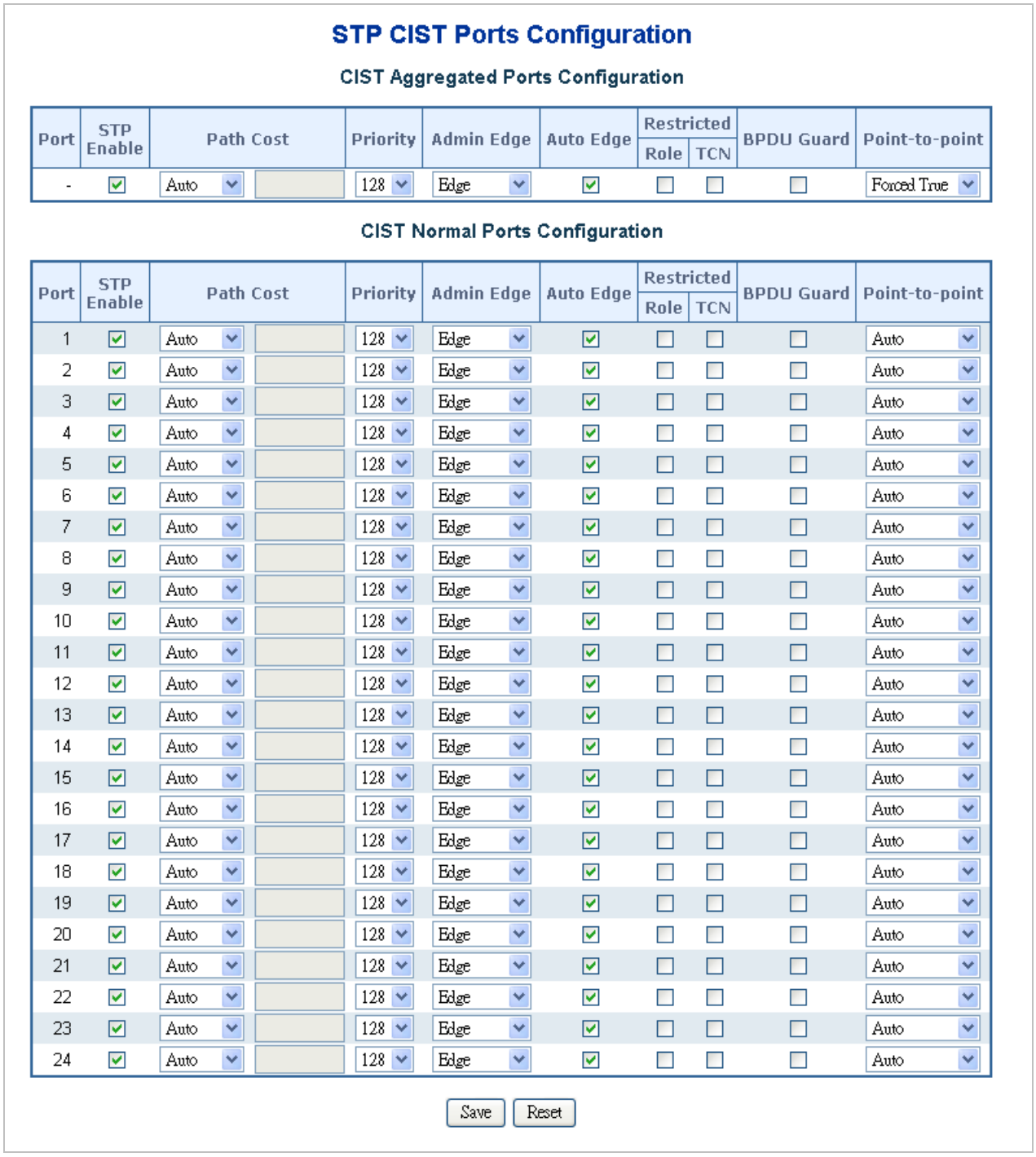


Figure 4-7-9 STP CIST Port Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **STP Enabled**	Controls whether RSTP is enabled on this switch port.
• **Path Cost**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Default: **128** Range: 0-240, in steps of 16
• **operEdge (state flag)**	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having operEdge true) than for other ports.
• **AdminEdge**	Controls whether the operEdge flag should start as beeing set or cleared. (The initial operEdge state when a port is initialized).
• **AutoEdge**	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
• **Restricted Role**	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also know as **Root Guard**.
• **Restricted TCN**	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.
• **BPDU Guard**	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port

	Error Recovery setting as well.
• **Point2Point**	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transitions to the forwarding state is faster for point-to-point LANs than for shared media. (This applies to physical ports only. Aggregations are always *forced Point2Point*).

Buttons

Save: Click to save changes.

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

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

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

Table 4-7-1 Recommended STP Path Cost Range

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

Table 4-7-2 Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000

Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

Table 4-7-3 Default STP Path Costs

4.7.5 MSTI Priority

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Priority screen in Figure 4-7-10 appears.

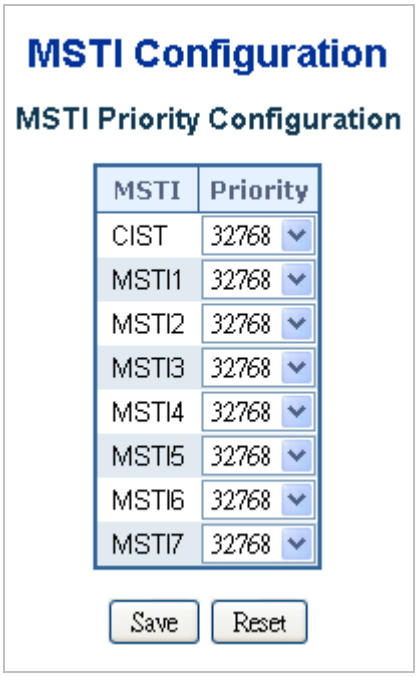


Figure 4-7-10 MSTI Priority page screenshot

The page includes the following fields:

Object	Description
• **MSTI**	The bridge instance. The CIST is the default instance, which is always active.
• **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

Save: Click to save changes.

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

4.7.6 MSTI Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Configuration screen in Figure 4-7-11 appears.

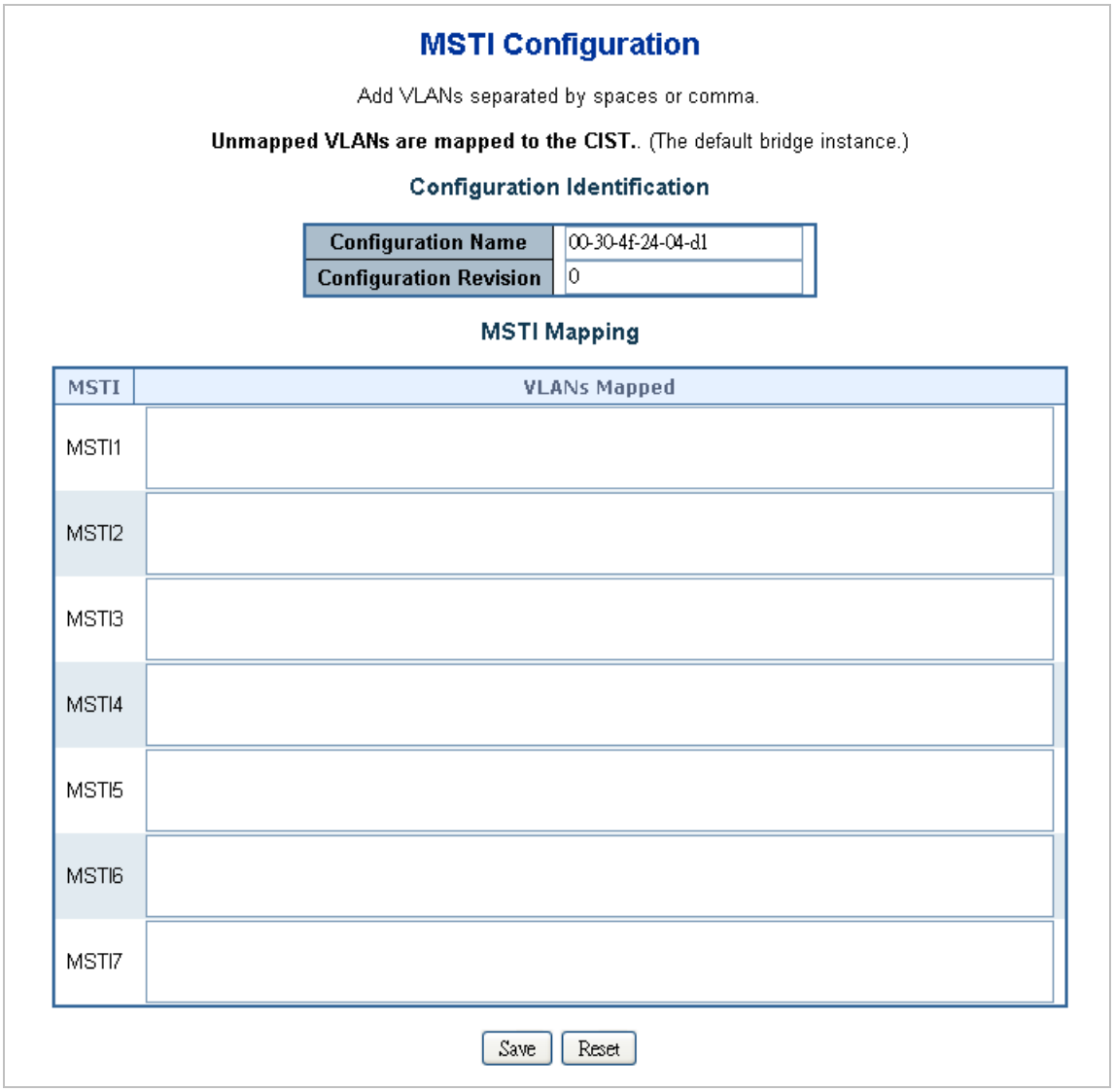


Figure 4-7-11 MSTI Configuration page screenshot

The page includes the following fields:

Configuration Identification

Object	Description
• **Configuration Name**	The name identifiying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
• **Configuration Revision**	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

Object	Description
• **MSTI**	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
• **VLANs Mapped**	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. A unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

Buttons

Save: Click to save changes.

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

4.7.7 MSTI Ports Configuration

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 Port Configuration screen in Figure 4-7-12 & Figure 4-7-13appears.

Figure 4-7-12 MSTI Port Configuration page screenshot

The page includes the following fields:

MSTI Port Configuration

Object	Description
• **Select MSTI**	Select the bridge instance and set more detail configuration.

Figure 4-7-13 MST1 MSTI Port Configuration page screenshot

The page includes the following fields:

MSTx MSTI Port Configuration

Object	Description

• **Port**	The switch port number of the corresponding STP CIST (and MSTI) port.
• **Path Cost**	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

Get: Click to set MSTx configuration

Refresh: Click to refresh the page immediately.

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

4.7.8 STP Port Status

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

The STP Port Status screen in Figure 4-7-14 appears.

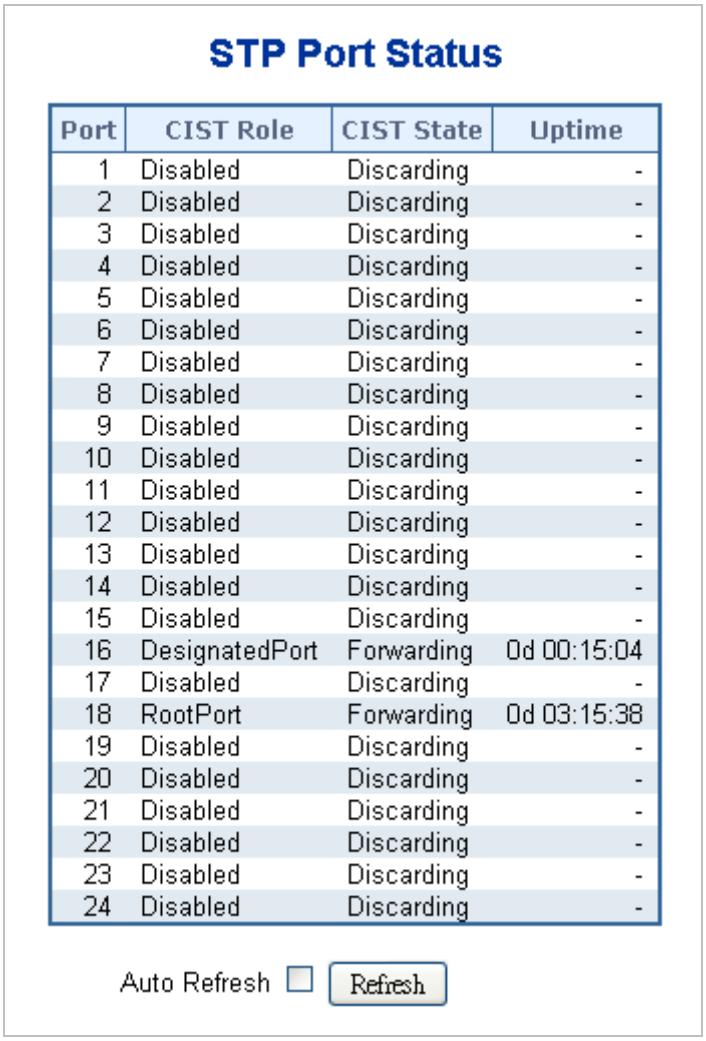


Figure 4-7-14 STP Port Status page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **CIST Role**	The current STP port role of the ICST port. The port role can be one of the following values: **AlternatePort** **BackupPort** **RootPort** **DesignatedPort**
• **State**	The current STP port state of the CIST port . The port state can be one of the following values:

	Disabled **Blocking** **Learning** **Forwarding** **Non-STP**
• **Uptime**	The time since the bridge port was last initialized.

Buttons

Refresh: Click to refresh the page immediately.

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

4.7.9 STP Port Statistics

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

The STP Port Statistics screen in Figure 4-7-15 appears.

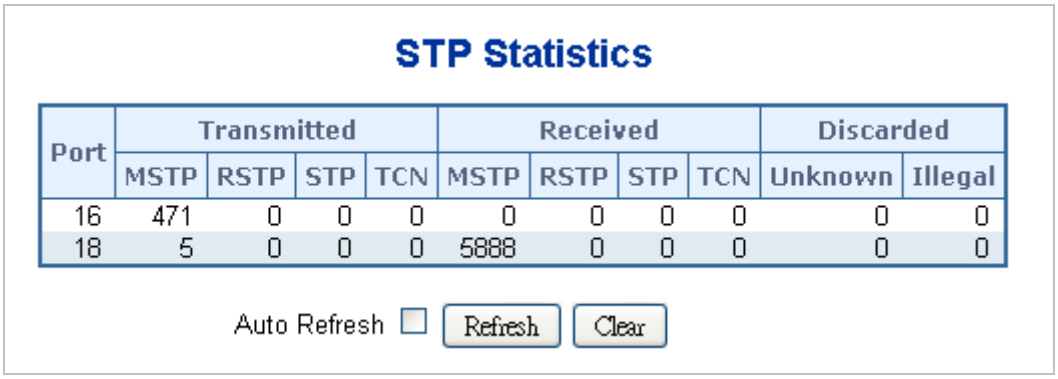


Figure 4-7-15 STP Statistics page screenshot

The page includes the following fields:

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

Buttons

Refresh: Click to refresh the page immediately.

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

Clear: Click to clear the information immediately.

4.8 Multicast

4.8.1 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.

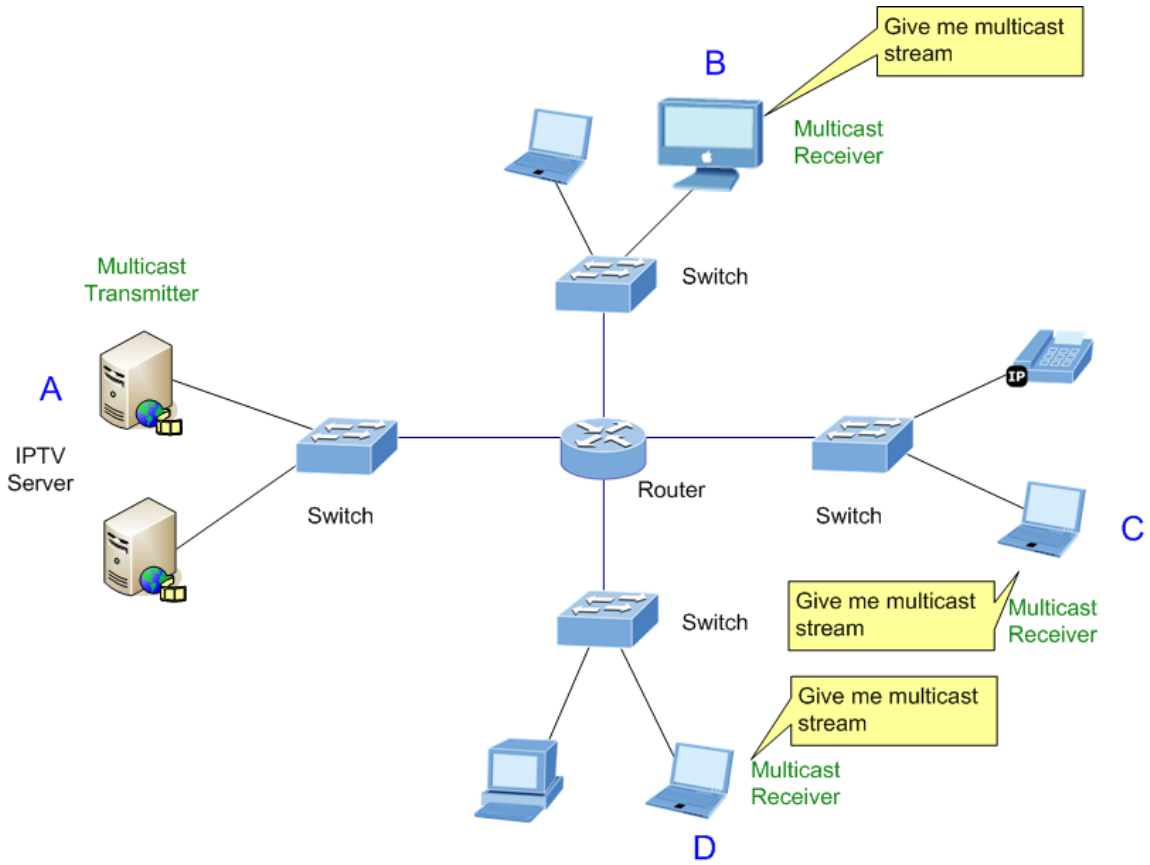


Figure 4-8-1 Multicast Service

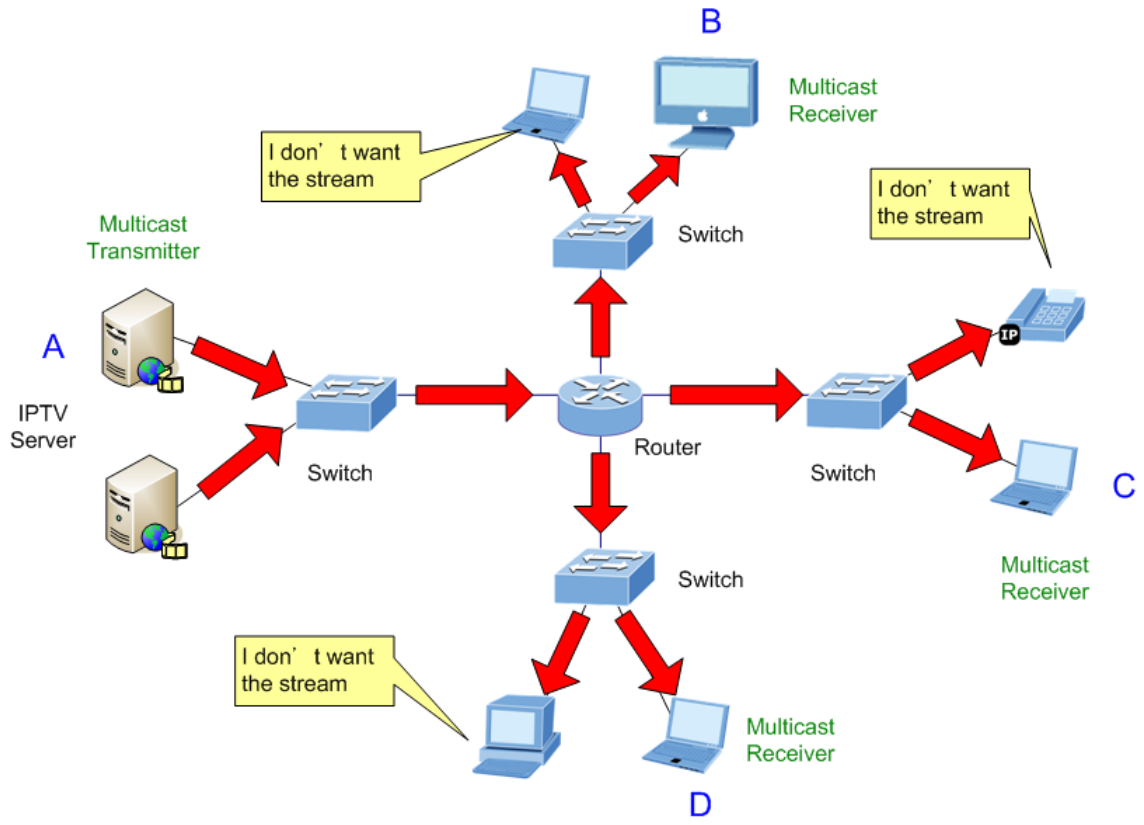


Figure 4-8-2 Multicast flooding

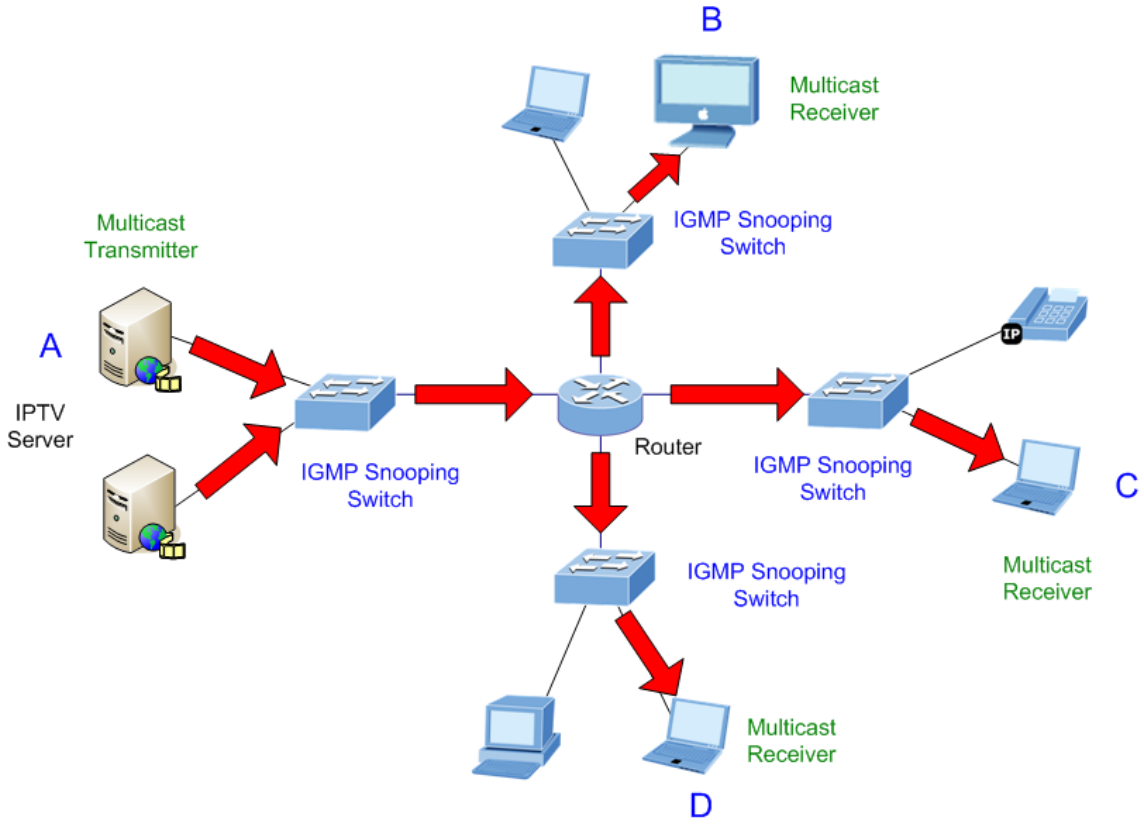


Figure 4-8-3 IGMP Snooping multicast stream control

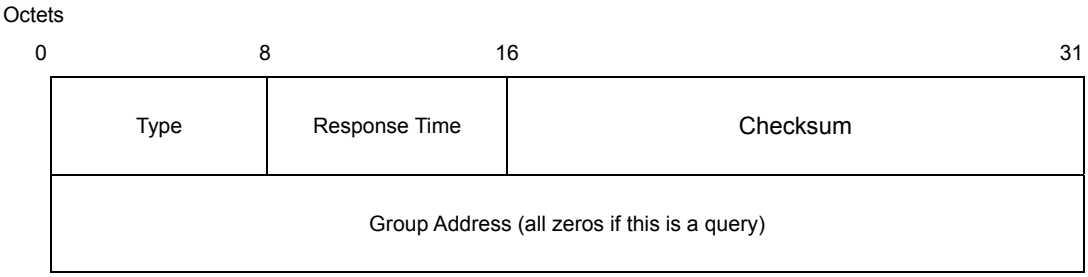
IGMP Versions 1 and 2

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



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:

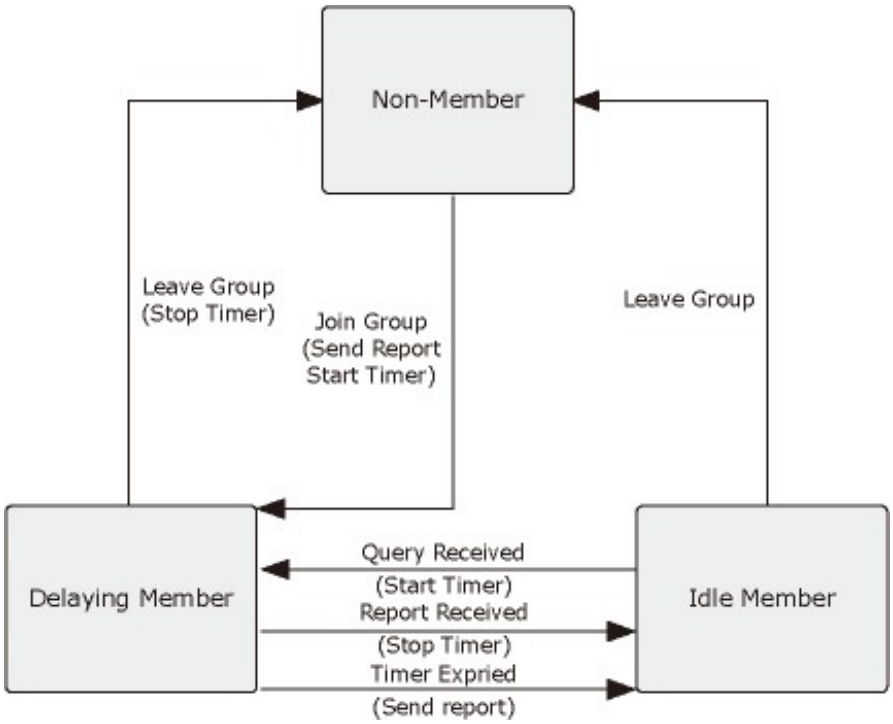


Figure 4-8-4 IGMP State Transitions

- **IGMP Querier –**

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

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

4.8.2 IGMP Snooping Configuration

This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header. The IGMP Snooping Configuration screen in Figure 4-8-5 appears.

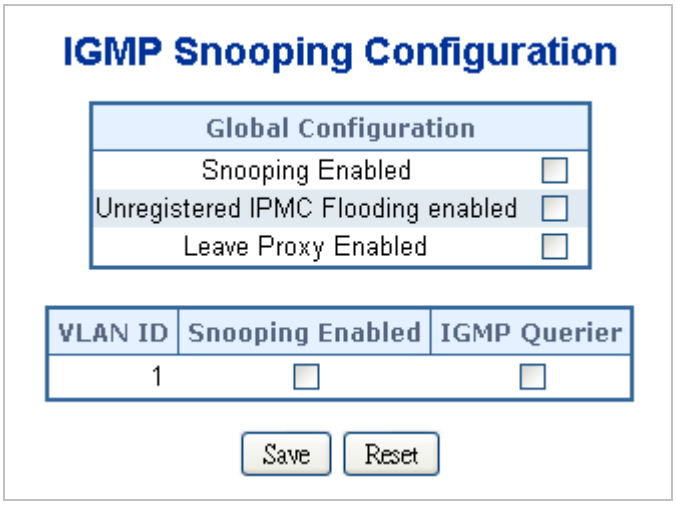


Figure 4-8-5 IGMP Snooping Configuration page screenshot

The page includes the following fields:

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

Buttons

Save: Click to save changes.

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

4.8.3 IGMP Port Related Configuration

This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header. The IGMP Port Related Configuration screen in Figure 4-8-6 appears.

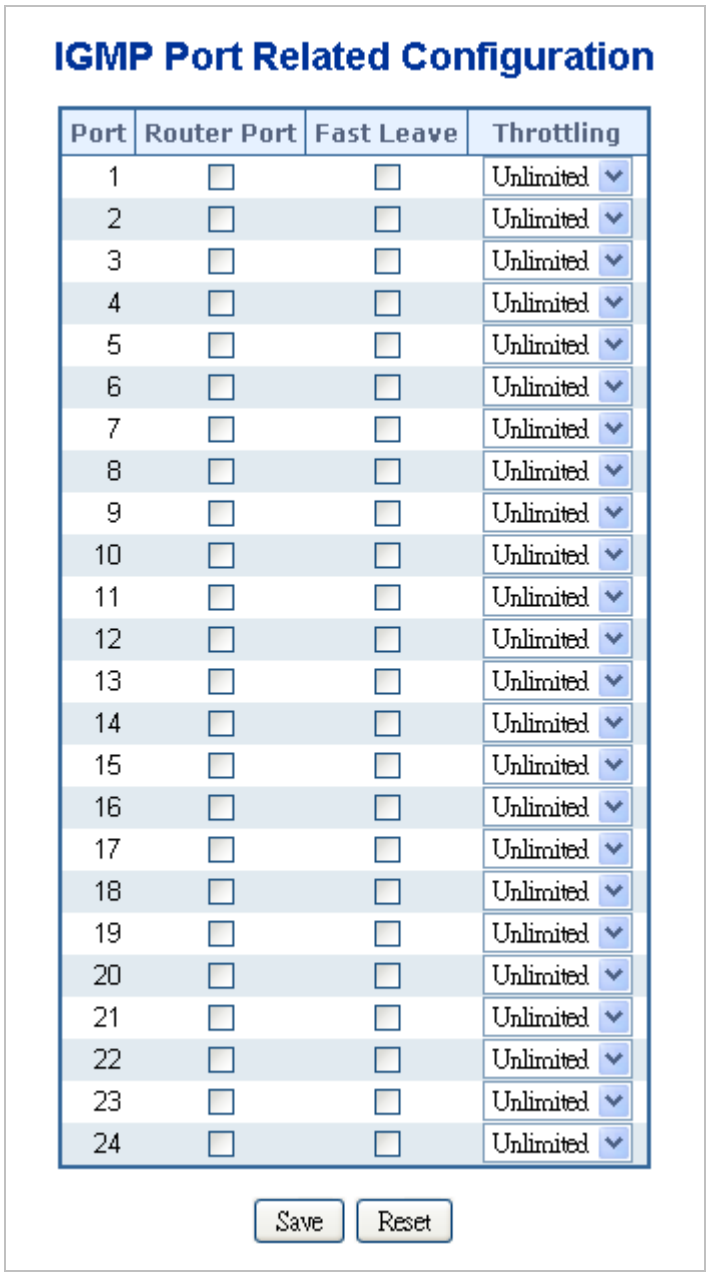


Figure 4-8-6 IGMP Port Related Configuration page screenshot

The page includes the following fields:

Object	Description
• **Router Port**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation

	will act as a router port.
• **Fast Leave**	Enable the Fast Leave on the port.
• **Throttling**	Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Save: Click to save changes.

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

4.8.4 IGMP Snooping VLAN Configuration

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

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The IGMP Snooping VLAN Configuration screen in Figure 4-8-7 appears.

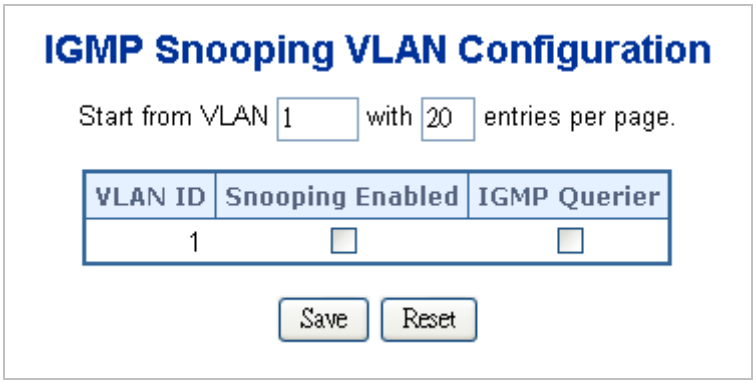


Figure 4-8-7 IGMP Snooping VLAN Configuration page screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **IGMP Snooping Enable**	Enable the per-VLAN IGMP Snooping. Only up to 64 VLANs can be selected.
• **IGMP Querier**	Enable the IGMP Querier in the VLAN. The Querier will send out if no Querier received in 255 seconds after IGMP Querier Enabled. Each Querier's interval is 125 second, and it will stop act as an IGMP Querier if received any Querier from other devices.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

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

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

Save: Click to save changes.

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

4.8.5 Port Group Filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace". If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The IGMP Snooping Port Group Filtering Configuration screen in Figure 4-8-8 appears.

Figure 4-8-8 IGMP Snooping Port Group Filtering Configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.

• **Port**	The logical port for the settings.
• **Filtering Group**	The IP Multicast Group that will be filtered.

Buttons

Delete: Check to delete the entry.

Add new Filtering Group: Click to add a new entry to the Group Filtering table.

Save: Click to save changes.

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

4.8.6 IGMP Snooping Status

This page provides IGMP Snooping status.

The status relate to the currently selected stack unit, as reflected by the page header. The IGMP Snooping Status screen in Figure 4-8-9 appears.

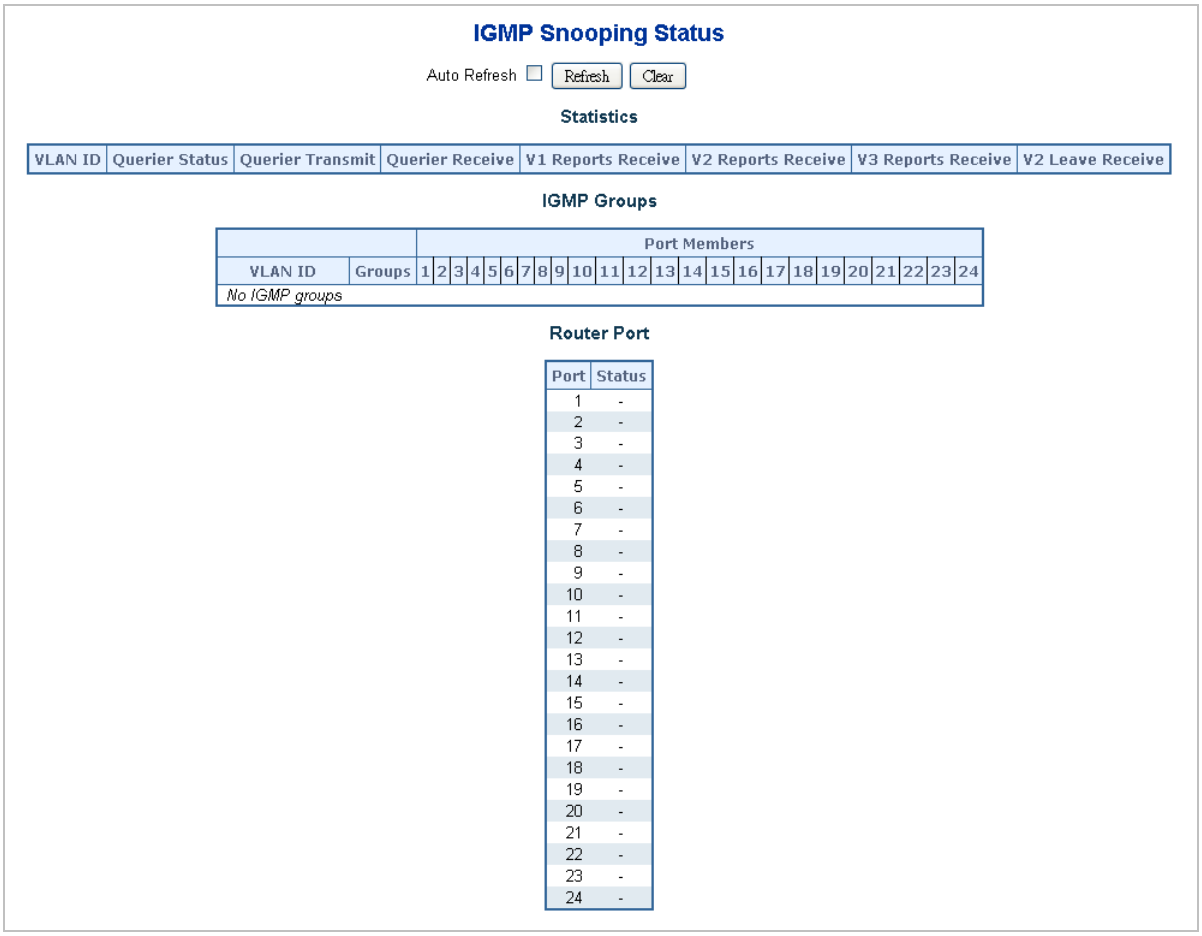


Figure 4-8-9 IGMP Snooping Status page screenshot

The page includes the following fields:

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

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

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

4.8.7 MVR Configuration

In multicast VLAN networks, subscribers to a multicast group can exist in more than one VLAN. If the VLAN boundary restrictions in a network consist of Layer 2 switches

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs. The alternative would be to use PIM or a similar protocol to route the traffic through a Layer 3- network, it might be necessary to replicate the multicast stream to the same group in different subnets, even if they are on the same physical network. Multicast VLAN Registration (MVR) routes packets received in a multicast source VLAN to one or more receive VLANs. Clients are in the receive VLANs and the multicast server is in the source VLAN. Multicast routing has to be disabled when MVR is enabled. Refer to the configuration guide at Understanding Multicast VLAN Registration for more information on MVR. MVR is typically used for IPTV-like services and is therefore usually only available on enterprise-level switches. Many manufacturers provide support for MVR on their high-end switches.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them.

This page provides MVR related configuration. The MVR Configuration screen in Figure 4-8-10 appears.

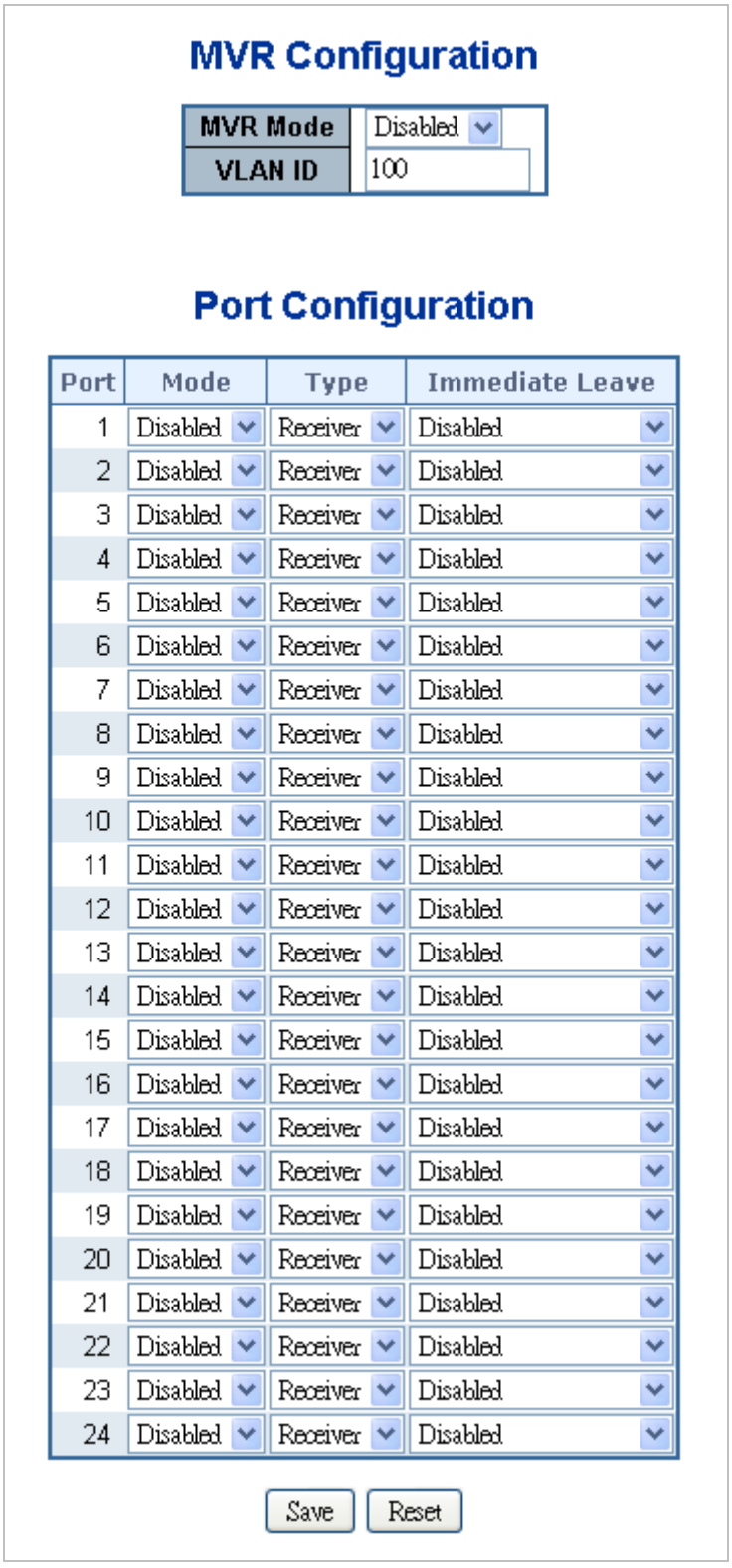


Figure 4-8-10 MVR Configuration page screenshot

The page includes the following fields:

Object	Description
• **MVR Mode**	Enable/Disable the Global MVR.

• **VLAN ID**	Specify the Multicast VLAN ID.
• **Mode**	Enable MVR on the port.
• **Type**	Specify the MVR port type on the port.
• **Immediate Leave**	Enable the fast leave on the port.

Buttons

Save: Click to save changes.

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

4.8.8 MVR Status

This page provides MVR status. The MVR Status screen in Figure 4-8-11 appears.

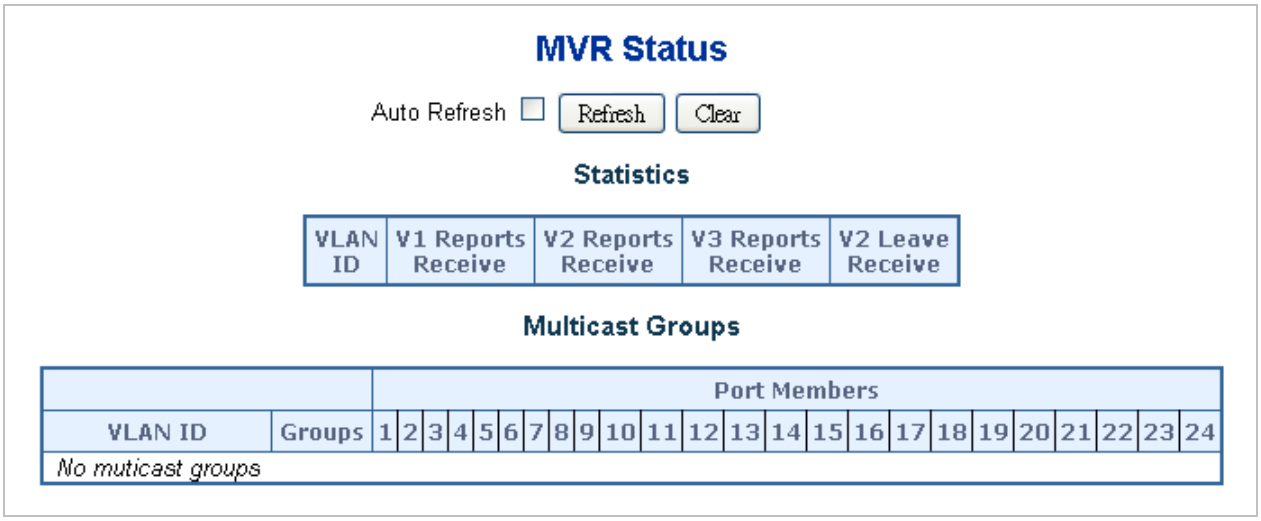


Figure 4-8-11 MVR Status page screenshot

The page includes the following fields:

Object	Description
• **Group**	The present multicast groups. Max. are 128 groups in the multicast VLAN.
• **Port Members**	The ports that are members of the entry.
• **V1 Reports Receive**	The number of Received V1 Reports.
• **V2 Reports Receive**	The number of Received V2 Reports.
• **V3 Reports Receive**	The number of Received V3 Reports.
• **V2 Leave Receive**	The number of Received V2 Leave.

Buttons

Save: Click to refresh the page immediately.

Reset: Clears all Statistics counters.

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

4.9 Quality of Service

4.9.1 Understand QOS

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

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

You can use QoS on your system to:

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

QoS Terminology

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

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

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

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

4.9.2 QCL Configuration Wizard

This handy wizard helps you set up a QCL quickly. The QCL Configuration Wizard screen in Figure 4-9-1 appears.

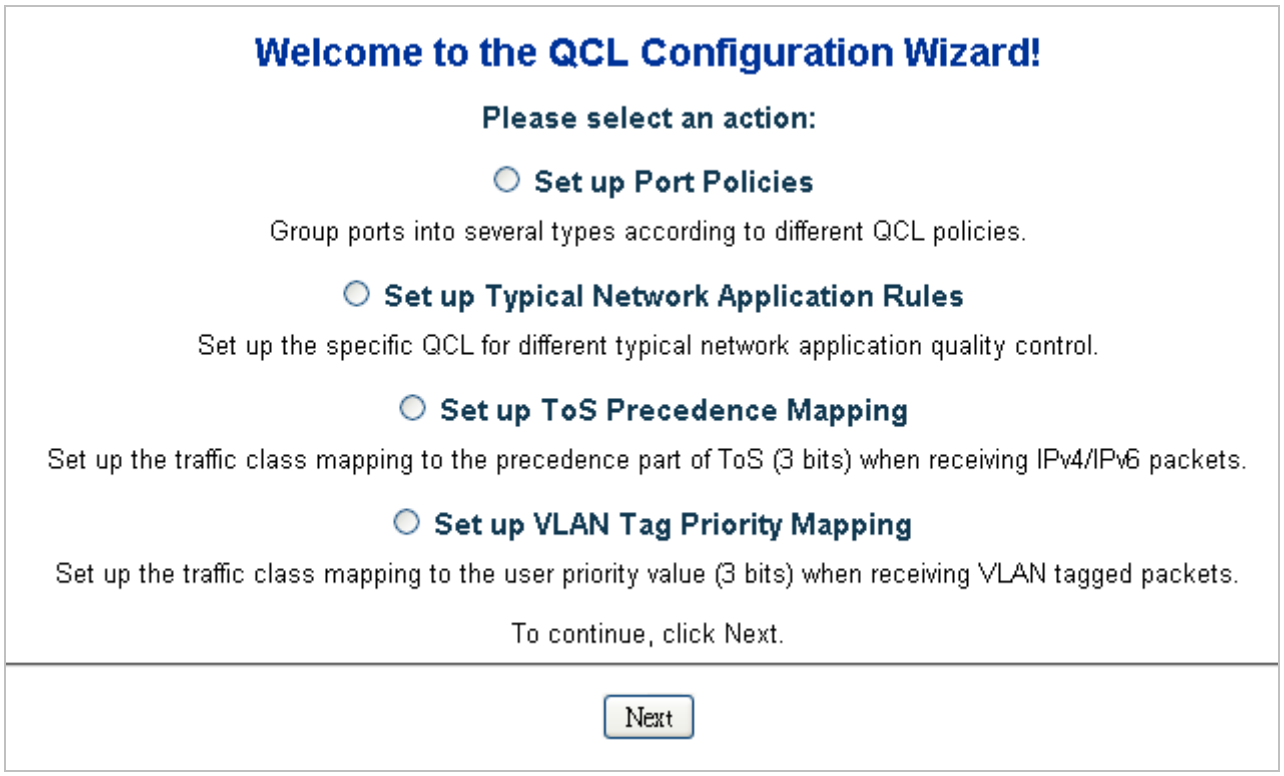


Figure 4-9-1 Welcome to the QCL Configuration Wizard page screenshot

The page includes the following fields:

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

Buttons

Next: Click to continue the wizard.

4.9.2.1 Set up Policy Rules

Group ports into several types according to different QCL policies. The settings relate to the currently selected stack unit, as reflected by the page header. The screen in Figure 4-9-2 appears.

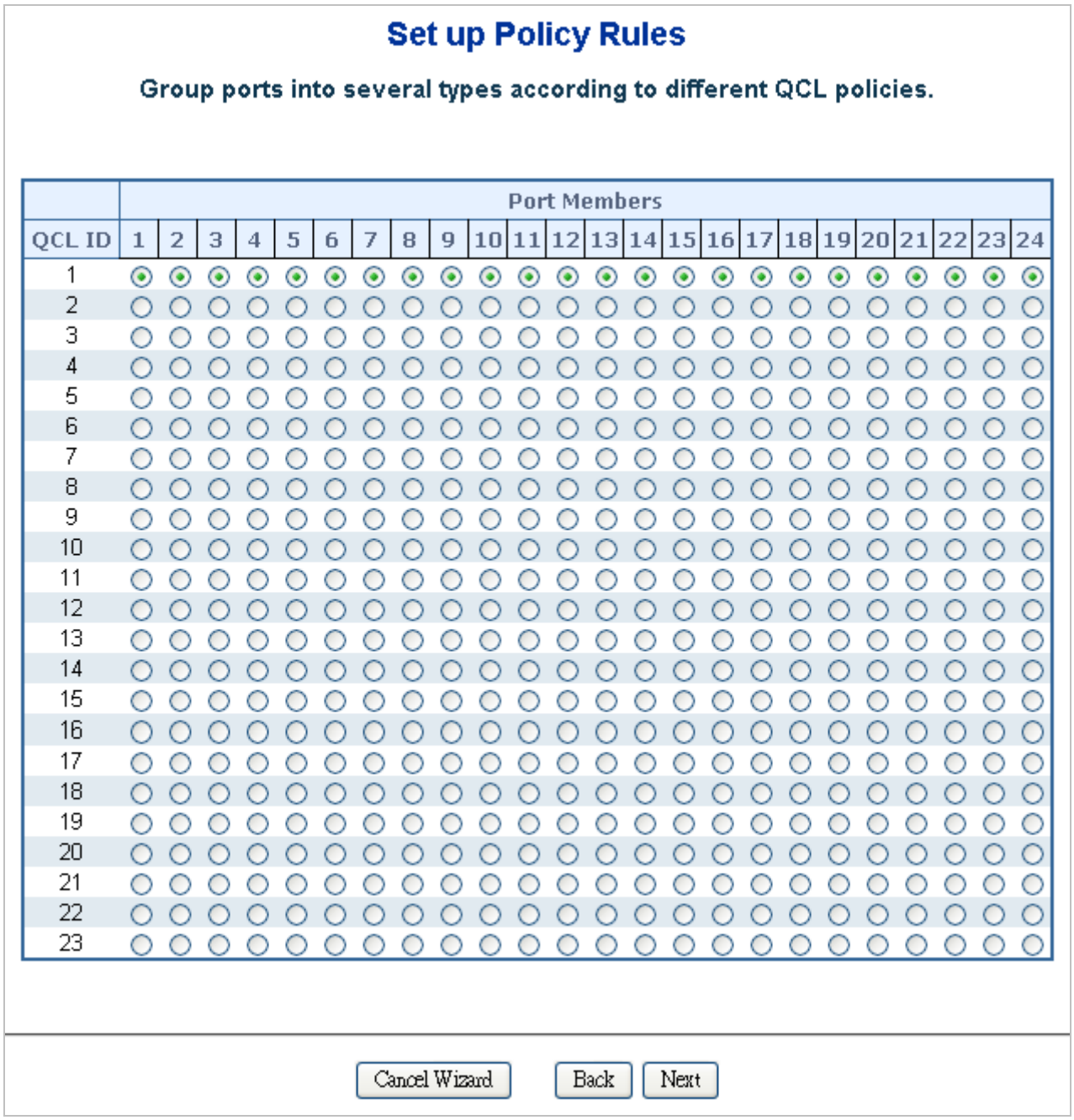


Figure 4-9-2 Set up Policy Rules page screenshot

The page includes the following fields:

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

	port in a QCL member, click the radio button.

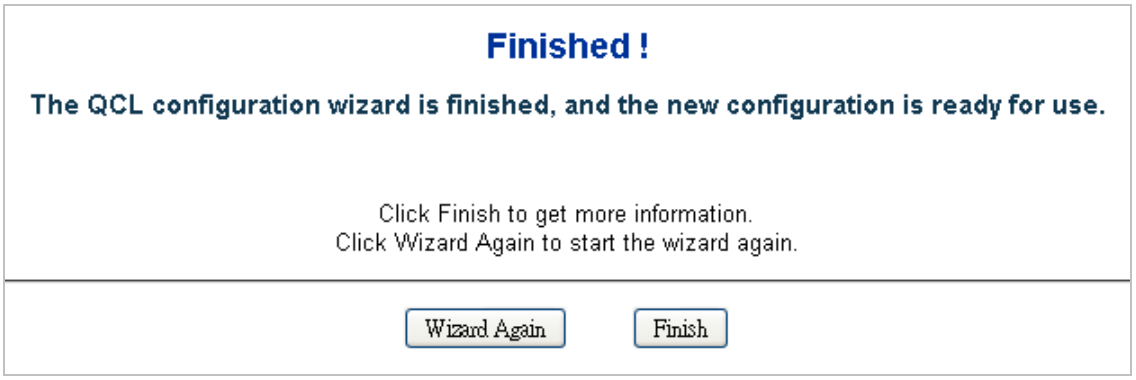
Buttons

Cancel Wizard: Click to start the wizard again.

Back: Click to get more information.

Next: Click to continue the wizard.

Once the QCL configuration wizard is finished, the below screen appears.



Buttons

Wizard Again: Click to start the wizard again.

Finish: Click to get more information.

4.9.2.2 Set up Typical Network Application Rules

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

- **STEP-1**

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

The Set up Typical Network Application Rules screen in Figure 4-9-3 appears..

Figure 4-9-3 Set up Typical Network Application Rules page screenshot

The page includes the following fields:

Object	Description
• **Audio and Video**	Indicates the common servers that apply to the specific QCE . The common servers are: **QuickTime 4 Server** **MSN Messenger Phone** **Yahoo Messenger Phone** **Napster** **Real Audio**
• **Games**	Indicates the common games that apply to the specific QCE.
• **User Definition**	Indicates the user definition that applies to the specific QCE. The user definitions are: **Ethernet Type**: Specify the Ethernet Type filter for this QCE. The allowed range is 0x600 to 0xFFFF. **VLAN ID**: VLAN ID filter for this QCE. The allowed range is 1 to 4095. **UDP/TCP Port**: Specify the TCP/UDP port filter for this QCE. The allowed range is 0 to 65535. **DSCP**: Specify the DSCP filter for this QCE. The allowed range is 0 to 63.

Buttons

Cancel Wizard: Click to cancel the wizard.

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

Next: Click to continue the wizard.

■ **STEP-2**

According to your selection on the previous page, this wizard will create specific QCEs (QoS Control Entries) automatically. First select the QCL ID for these QCEs, and then select the traffic class. Different parameter options are displayed depending on the frame type that you selected.

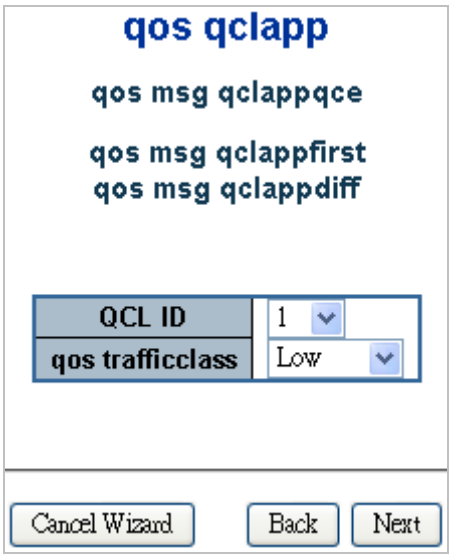


Figure 4-9-4 Set up Typical Network Application Rules page 2 screenshot

The page includes the following fields:

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

Buttons

Cancel Wizard: Click to cancel the wizard.

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

Next: Click to continue the wizard.

4.9.2.3 Set up ToS Precedence Mapping

Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets. The Set up ToS Precedence Mapping screen in Figure 4-9-5 appears.

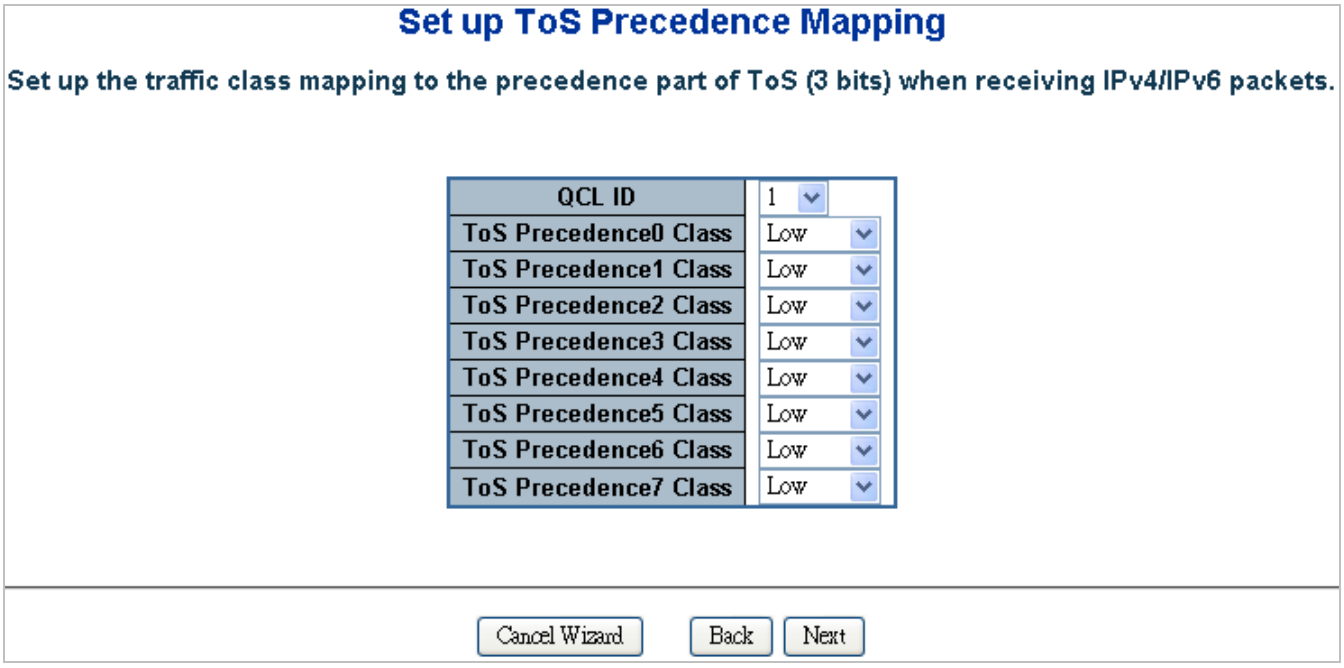


Figure 4-9-5 Set up ToS Precedence Mapping page screenshot

The page includes the following fields:

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

Buttons

Cancel Wizard: Click to cancel the wizard.

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

Next: Click to continue the wizard.

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

4.9.2.4 Set up VLAN Tag Priority Mapping

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

The Set up VLAN Tag Priority Mapping screen in Figure 4-9-6 appears.

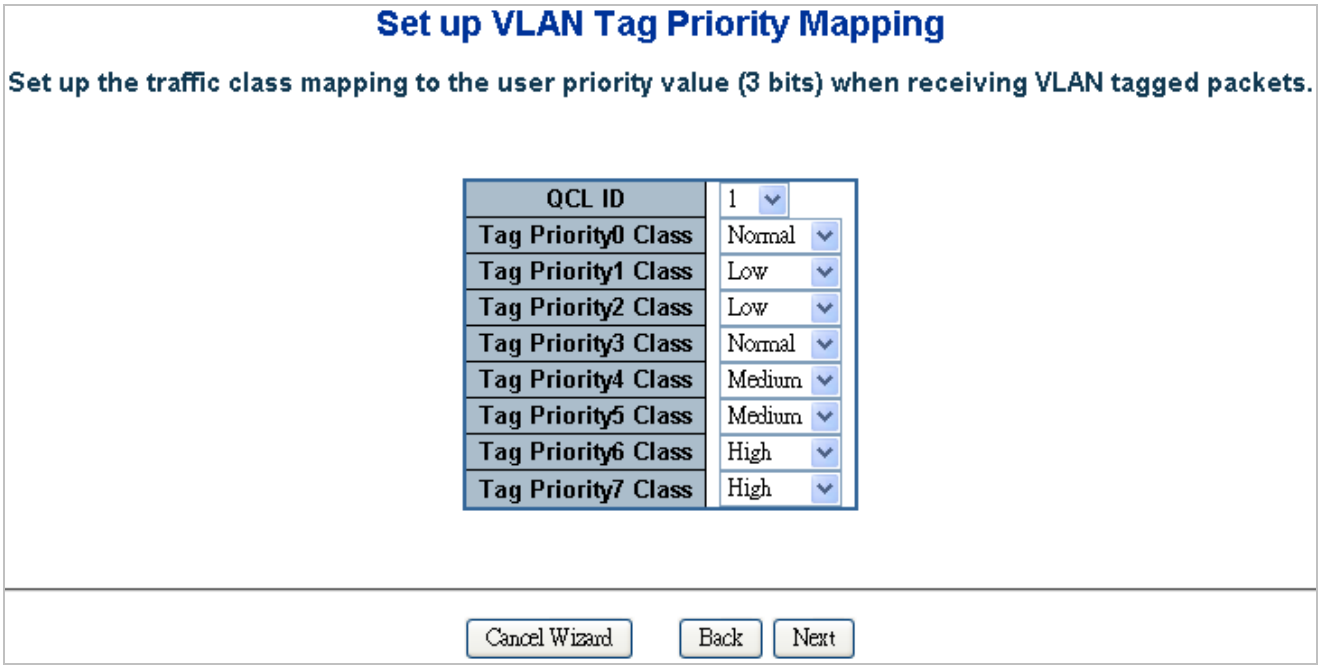


Figure 4-9-6 Set up VLAN Tag Priority Mapping page screenshot

The page includes the following fields:

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

Buttons

Cancel Wizard: Click to cancel the wizard.

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

Next: Click to continue the wizard.

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

4.9.3 QoS Control List Configuration

This page lists the QCEs for a given QCL.

- Frames can be classified by 4 different QoS classes: **Low**, **Normal**, **Medium**, and **High**.
- The classification is controlled by a QoS assigned to each port.
- A QCL consists of an ordered list of up to 12 QCEs.
- Each QCE can be used to classify certain frames to a specific QoS class.
- This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS Class for the port.

The QoS Control List Configuration screen in Figure 4-9-7 appears.

Figure 4-9-7 QoS Control List Configuration page screenshot

The page includes the following fields:

Object	Description
• **QCL #**	Select a QCL to display a table that lists all the QCEs for that particular QCL.
• **QCE Type**	Specifies which frame field the QCE processes to determine the QoS class of the frame. The following QCE types are supported: **Ethernet Type**: The Ethernet Type field. If frame is tagged, this is the Ethernet Type that follows the tag header. **VLAN ID**: VLAN ID. Only applicable if the frame is VLAN tagged. **TCP/UDP Port**: IPv4 TCP/UDP source/destination port.

	DSCP: IPv4 and IPv6 DSCP. **ToS**: The 3 precedence bit in the ToS byte of the IPv4/IPv6 header (also known as DS field). **Tag Priority**: User Priority. Only applicable if the frame is VLAN tagged or priority tagged.
• **Type Value**	Indicates the value according to its QCE type. **Ethernet Type**: The field shows the Ethernet Type value. **VLAN ID**: The field shows the VLAN ID. **TCP/UDP Port**: The field shows the TCP/UDP port range. **DSCP**: The field shows the IPv4/IPv6 DSCP value.
• **Traffic Class**	The QoS class associated with the QCE.
• **Modification Buttons**	You can modify each QCE in the table using the following buttons: : Inserts a new QCE before the current row. : Edits the QCE. : Moves the QCE up the list. : Moves the QCE down the list. : Deletes the QCE. : The lowest plus sign adds a new entry at the bottom of the list of QCL.

4.9.3.1 QoS Control Entry Configuration

Configure a new QoS Control Entry on this page.

- Frames can be classified by up to 4 different QoS classes: **Low**, **Normal**, **Medium**, and **High**.
- The classification is controlled by a QCL assigned to each port.
- A QCL consists of an ordered list of up to **12** QCEs.
- Each QCE can be used to classify certain frames to a specific QoS Class.
- This classification can be based on parameters such as **VLAN ID**, **UDP/TCP port**, **IPv4/IPv6 DSCP** or **Tag Priority.**

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

The QCE Configuration screen in Figure 4-9-8 appears.

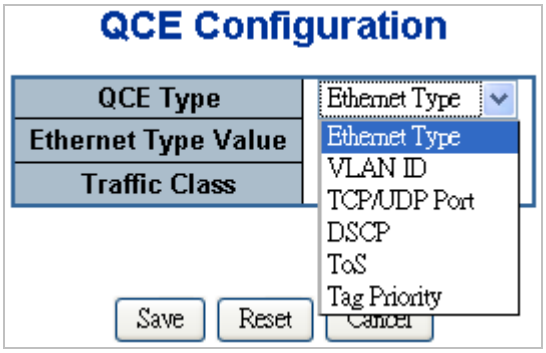


Figure 4-9-8 QCE Configuration page screenshot

The page includes the following fields:

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

Buttons

Save: Click to save changes.

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

Cancel: Return to the previous page.

4.9.4 Port QoS Configuration

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

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

- The classification is controlled by a QCL that is assigned to each port.
- A QCL consists of an ordered list of up to 12 QCEs.
- Each QCE can be used to classify certain frames to a specific QoS class.
- This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority.
- Frames not matching any of the QCEs are classified to the default QoS class for the port.
- The settings relate to the currently selected stack unit, as reflected by the page header.

The Port QoS Configuration screen in Figure 4-9-9 appears.

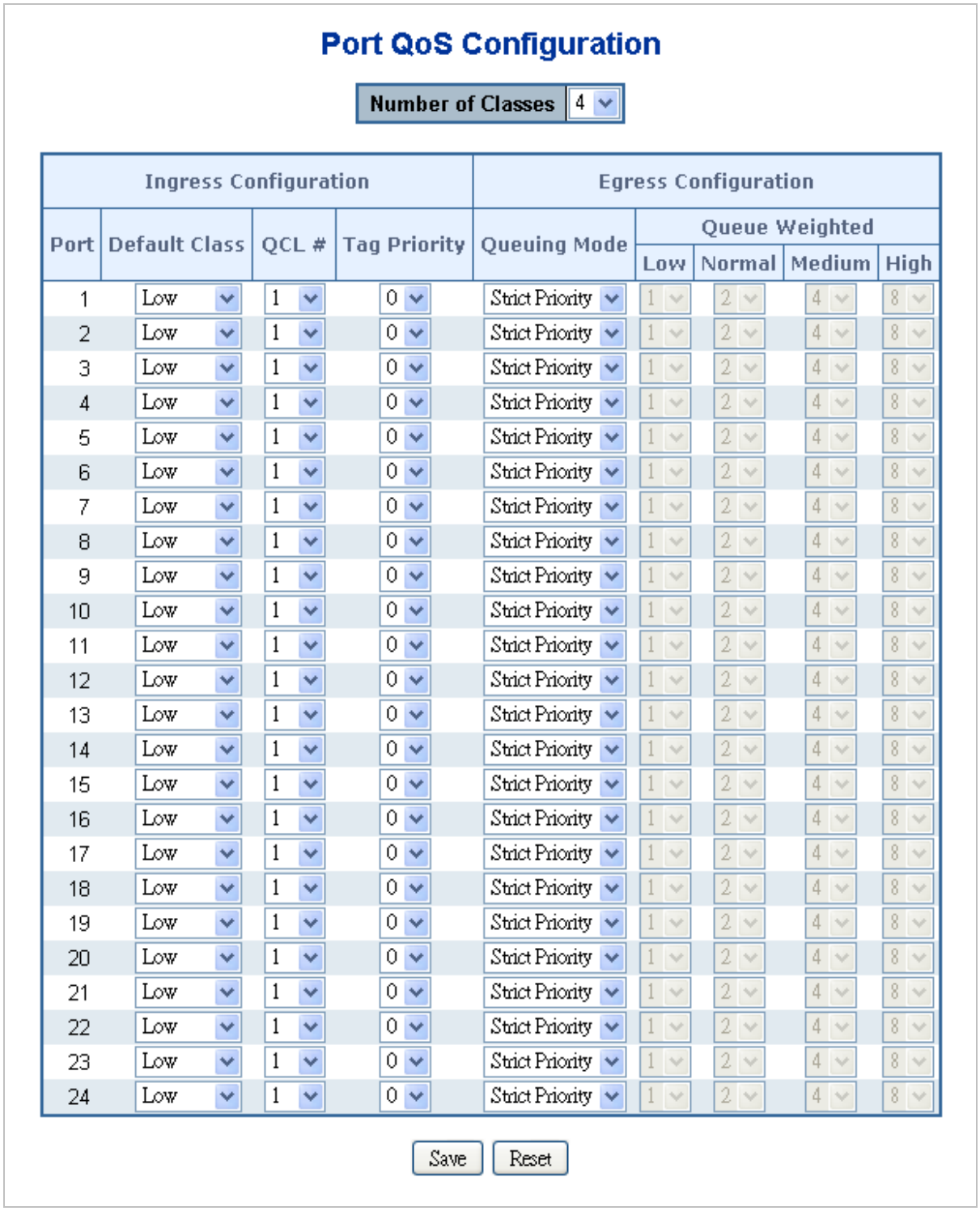


Figure 4-9-9 Port QoS Configuration page screenshot

The page includes the following fields:

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

Buttons

Save: Click to save changes.

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

4.9.5 Bandwidth Control

Configure the switch port rate limit for Polices and Shapers on this page. The settings relate to the currently selected stack unit, as reflected by the page header. The screen Bandwidth Control in Figure 4-9-10 appears.

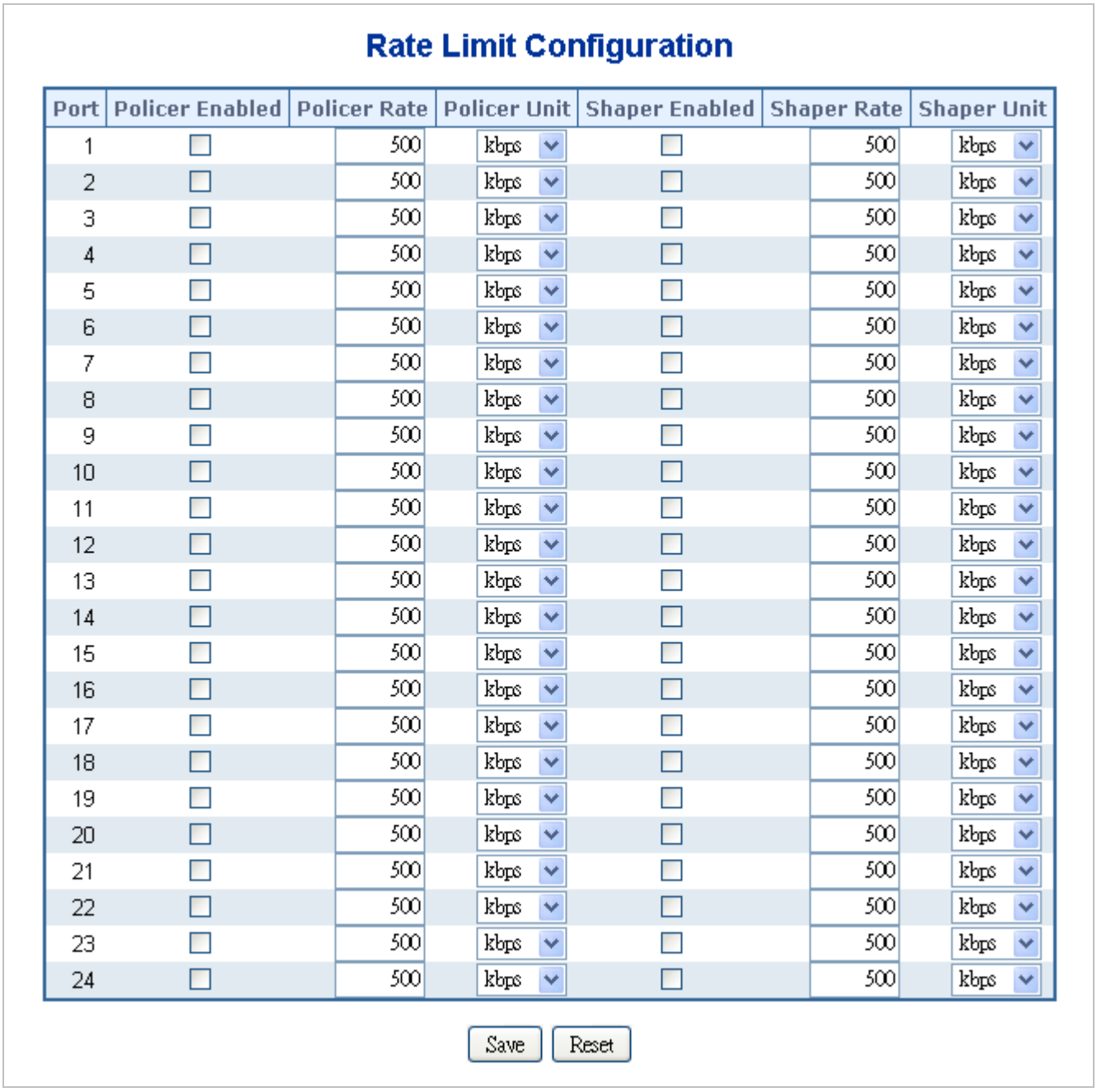


Figure 4-9-10 Rate Limit Configuration page screenshot

The page includes the following fields:

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

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

4.9.6 Storm Control Configuration

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

- **Unicast** storm rate control
- **Multicast** storm rate control
- **Broadcast** storm rate control.

The rate is 2^n, where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch. The Storm Control Configuration screen in Figure 4-9-11 appears.

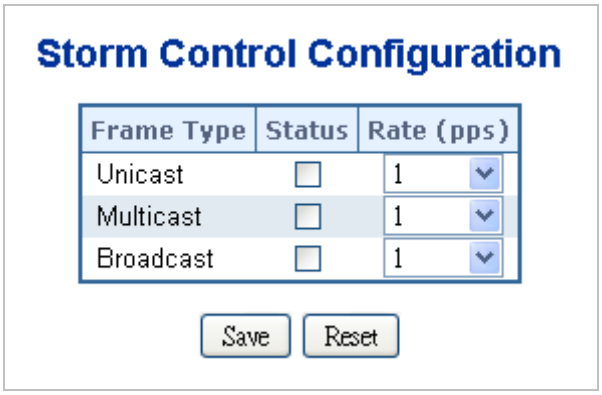


Figure 4-9-11 Storm Control Configuration page screenshot

The page includes the following fields:

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

	64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

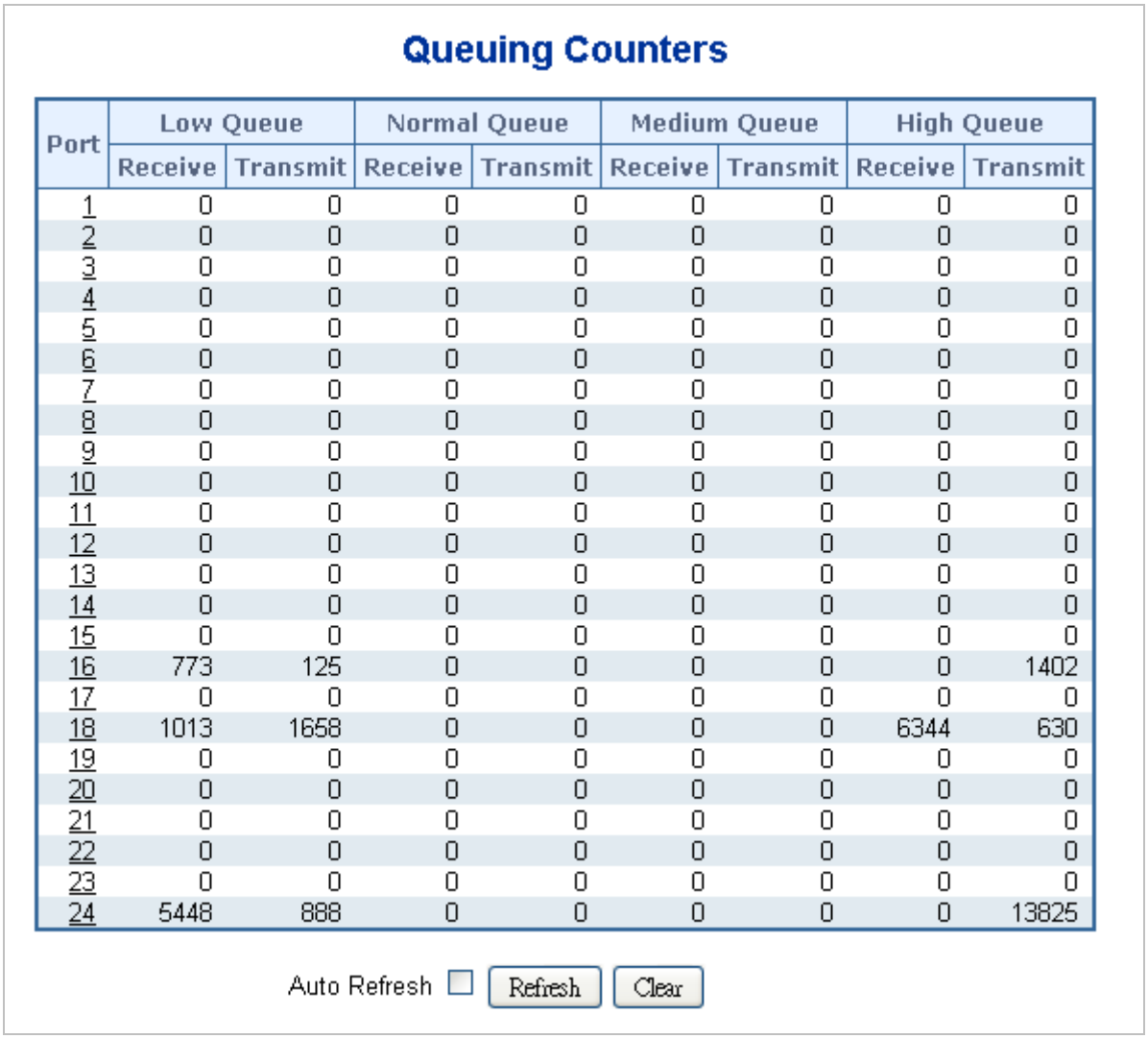
Buttons

Save: Click to save changes.

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

4.9.7 QoS Statistics

This page provides statistics for the different queues for all switch ports. The ports belong to the currently selected stack unit, as reflected by the page header. The QoS Statistics screen in Figure 4-9-12 appears.



Queuing Counters

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	773	125	0	0	0	0	0	1402
17	0	0	0	0	0	0	0	0
18	1013	1658	0	0	0	0	6344	630
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	5448	888	0	0	0	0	0	13825

Auto Refresh ☐ Refresh Clear

Figure 4-9-12 QoS Statistics page screenshot

The page includes the following fields:

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

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

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

4.9.8 DSCP Remarking

This page allows you to configure DSCP remarking related settings for each port.

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

The classification can be controlled by Port QoS configuration page.

And this page is used to configure DSCP remarking.

The DSCP value of incoming frames will be changed according to its mapping queue once this packet is transmitted by the egress port. The DSCP Remarking Configuration screen in Figure 4-9-13 appears.

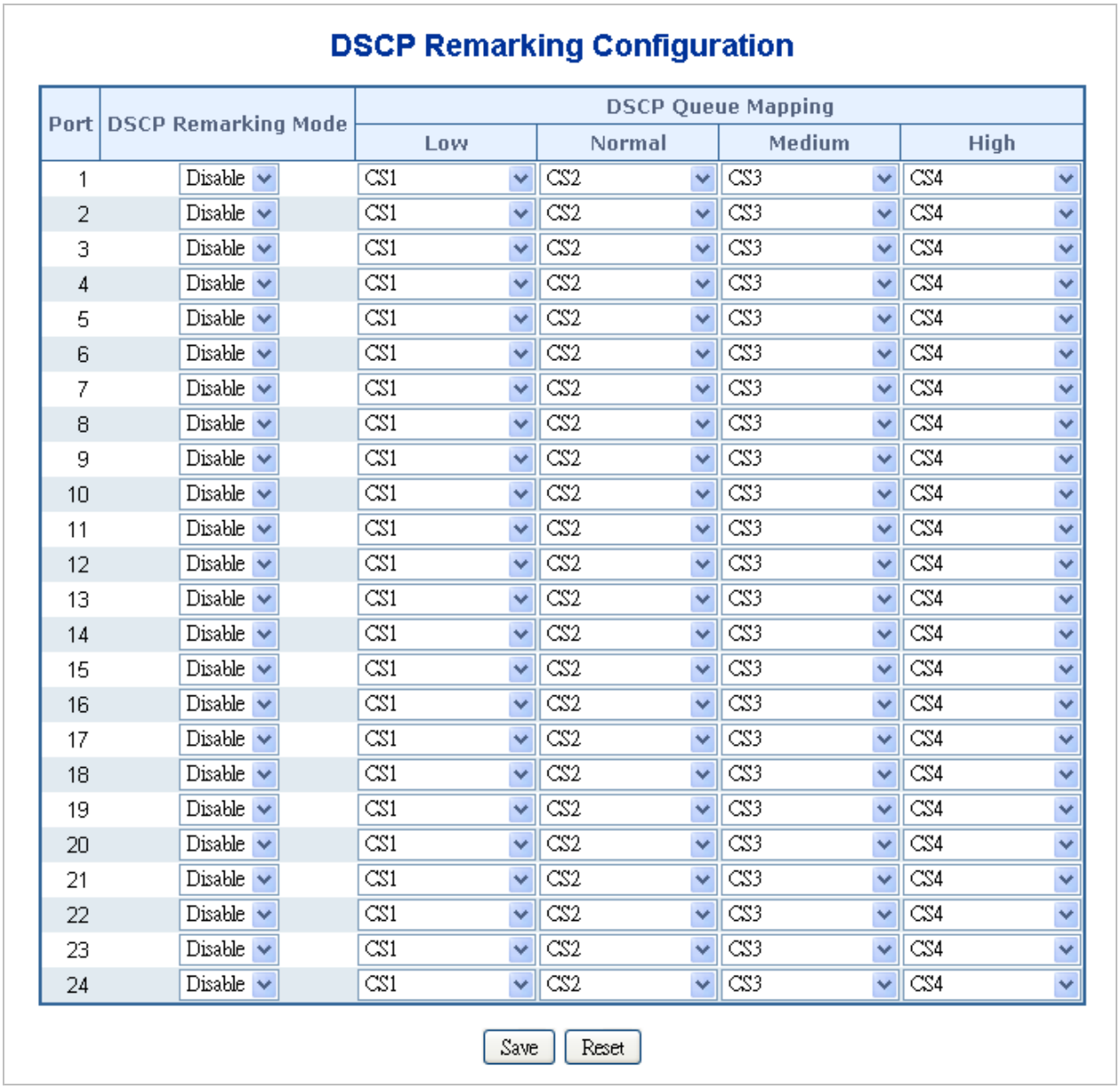


Figure 4-9-13 DSCP Remarking Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **DSCP Remarking Mode**	If the QoS remarking mode is set to enabled, it should be with this DSCP remarking/correction function according to RFC2474 on this port.
• **DSCP Queue Mapping**	Configure the mapping table between the queue and its DSCP value that is used for DSCP remarking if the DSCP value of incoming packets is not specified in RCF2474. Best Effort = DSCP (0) CS1 = DSCP (8) CS2 = DSCP (16)

	CS3 = DSCP (24) CS4 = DSCP (32) CS5 = DSCP (40) CS6 = DSCP (48) CS7 = DSCP (56) Expedite Forward = DSCP (46)

Buttons

Save: Click to save changes.

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

4.9.9 Voice VLAN Configuration

The Voice VLAN feature enables the voice traffic forwarding on the Voice VLAN, then the switch can classifying and scheduling to network traffic. It is recommands there are two VLANs on a port - one for voice, one for data. Before connect the IP device to the switch. The IP phone should configure the voice VLAN ID correctly. It should be configure through its own GUI. The Voice VLAN Configuration screen in Figure 4-9-14 appears.

Figure 4-9-14 Voice VLAN Configuration page screenshot

The page includes the following fields:

Object	Description

• **Mode**	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible modes are: **Enabled**: Enable Voice VLAN mode operation. **Disabled**: Disable Voice VLAN mode operation.
• **VLAN ID**	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is conflict configuration if the value equal management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
• **Age Time**	Indicates the Voice VLAN secure learning age time. The allowed range is 10 to 10000000 seconds. It used when security mode or auto detect mode is enabled. In other cases, it will based hardware age time. The actual age time will be situated in the [age_time; 2 * age_time] interval.
• **Traffic Class**	Indicates the Voice VLAN traffic class. All traffic on Voice VLAN will apply this class.
• **Port Mode**	Indicates the Voice VLAN port mode. When the port mode isn't disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible port modes are: **Disabled**: Disjoin from Voice VLAN. **Auto**: Enable auto detect mode. It detects whether there is VoIP phone attached on the specific port and configure the Voice VLAN members automatically. **Forced**: Forced join to Voice VLAN.
• **Port Security**	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN will be blocked 10 seconds. Possible port modes are: **Enabled**: Enable Voice VLAN security mode operation. **Disabled**: Disable Voice VLAN security mode operation.

Buttons

Save: Click to save changes.

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

4.9.10 Voice VLAN OUI Table

Configure VOICE VLAN OUI table on this page. The maximum entry number is 16. Modify OUI table will restart auto detect OUI process. The Voice VLAN OUI Table screen in Figure 4-9-15 appears.

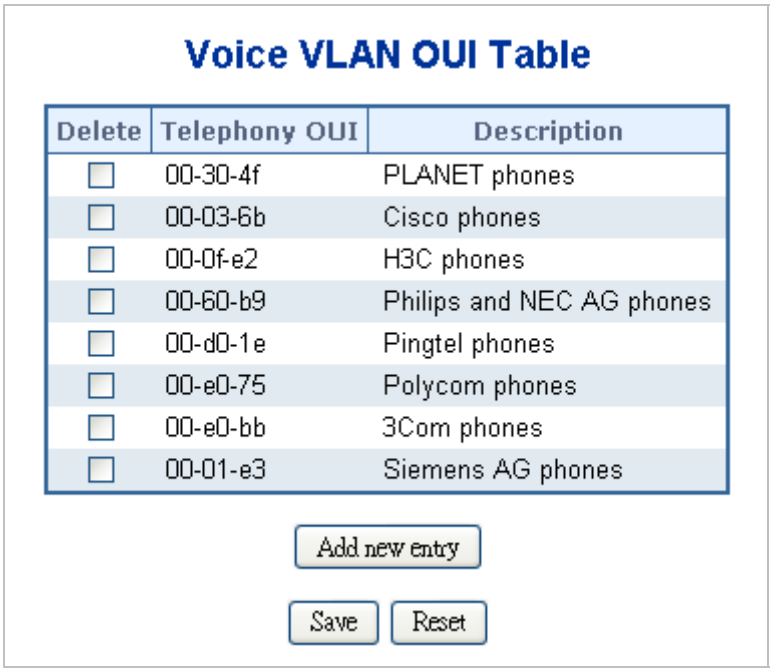


Figure 4-9-15 Voice VLAN OUI Table page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Telephony OUI**	An telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
• **Description**	The description of OUI address. Normaly, it descript which vendor telephony device. The allowed string length is 0 to 32.

Buttons

Add new entry: Click to add a new access management entry.

Save: Click to save changes.

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

4.10 Access Control Lists

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

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

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.
There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

4.10.1 Access Control List Status

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 4-9-15 appears.

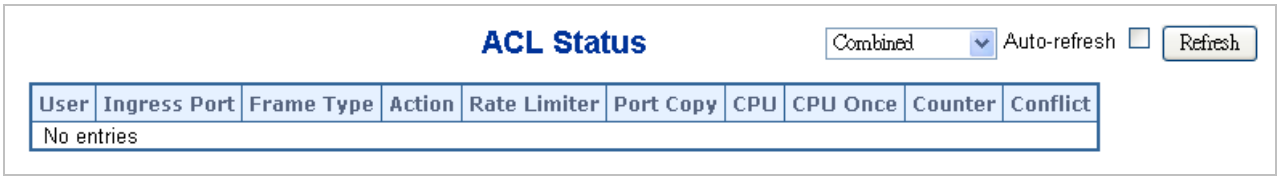


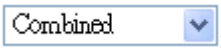
Figure 4-10-1 Voice VLAN OUI Table page screenshot

The page includes the following fields:

Object	Description
• **User**	Indicates the ACL user.
• **Ingress Port**	Indicates the ingress port of the ACE. Possible values are: **Any**: The ACE will match any ingress port. **Policy**: The ACE will match ingress ports with a specific policy. **Port**: The ACE will match a specific ingress port.
• **Frame Type**	Indicates the frame type of the ACE. Possible values are: **Any**: The ACE will match any frame type. **EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. **ARP**: The ACE will match ARP/RARP frames.

	IPv4: The ACE will match all IPv4 frames. **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
• **Action**	Indicates the forwarding action of the ACE. **Permit**: Frames matching the ACE may be forwarded and learned. **Deny**: Frames matching the ACE are dropped.
• **Rate Limiter**	Indicates the rate limiter number of the ACE. The allowed range is 1 to 15. When Disabled is displayed, the rate limiter operation is disabled.
• **Port Copy**	Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
• **CPU**	Forward packet that matched the specific ACE to CPU.
• **CPU Once**	Forward first packet that matched the specific ACE to CPU.
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.
• **Conflict**	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons



: Select the ACL status from this drop down list.

Auto-refresh  : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.

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

4.10.2 Access Control List Configuration

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

- The maximum number of ACEs is 128.
- Click on the lowest plus sign to add a new ACE to the list.

The Access Control List Configuration screen in Figure 4-10-2 appears.

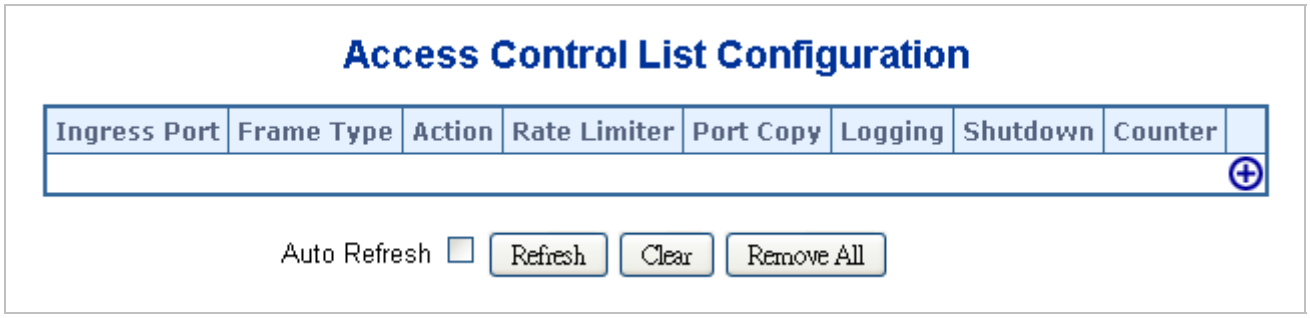


Figure 4-10-2 Access Control List Configuration page screenshot

The page includes the following fields:

Object	Description
• **Ingress Port**	Indicates the ingress port of the ACE. Possible values are: **Any**: The ACE will match any ingress port. **Policy**: The ACE will match ingress ports with a specific policy. **Port**: The ACE will match a specific ingress port.
• **Frame Type**	Indicates the frame type of the ACE. Possible values are: **Any**: The ACE will match any frame type. **EType**: The ACE will match Ethernet Type frames. **ARP**: The ACE will match ARP/RARP frames. **IPv4**: The ACE will match all IPv4 frames. **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
• **Action**	Indicates the forwarding action of the ACE. **Permit**: Frames matching the ACE may be forwarded and learned. **Deny**: Frames matching the ACE are dropped.
• **Rate Limiter**	Indicates the rate limiter number of the ACE. The allowed range is 1 to 15. When Disabled is displayed, the rate limiter operation is disabled.
• **Port Copy**	Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
• **Logging**	Indicates the logging operation of the ACE. Possible values are: **Enabled**: Frames matching the ACE are stored in the System Log. **Disabled**: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
• **Shutdown**	Indicates the port shut down operation of the ACE. Possible values are: **Enabled**: If a frame matches the ACE, the ingress port will be disabled. **Disabled**: Port shut down is disabled for the ACE.

• **Counter**	The counter indicates the number of times the ACE was hit by a frame.
• **Modification Buttons**	You can modify each ACE (Access Control Entry) in the table using the following buttons: : Inserts a new ACE before the current row. : Edits the ACE row. : Moves the ACE up the list. : Moves the ACE down the list. : Deletes the ACE. : The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.

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

Clear: Click to clear the counters.

Remove All: Click to remove all ACEs.

4.10.3 ACE Configuration

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

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type that you selected. The ACE Configuration screen in Figure 4-10-3 appears.

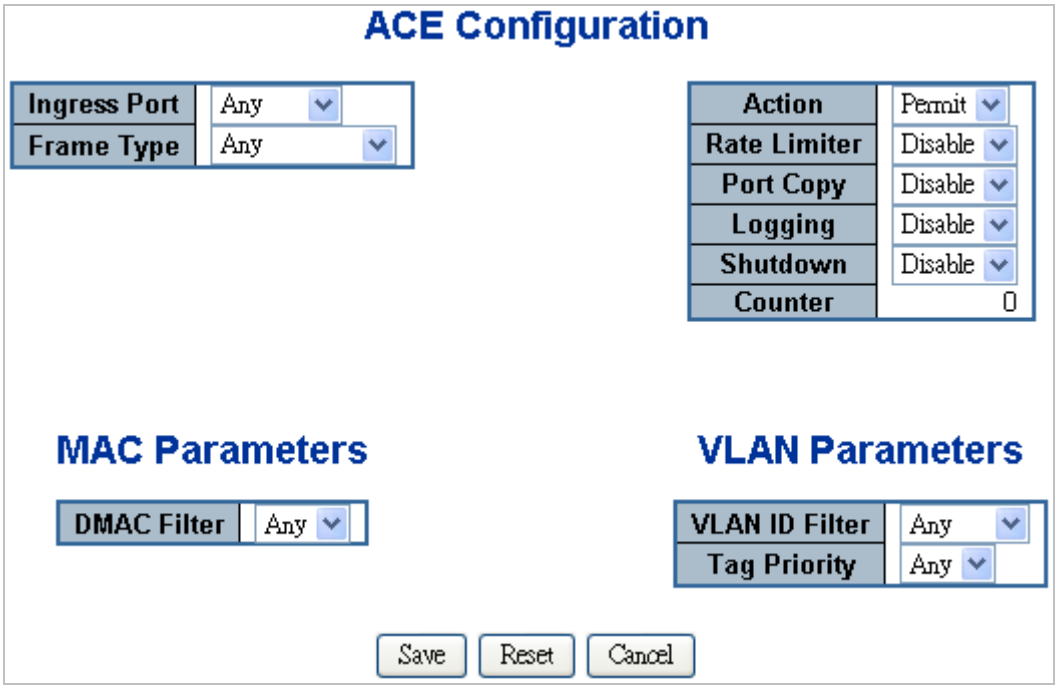


Figure 4-10-3 ACE Configuration page screenshot

The page includes the following fields:

Object	Description
• **Ingress Port**	Select the ingress port for which this ACE applies. **Any**: The ACE applies to any port. **Port n**: The ACE applies to this port number, where n is the number of the switch port. **Policy n**: The ACE applies to this policy number, where n can range from 1 through 8.
• **Frame Type**	Select the frame type for this ACE. **Any**: Any frame can match this ACE. **Ethernet Type**: Only Ethernet Type frames can match this ACE. **ARP**: Only ARP frames can match this ACE. **IPv4**: Only IPv4 frames can match this ACE.
• **Action**	Specify the action to take with a frame that hits this ACE. **Permit**: The frame that hits this ACE is granted permission for the ACE operation. **Deny**: The frame that hits this ACE is dropped.
• **Rate Limiter**	Specify the rate limiter in number of base units. The allowed range is 1 to 15. Disabled indicates that the rate limiter operation is disabled.
• **Port Copy**	Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.
• **Logging**	Specify the logging operation of the ACE. The allowed values are: **Enabled**: Frames matching the ACE are stored in the System Log.

	Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
• **Shutdown**	Specify the port shut down operation of the ACE. The allowed values are: **Enabled**: If a frame matches the ACE, the ingress port will be disabled. **Disabled**: Port shut down is disabled for the ACE.
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.

■ MAC Parameters

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

■ VLAN Parameters

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

	this VLAN ID value.
• **Tag Priority**	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

■ ARP Parameters

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

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

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

■ IP Parameters

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

Object	Description
• **IP Protocol Filter**	Specify the IP protocol filter for this ACE. **Any**: No IP protocol filter is specified ("don't-care"). **Specific**: If you want to filter a specific IP protocol filter with this ACE, choose this

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

• **DIP Filter**	Specify the destination IP filter for this ACE. **Any**: No destination IP filter is specified. (Destination IP filter is "don't-care".) **Host**: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. **Network**: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.
• **DIP Address**	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
• **DIP Mask**	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

■ ICMP Parameters

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

■ TCP/UDP Parameters

Object	Description
• **TCP/UDP Source Filter**	Specify the TCP/UDP source filter for this ACE. **Any**: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). **Specific**: If you want to filter a specific TCP/UDP source filter with this ACE, you

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

	0: TCP frames where the ACK field is set must not be able to match this entry. **1**: TCP frames where the ACK field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").
• **TCP URG**	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. **0**: TCP frames where the URG field is set must not be able to match this entry. **1**: TCP frames where the URG field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").

■ Ethernet Type Parameters

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

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

Buttons

Save: Click to save changes.

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

Cancel: Return to the previous page.

4.10.4 ACL Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE. The settings relate to the currently selected stack unit, as reflected by the page header.

The ACL Ports Configuration screen in Figure 4-10-4 appears.

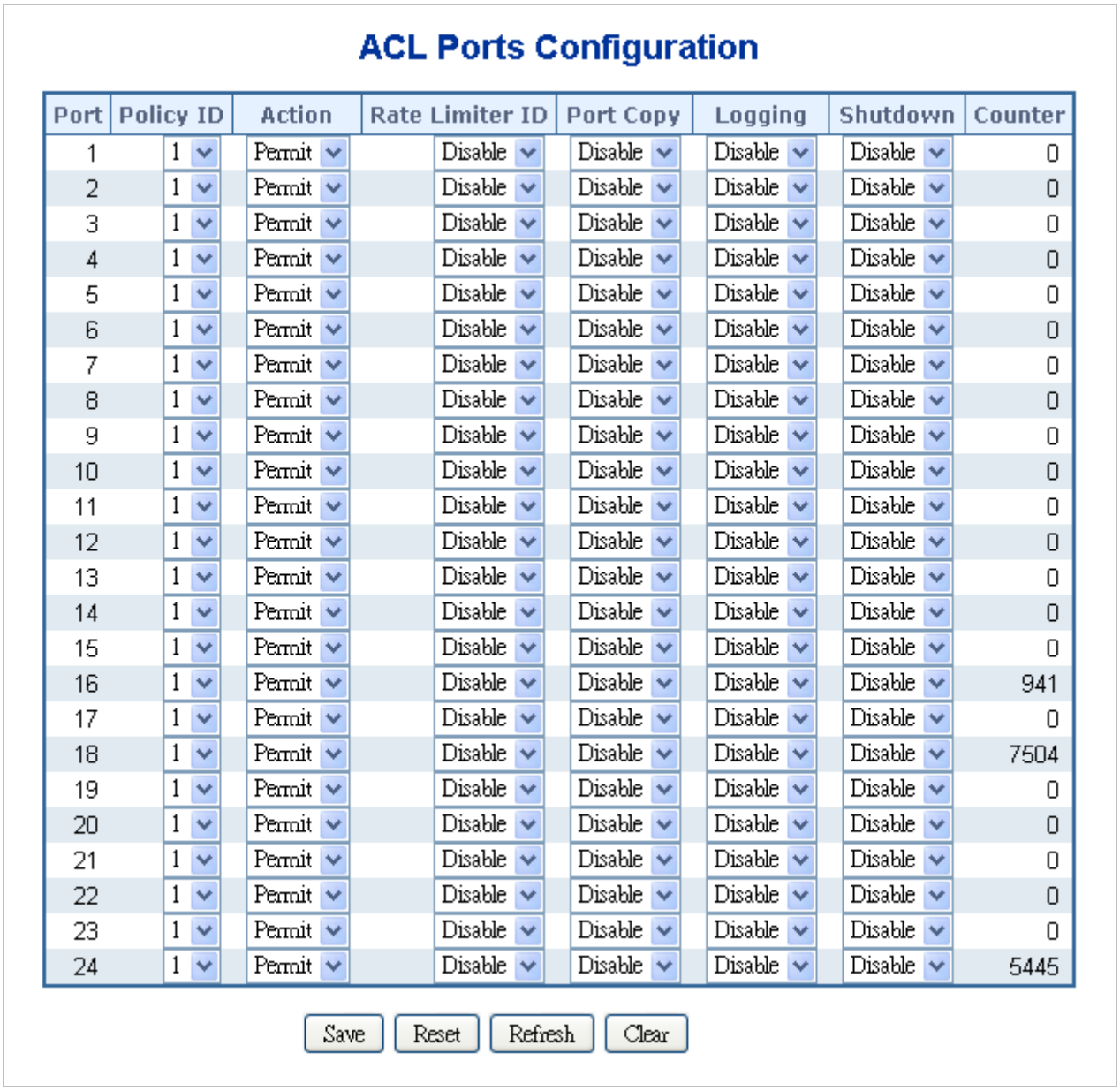


Figure 4-10-4 ACL Ports Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Policy ID**	Select the policy to apply to this port. The allowed values are **1** through **8**. The default value is 1.
• **Action**	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
• **Rate Limiter ID**	Select which rate limiter to apply to this port. The allowed values are **Disabled** or the values **1** through **15**. The default value is "Disabled".
• **Port Copy**	Select which port frames are copied to. The allowed values are **Disabled** or a specific port number. The default value is "Disabled".

• **Logging**	Specify the logging operation of this port. The allowed values are: **Enabled**: Frames received on the port are stored in the System Log. **Disabled**: Frames received on the port are not logged. The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.
• **Shutdown**	Specify the port shut down operation of this port. The allowed values are: **Enabled**: If a frame is received on the port, the port will be disabled. **Disabled**: Port shut down is disabled. The default value is "Disabled".
• **Counter**	Counts the number of frames that match this ACE.

Buttons

Save: Click to save changes.

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

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

Clear: Click to clear the counters.

4.10.5 ACL Rate Limiter Configuration

Configure the rate limiter for the ACL of the switch.

The ACL Rate Limiter Configuration screen in Figure 4-10-5 appears.

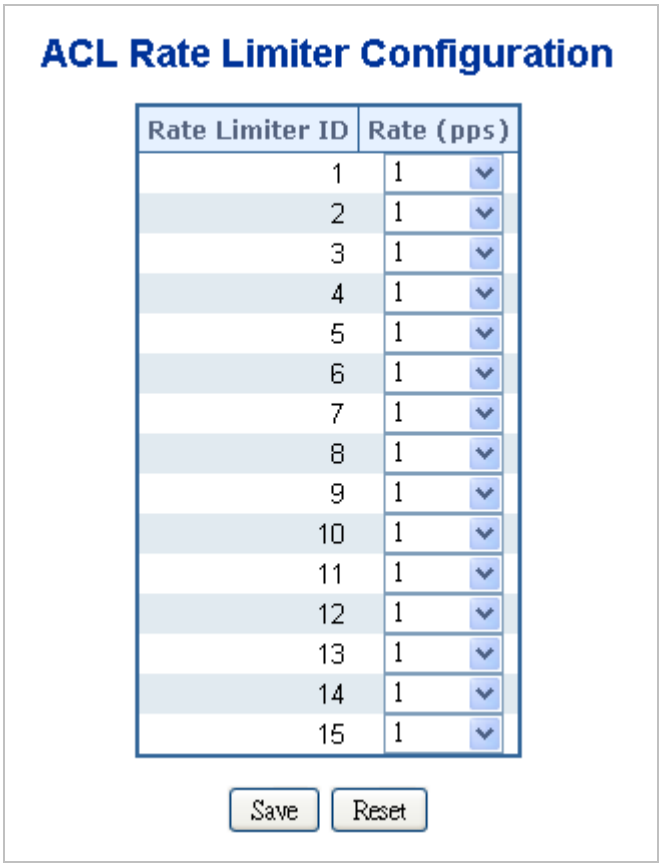


Figure 4-10-5 ACL Rate Limiter Configuration page screenshot

The page includes the following fields:

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

Buttons

Save: Click to save changes.

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

4.11 Authentication

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

The Authentication section contains links to the following main topics:

- **IEEE 802.1X Port-Based Network Access Control**
- **MAC-Based Authentication**
- **User Authentication**

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as **EAPOL (EAP Over LANs)** frames. EAPOL frames encapsulate **EAP 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 MAC-Based Authentication

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

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

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

is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.
The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide.

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)**
- **Terminal Access Controller Access Control System Plus (TACACS+)**
- **Local user name and Priviledge Level control**

RADIUS and TACACS+ are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An **authentication server** contains a database of multiple user name / password pairs with associated privilege levels for each user that requires management access to the Managed Switch.

4.11.1 Understanding IEEE 802.1X Port-Based Authentication

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

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

This section includes this conceptual information:

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

- **Device Roles**

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

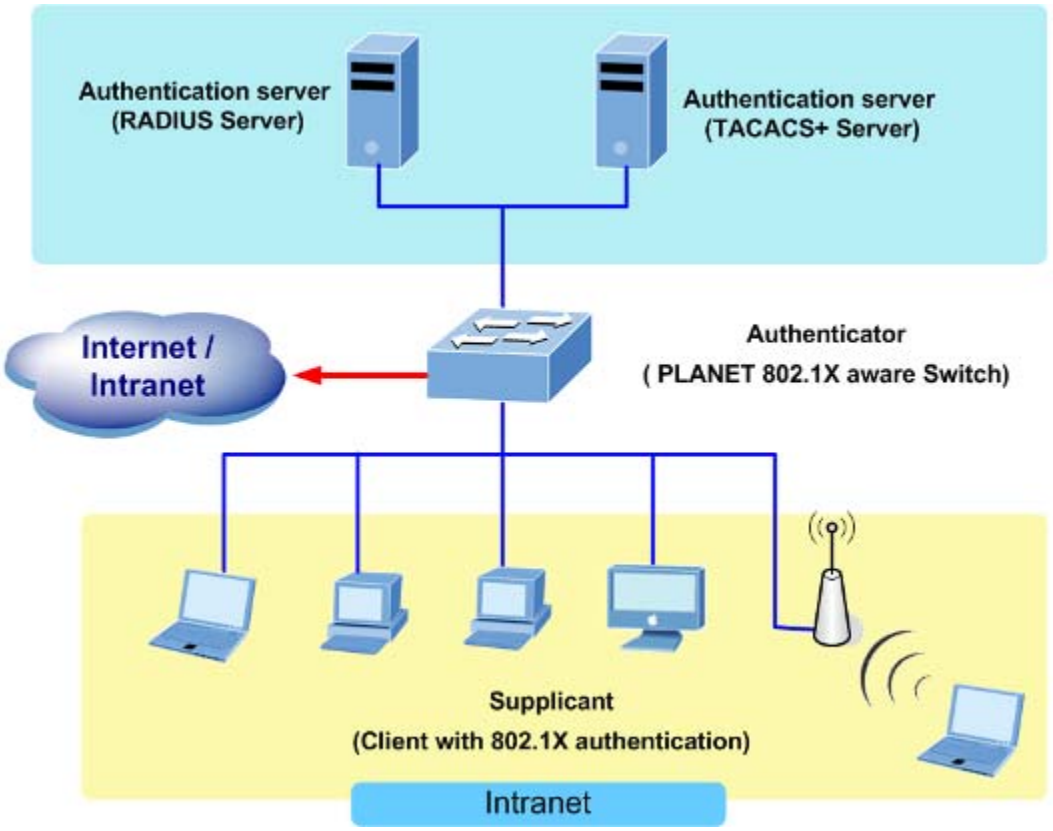


Figure 4-11-1

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

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

- ***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 4-11-2" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

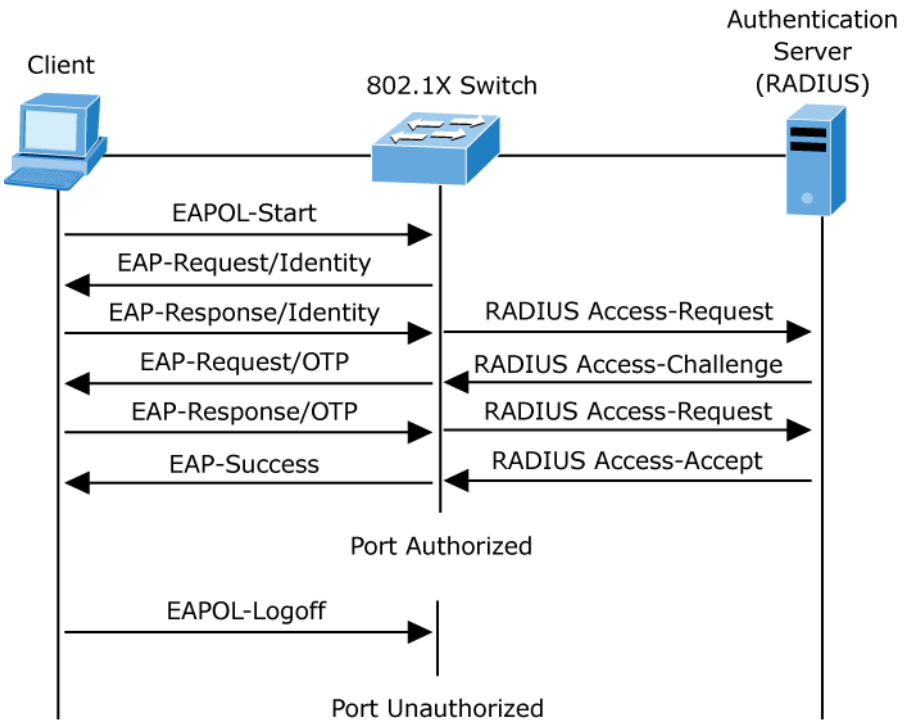


Figure 4-11-2 EAP message exchange

■ **Ports in Authorized and Unauthorized States**

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

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

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

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

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

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

4.11.2 Authentication Configuration

This page allows you to configure how an administrator is authenticated when he logs into the switch via TELNET, SSH or the web pages. The Authentication Method Configuration screen in Figure 4-11-3 appears.

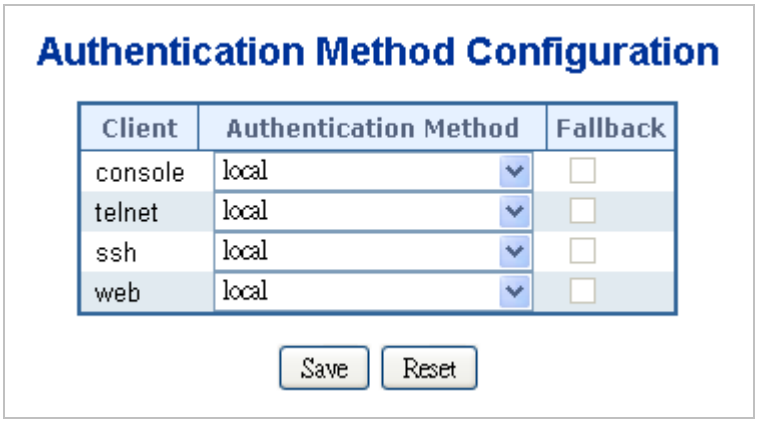


Figure 4-11-3 Authentication Method Configuration page screenshot

The page includes the following fields:

Object	Description
• **Client**	The management client for which the configuration below applies.
• **Authentication Method**	Authentication Method can be set to one of the following values: **None**: authentication is disabled and login is not possible. **local**: use the local user database on the switch stack for authentication. **radius**: use a remote RADIUS server for authentication. **tacacs+**: use a remote TACACS+ server for authentication.
• **Fallback**	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to something else than 'none or 'local'.

Buttons

Save: Click to save changes.

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

4.11.3 Network Access Server Configuration

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.
The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. 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 "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.
MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication. The NAS configuration consists of two sections, a system- and a port-wide. The Network Access Server Configuration screen in Figure 4-11-4 appears.

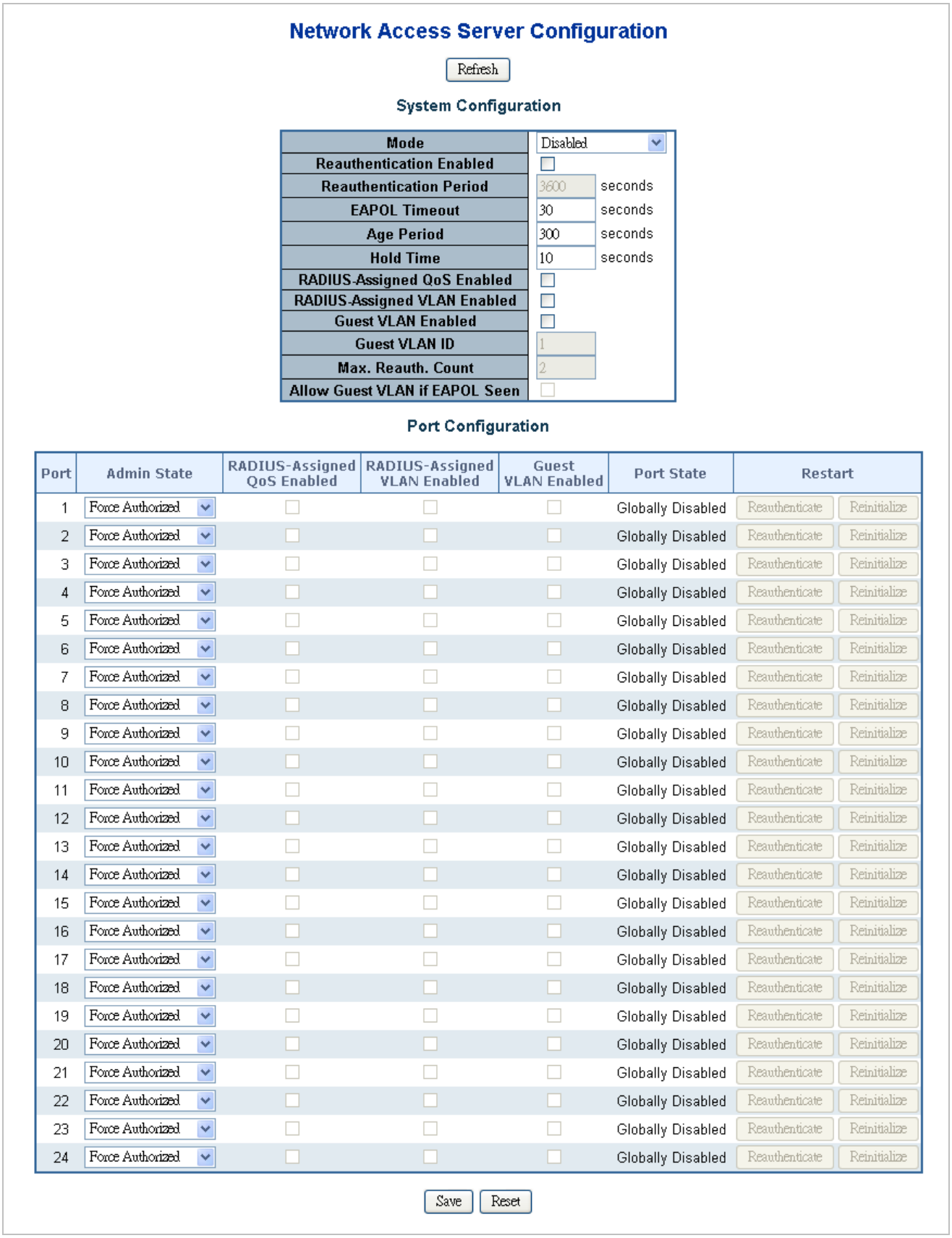


Figure 4-11-4 Network Access Server Configuration page screenshot

The page includes the following fields:

System Configuration

Object	Description
• **Mode**	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
• **Reauthentication Enabled**	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. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port.
• **Reauthentication Period**	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
• **EAPOL Timeout**	Determines the time between retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.
• **Age Period**	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: **Single 802.1X** **Multi 802.1X** **MAC-Based Auth**. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in a 802.1X-based mode, this is not so criticial, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

• **Hold Time**	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: **Single 802.1X** **Multi 802.1X** **MAC-Based Auth**. If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the The switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
• **RADIUS-Assigned QoS Enabled**	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled for that port. When unchecked, RADIUS-server assigned QoS Class is disabled for all ports.
• **RADIUS-Assigned VLAN Enabled**	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled for that port. When unchecked, RADIUS-server assigned VLAN is disabled for all ports.
• **Guest VLAN Enabled**	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

	The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled for all ports.
• **Guest VLAN ID**	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].
• **Max. Reauth. Count**	The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].
• **Allow Guest VLAN if EAPOL Seen**	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

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

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Admin State**	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.

Port-based 802.1X

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

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single

802.1X variant.
Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.
Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.
In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.
The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

MAC-based Auth.

Unlike port-based 802.1X, MAC-based authentication is not a standard, but

	merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.
• **RADIUS-Assigned QoS Enabled**	When RADIUS-Assigned QoS is both globally enabled and enabled (checked) for a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. • **Port-based 802.1X** • **Single 802.1X**

	RADIUS attributes used in identifying a QoS Class: Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule: All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].
• **RADIUS-Assigned VLAN Enabled**	- When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. **• Port-based 802.1X** **• Single 802.1X** For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. **RADIUS attributes used in identifying a VLAN ID:** RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used: - The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. - The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):

	- Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). - Value of Tunnel-Type must be set to "VLAN" (ordinal 13). - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].
• **Guest VLAN Enabled**	When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.: **• Port-based 802.1X** **• Single 802.1X** **• Multi 802.1X** For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. **Guest VLAN Operation:** When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

• **Port State**	The current state of the port. It can undertake one of the following values: **Globally Disabled**: NAS is globally disabled. **Link Down**: NAS is globally enabled, but there is no link on the port. **Authorized**: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. **Unauthorized**: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. **X Auth/Y Unauth**: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
• **Restart**	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. **Reauthenticate**: Schedules a reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized. **Reinitialize**: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons

Refresh: Click to refresh the page.

Save: Click to save changes.

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

4.11.4 Network Access Overview

This page provides an overview of the current NAS port states for the selected switch. The Network Access Overview screen in Figure 4-11-5 appears.

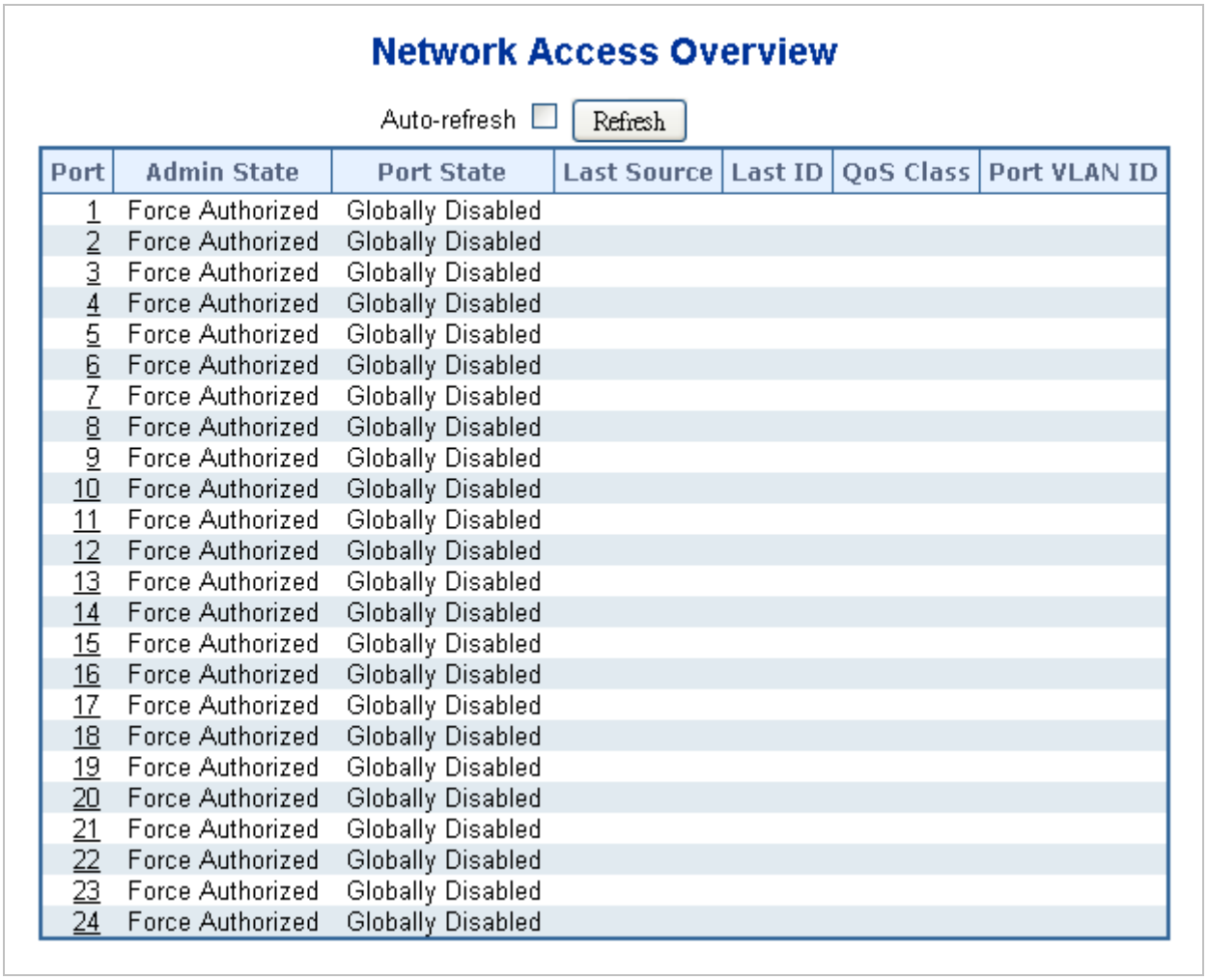


Figure 4-11-5 Network Access Overview page screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number. Click to navigate to detailed NAS statistics for this port.
• **Admin State**	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
• **Port State**	The current state of the port. Refer to NAS Port State for a description of the individual states.
• **Last Source**	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

• **Last ID**	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
• **Port VLAN ID**	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

Refresh: Click to refresh the page immediately.

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

4.11.5 Network Access Statistics

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed. The Network Access Statistics screen in Figure 4-11-6 appears.

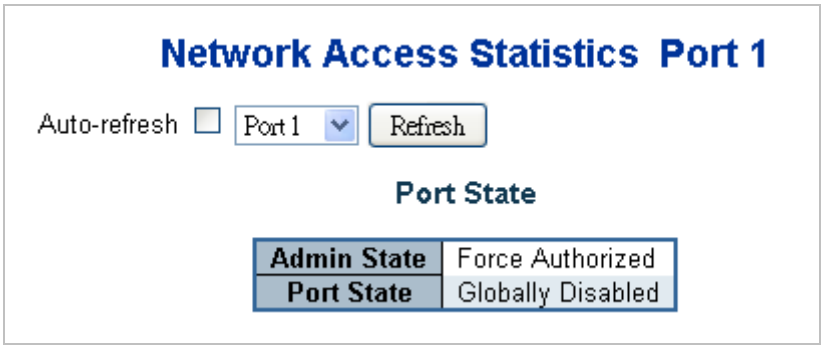


Figure 4-11-6 Network Access Statistics page screenshot

The page includes the following fields:

Port State

Object	Description
• **Admin State**	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
• **Port State**	The current state of the port. Refer to NAS Port State for a description of the individual states.

• **QoS Class**	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
• **Port VLAN ID**	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Port Counters

Object	Description
• **EAPOL Counters**	These supplicant frame counters are available for the following administrative states: **Force Authorized** **Force Unauthorized** **Port-based 802.1X** **Single 802.1X** **Multi 802.1X**

Direction	Name	IEEE Name	Description
Rx	**Total**	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	**Response ID**	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	**Responses**	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	**Start**	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	**Logoff**	dot1xAuthEapolLogoffFr	The number of valid EAPOL Logoff frames that have

			amesRx	been received by the switch.
	Rx	**Invalid Type**	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
	Rx	**Invalid Length**	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
	Tx	**Total**	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
	Tx	**Request ID**	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
	Tx	**Requests**	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

- **Backend Server Counters**

These backend (RADIUS) frame counters are available for the following administrative states:

Port-based 802.1X

Single 802.1X

Multi 802.1X

MAC-based Auth.

Direction	Name	IEEE Name	Description
Rx	**Access Challenges**	dot1xAuthBackendAccessChallenges	**802.1X-based**: Counts the number of times that the switch receives the first request from the backend

				server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
	Rx	**Other Requests**	dot1xAuthBackendOtherRequestsToSupplicant	**802.1X-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based**: Not applicable.
	Rx	**Auth. Successes**	dot1xAuthBackendAuthSuccesses	**802.1X- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
	Rx	**Auth. Failures**	dot1xAuthBackendAuthFails	**802.1X- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
	Tx	**Responses**	dot1xAuthBackendResponses	**802.1X-based:** Counts the number of times that the switch attempts to

		send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.
• **Last Supplicant/Client Info**	Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states: **Port-based 802.1X** **Single 802.1X** **Multi 802.1X** **MAC-based Auth**.	

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.
Identity	-	**802.1X-based**: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame.

	MAC-based: Not applicable.

Selected Counters

Object	Description
• **Selected Counters**	The Selected Counters table is visible when the port is one of the following administrative states: **Multi 802.1X** **MAC-based Auth**. The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Port Counters

Object	Description
• **Identity**	Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached. This column is not available for MAC-based Auth.
• **MAC Address**	For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.
• **VLAN ID**	This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.
• **State**	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
• **Last Authentication**	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: This button is available in the following modes:

Force Authorized

Force Unauthorized

Port-based 802.1X

Single 802.1X

Click to clear the counters for the selected port.

Clear All: This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.

Clear This: This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

4.11.6 Authentication Server Configuration

This page allows you to configure the Authentication Servers. The Authentication Server Configuration screen in Figure 4-11-7 appears.

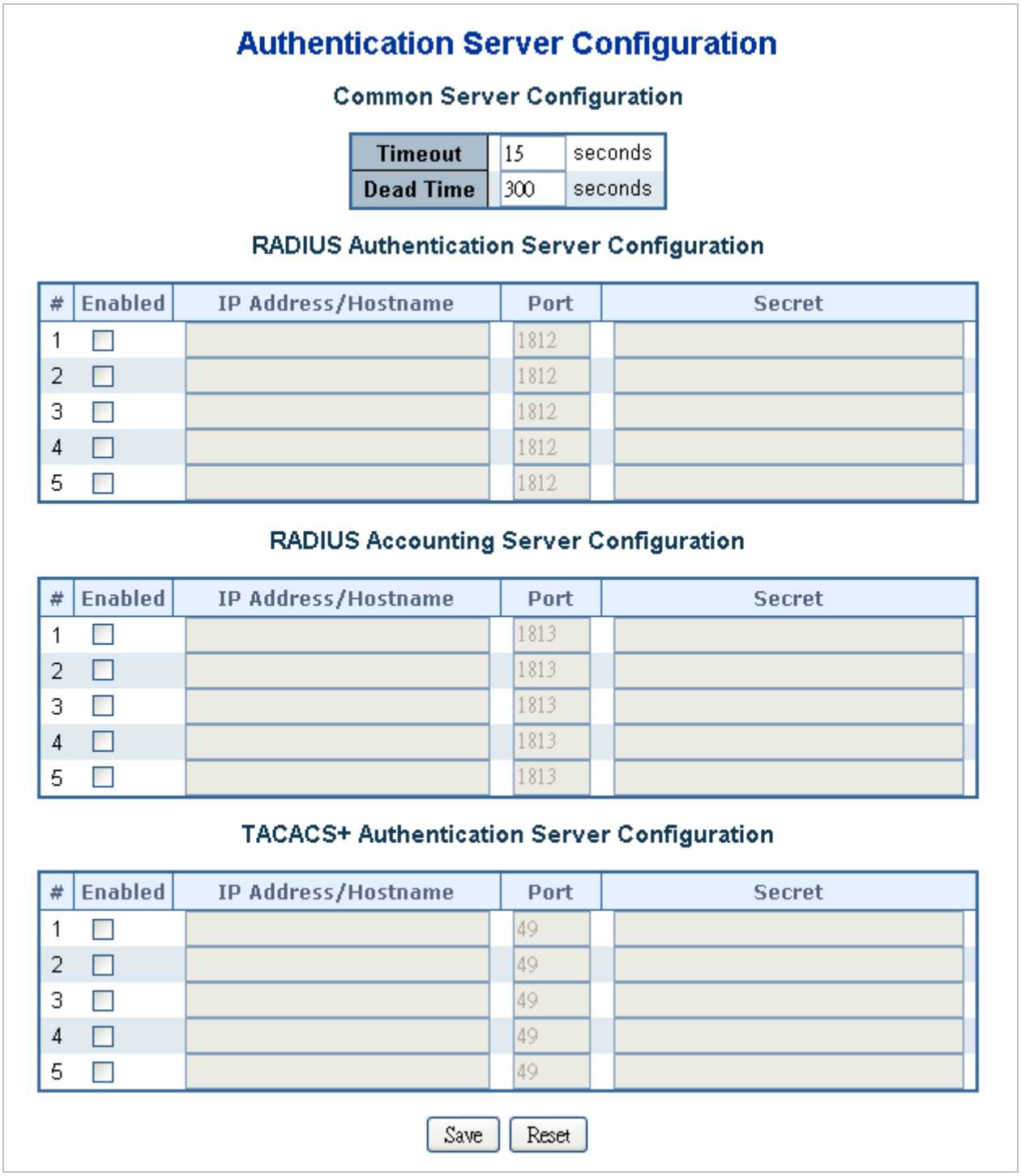


Figure 4-11-7 Authentication Server Configuration page screenshot

The page includes the following fields:

Port State

These setting are common for all of the Authentication Servers.

Object	Description
• **Timeout**	The Timeout, which can be set to a number between 3 and 3600 seconds, is the

	maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
• **Dead Time**	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

Object	Description
• #	The RADIUS Authentication Server number for which the configuration below applies.
• **Enabled**	Enable the RADIUS Authentication Server by checking this box.
• **IP Address/Hostname**	The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
• **Port**	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.
• **Secret**	The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.

RADIUS Accounting Server Configuration

The table has one row for each RADIUS Accounting Server and a number of columns, which are:

Object	Description
• #	The RADIUS Accounting Server number for which the configuration below

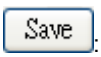
	applies.
• **Enabled**	Enable the RADIUS Accounting Server by checking this box.
• **IP Address/Hostname**	The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.
• **Port**	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
• **Secret**	The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch.

TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ Authentication Server and a number of columns, which are:

Object	Description
• #	The TACACS+ Authentication Server number for which the configuration below applies.
• **Enabled**	Enable the TACACS+ Authentication Server by checking this box.
• **IP Address/Hostname**	The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.
• **Port**	The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.
• **Secret**	The secret - up to 29 characters long - shared between the TACACS+ Authentication Server and the switch.

Buttons



: Click to save changes.

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

4.11.7 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page. The RADIUS Authentication/Accounting Server Overview screen in Figure 4-11-8 appears.

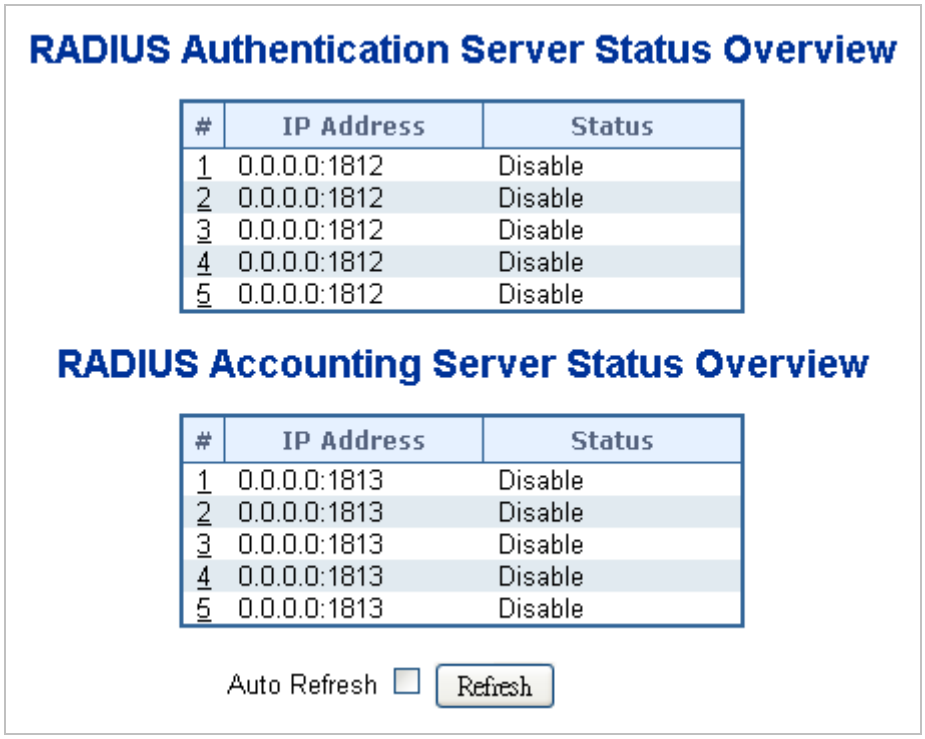


Figure 4-11-8 RADIUS Authentication/Accounting Server Overview page screenshot

The page includes the following fields:

RADIUS Authentication Servers

Object	Description
• #	The RADIUS server number. Click to navigate to detailed statistics for this server.
• **IP Address**	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
• **State**	The current state of the server. This field takes one of the following values: **Disabled**: The server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled,

	but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Servers

Object	Description
• #	The RADIUS server number. Click to navigate to detailed statistics for this server.
• **IP Address**	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
• **State**	The current state of the server. This field takes one of the following values: **Disabled**: The server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

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

Refresh: Click to refresh the page immediately.

4.11.8 RADIUS Details

This page provides detailed statistics for a particular RADIUS server. The RADIUS Authentication/Accounting for Server Overview screen in Figure 4-11-9 appears.

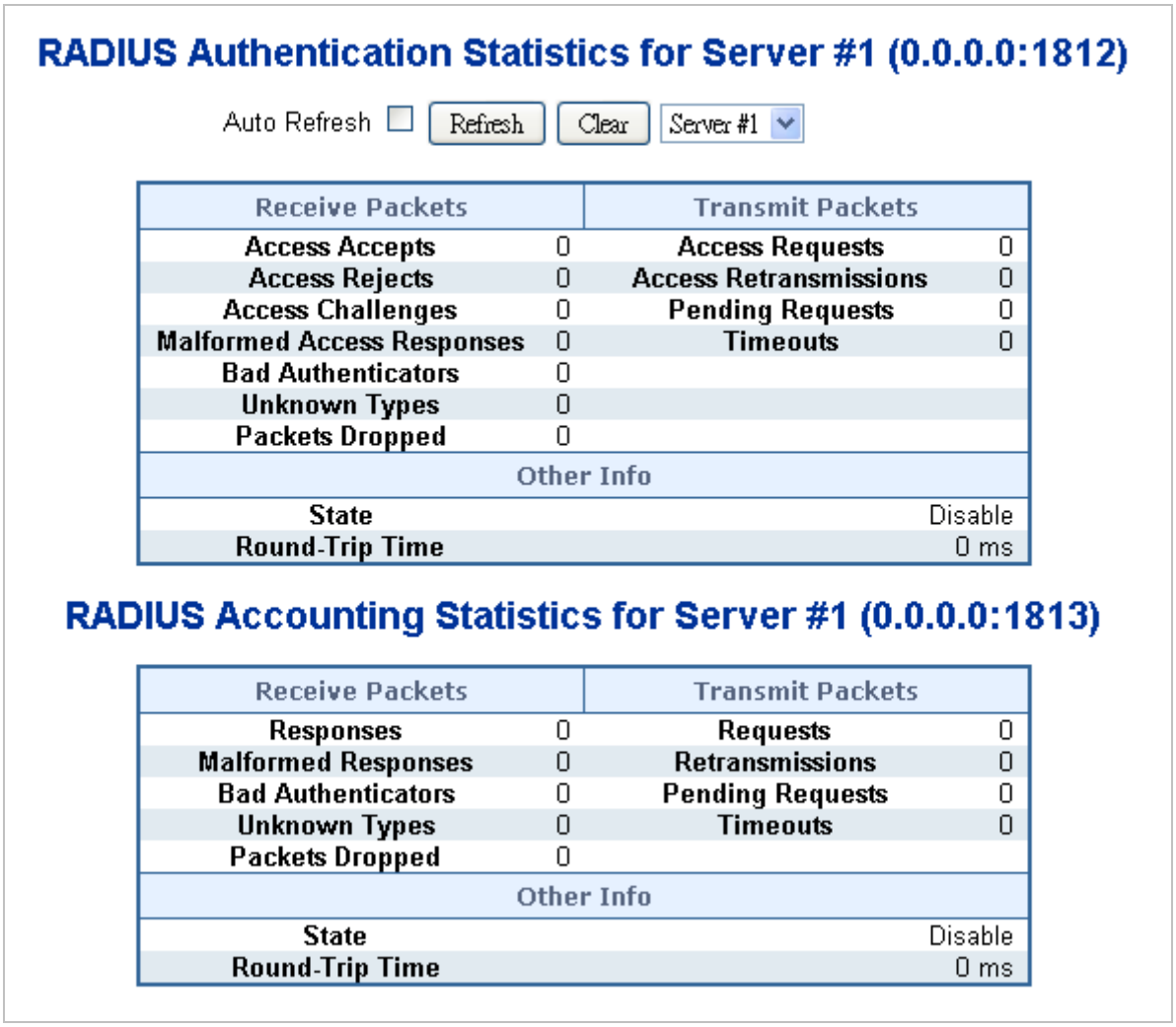


Figure 4-11-9 RADIUS Authentication/Accounting for Server Overview page screenshot

The page includes the following fields:

RADIUS Authentication Servers

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Use the server select box to switch between the backend servers to show details for.

Object	Description			
• **Packet Counters**	RADIUS authentication server packet counter. There are seven receive and four transmit counters.			
	Direction	**Name**	**RFC4668 Name**	**Description**
	Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
	Rx	**Access Rejects**	radiusAuthClientExtA	The number of RADIUS

			ccessRejects	Access-Reject packets (valid or invalid) received from the server.
	Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
	Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
	Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
	Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
	Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
	Tx	**Access**	radiusAuthClientExtA	The number of RADIUS Access-Request packets sent

		Requests	ccessRequests	to the server. This does not include retransmissions.
	Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
	Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
	Tx	**Timeouts**	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **Other Info**

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
State	-	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is

			up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
	Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Servers

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.

Use the server select box to switch between the backend servers to show details for.

Object	Description			
• **Packet Counters**	RADIUS accounting server packet counter. There are five receive and four transmit counters.			
	Direction	**Name**	**RFC4670 Name**	**Description**
	Rx	**Responses**	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
	Rx	**Malformed Responses**	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or or unknown types are not included as malformed access responses.

	Rx	**Bad Authenticators**	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
	Rx	**Unknown Types**	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
	Rx	**Packets Dropped**	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
	Tx	**Requests**	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
	Tx	**Retransmissions**	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
	Tx	**Pending Requests**	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
	Tx	**Timeouts**	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a

different server is counted as a Request as well as a timeout.

- **Other Info**

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
State	-	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. **Dead (X seconds left)**: Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

4.11.9 Windows Platform RADIUS Server Configuration

Setup the RADIUS server and assign the client IP address to the Managed switch. In this case, field in the default IP Address of the Managed Switch with 192.168.0.100. And also make sure the shared **secret key** is as same as the one you had set at the Managed Switch's 802.1x system configuration – **12345678** at this case.

1. Configure the IP Address of remote RADIUS server and secret key.

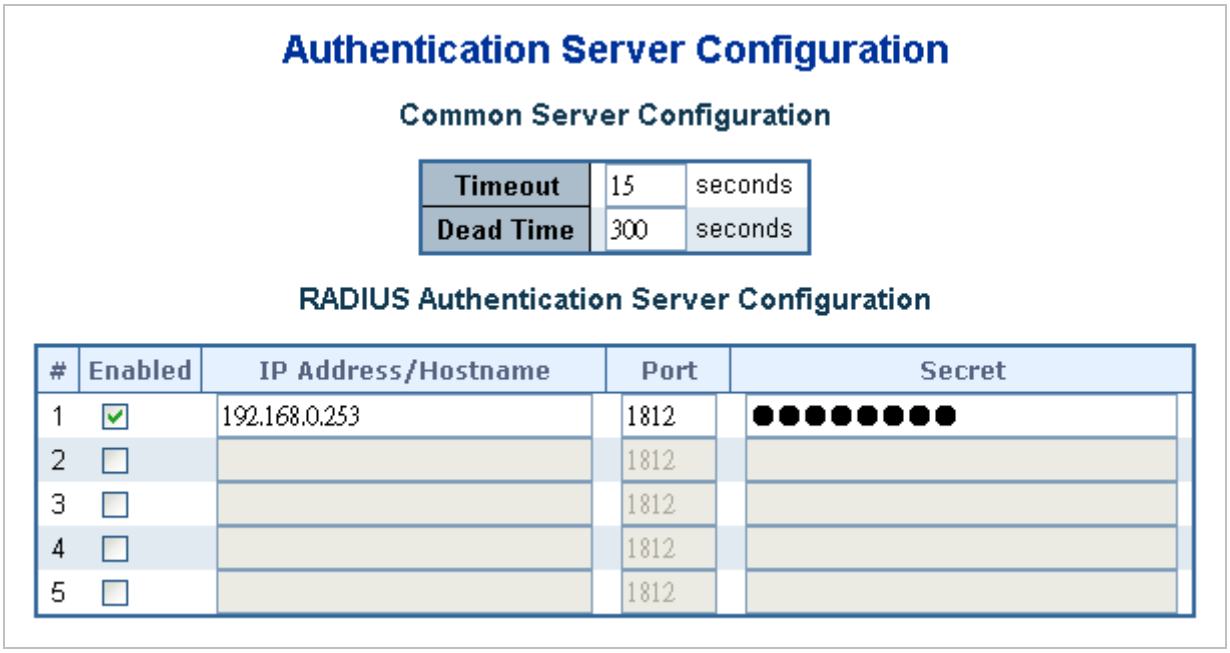


Figure 4-11-10 RADIUS Server Configuration screenshot

2. Add New RADIUS Cleint on the Windows 2003 server

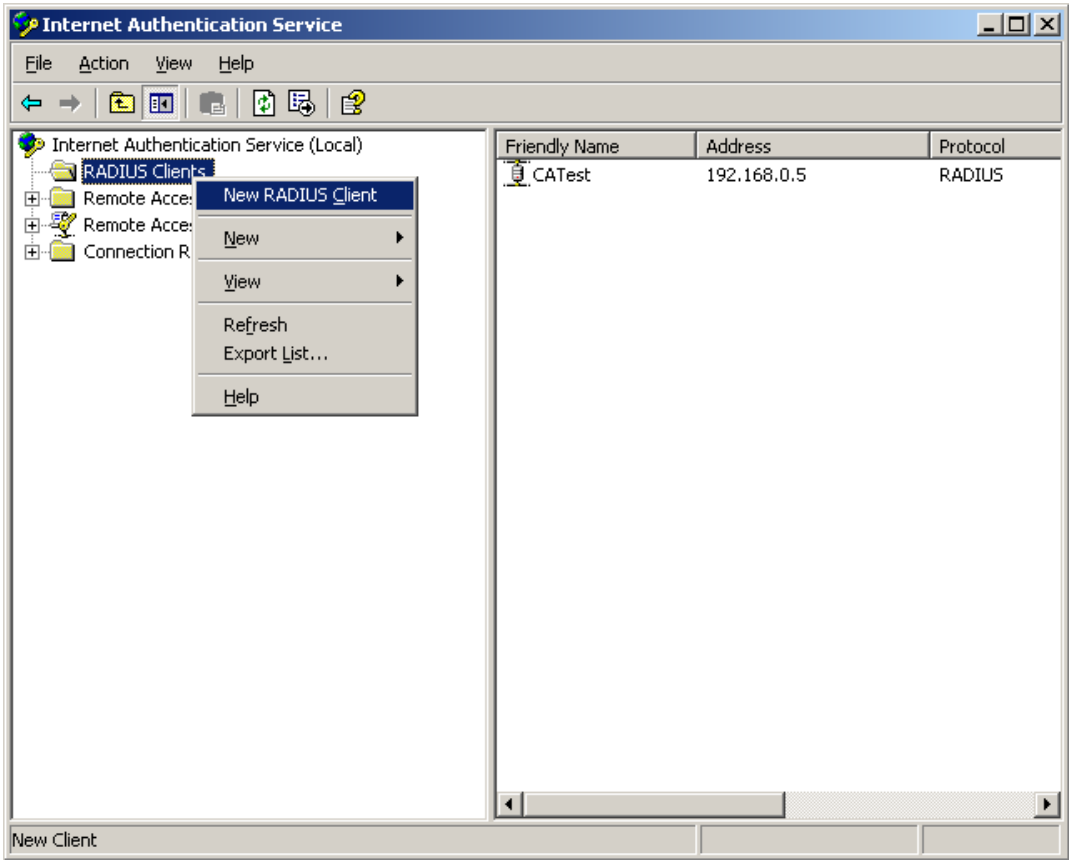


Figure 4-11-11 Windows Server – add new RADIUS client setting

3. Assign the client IP address to the Managed switch

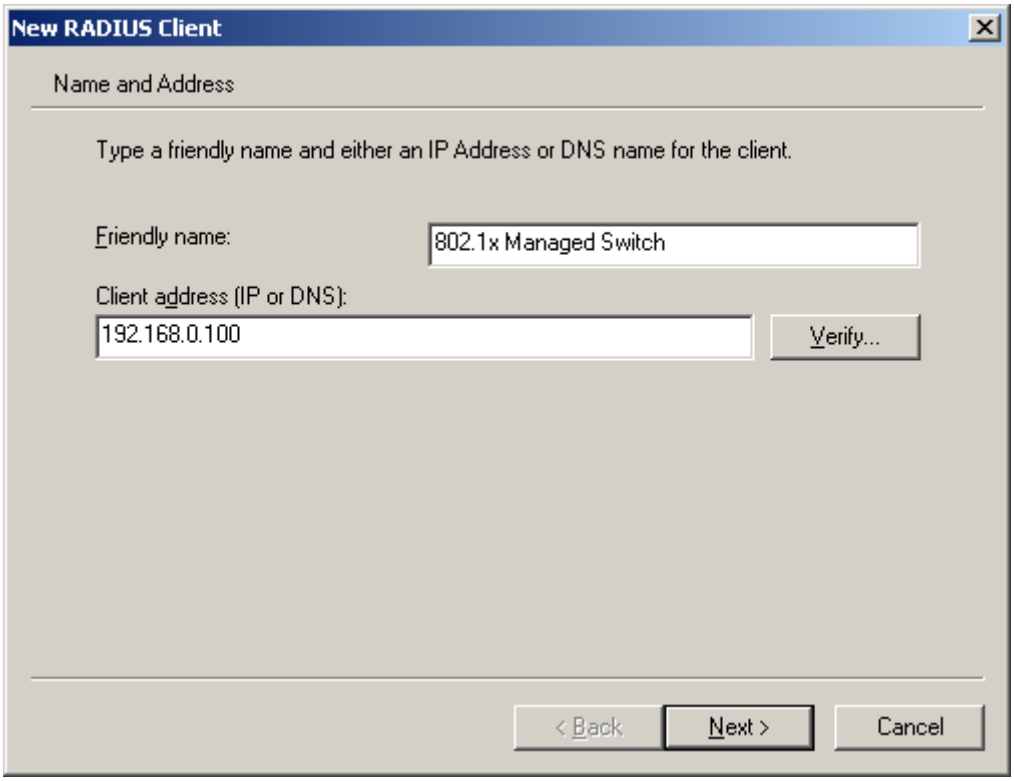


Figure 4-11-12 Windows Server RADIUS Server setting

4. The shared **secret key** should be as same as the key configured on the Managed Switch.

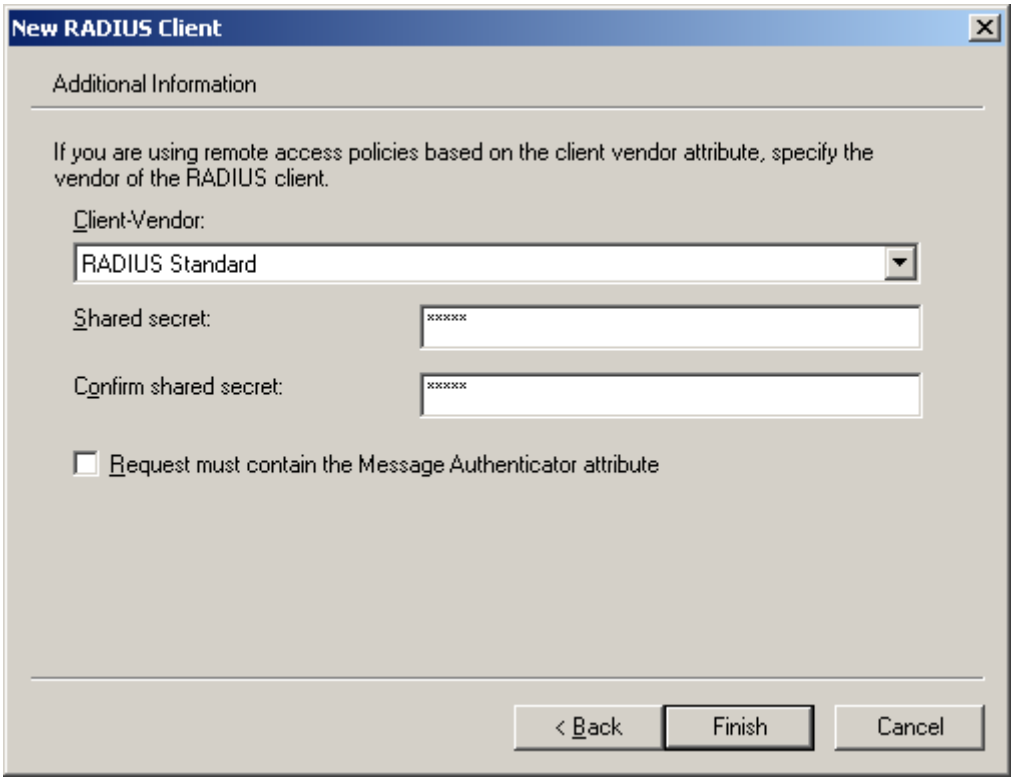


Figure 4-11-13 Windows Server RADIUS Server setting

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

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
1	Port-based 802.1X	☐	☐	☐	Globally Disabled	Reauthenticate / Reinitialize
2	Port-based 802.1X	☐	☐	☐	Globally Disabled	Reauthenticate / Reinitialize

Figure 4-11-14 802.1x Port Configuration

6. Create user data. The establishment of the user data needs to be created on the Radius Server PC. For example, the Radius Server founded on Win2003 Server, and then:

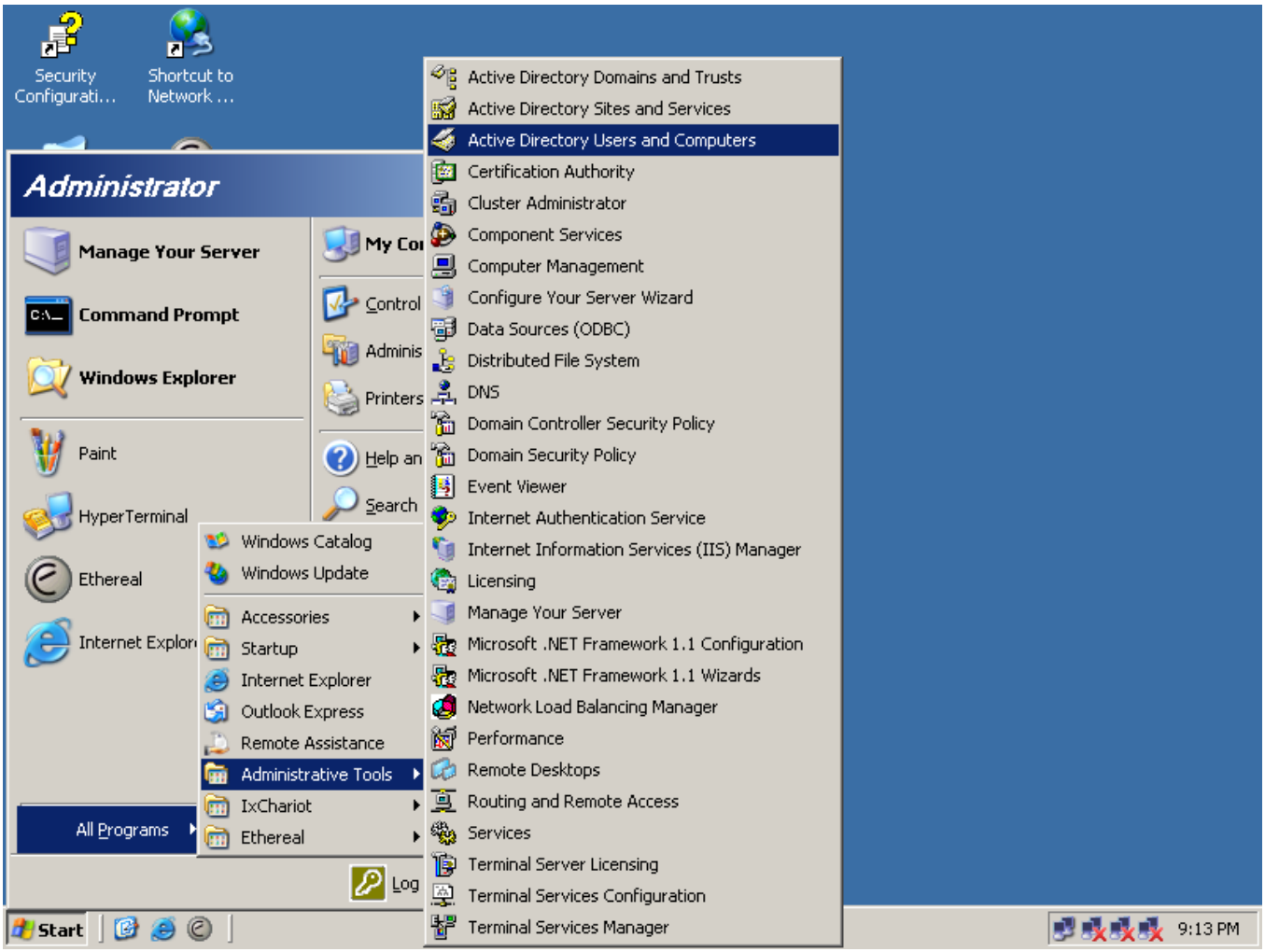


Figure 4-11-15 Windows 2003 AD server setting path

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

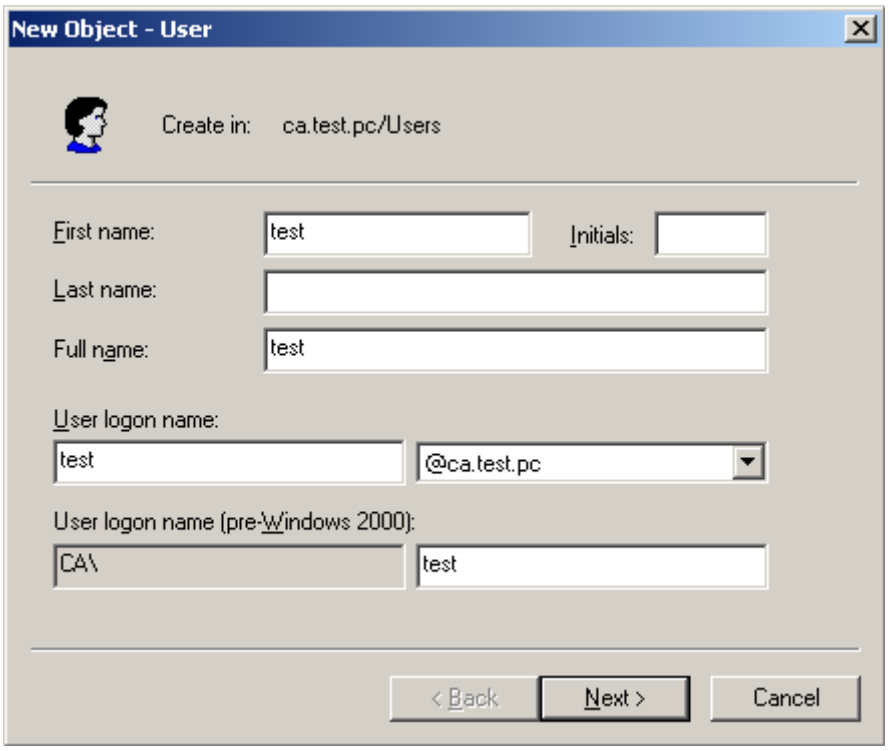


Figure 4-11-16 Add User Properties screen

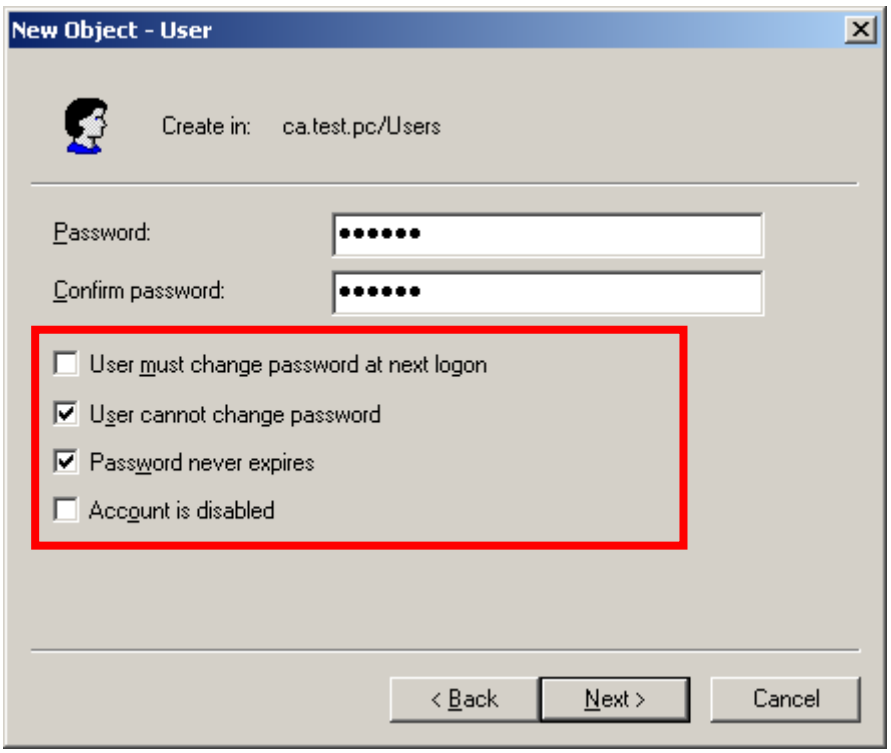


Figure 4-11-17 Add User Properties screen

Note

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

4.11.10 802.1X Client Configuration

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

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

■ Configure Sample: EAP-MD5 Authentication

1. Go to **Start** > **Control Panel,** double-click on "**Network Connections**".
2. Right-click on the Local Network Connection.
3. Click "**Properties**" to open up the Properties setting window.

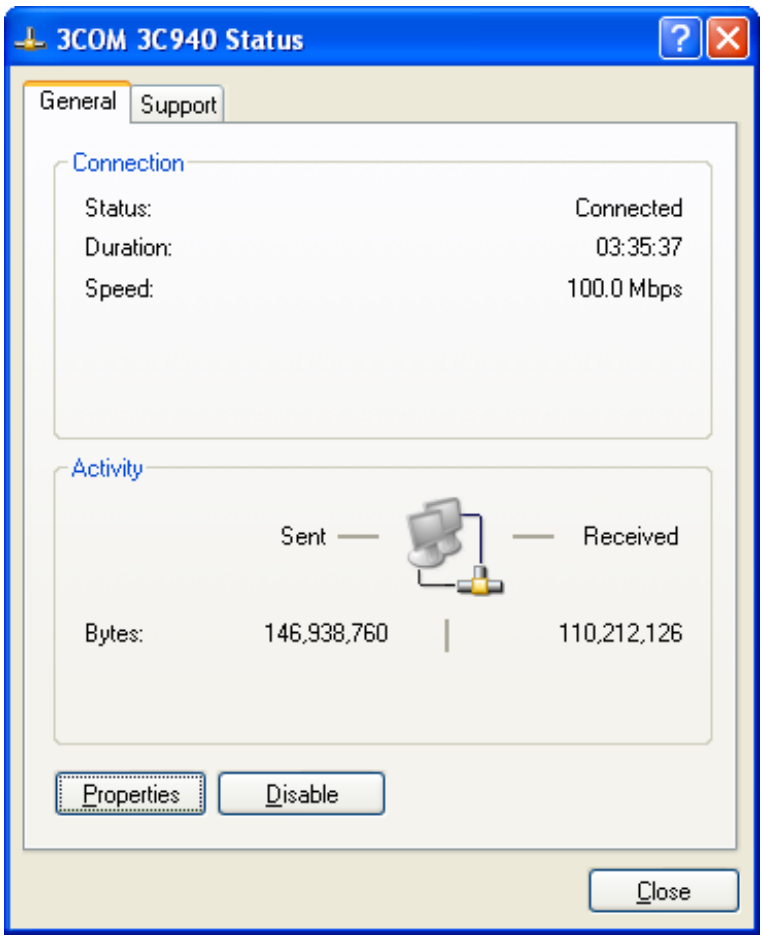


Figure 4-11-18

4. Select "**Authentication**" tab.
5. Select "**Enable network access control using IEEE 802.1X**" to enable 802.1x authentication.
6. Select "**MD-5 Challenge**" from the drop-down list box for EAP type.

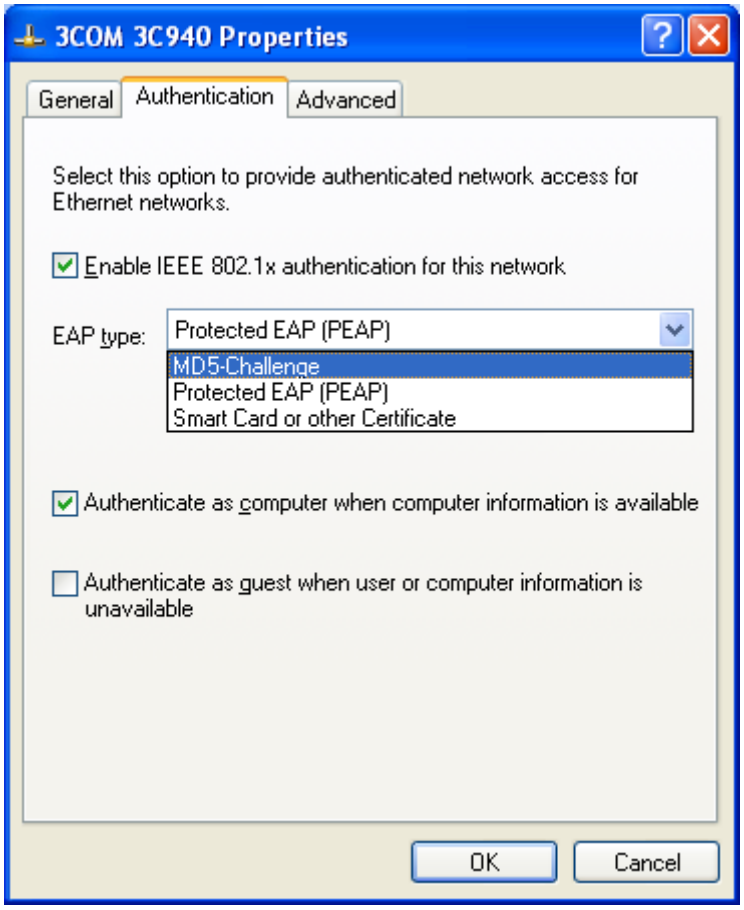


Figure 4-11-19

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

Figure 4-11-20 Windows client popup login request message

9. Enter the user name, password and the logon domain that your account belongs.
10. Click "**OK**" to complete the validation process.

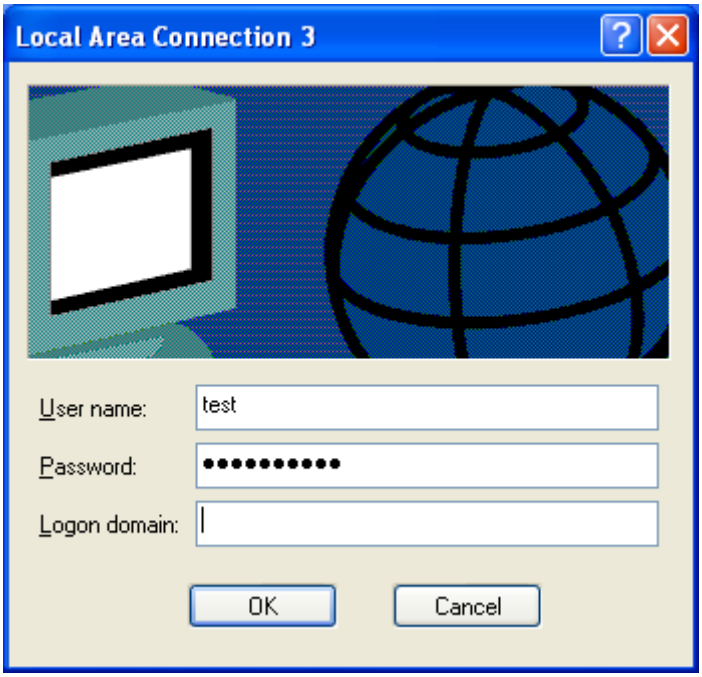


Figure 4-11-21

4.12 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:

- **Port Limit Control**
- **Access Management**
- **HTTPs / SSH**
- **DHCP Snooping**
- **IP Source Guard**
- **ARP Inspection**

4.12.1 Port Limit Control

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 Limit Control Configuration screen in Figure 4-12-1 appears.

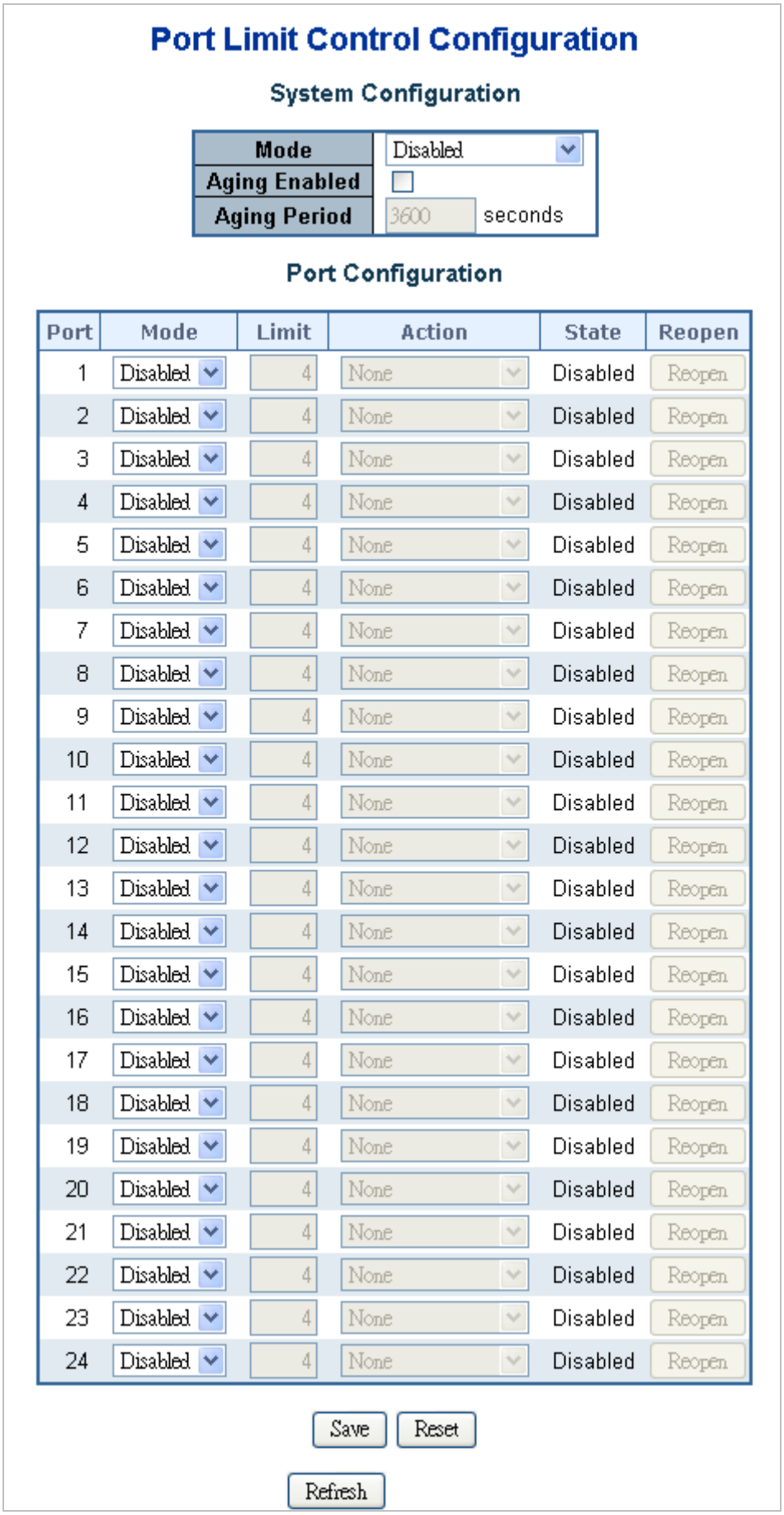


Figure 4-12-1 Port Limit Control Configuration Overview page screenshot

The page includes the following fields:

System Configuration

Object	Description
• **Mode**	Indicates if Limit Control is globally enabled or disabled on the switchstack. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
• **Aging Enabled**	If checked, secured MAC addresses are subject to aging as discussed under Aging Period.
• **Aging Period**	If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

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

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Mode**	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

• **Limit**	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The 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.
• **Action**	If Limit is reached, the switch can take one of the following actions: **None**: Do not allow more than Limit MAC addresses on the port, but take no further action. **Trap**: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent everytime the limit gets exceeded. **Shutdown**: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Boot the stack or elect a new masterthe switch, 2) Disable and re-enable Limit Control on the port or the stackswitch, 3) Click the Reopen button. **Trap & Shutdown**: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.
• **State**	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: **Disabled**: Limit Control is either globally disabled or disabled on the port. **Ready**: The limit is not yet reached. This can be shown for all actions. **Limit Reached**: Indicates that the limit is reached on this port. This state can only be shown if Action is set to **None** or **Trap**. **Shutdown**: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to **Shutdown** or **Trap & Shutdown**.
• **Reopen Button**	If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to **Shutdown** in the Action section. Note, that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

Buttons

Refresh: Click to refresh the page. Note that non-committed changes will be lost.

Save: Click to save changes.

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

4.12.2 Access Management

Configure access management table on this page. The maximum entry number is 16. If the application's type match any one of access management entry, it will allow to access the switch. The Access Management Configuration screen in Figure 4-12-2 appears.

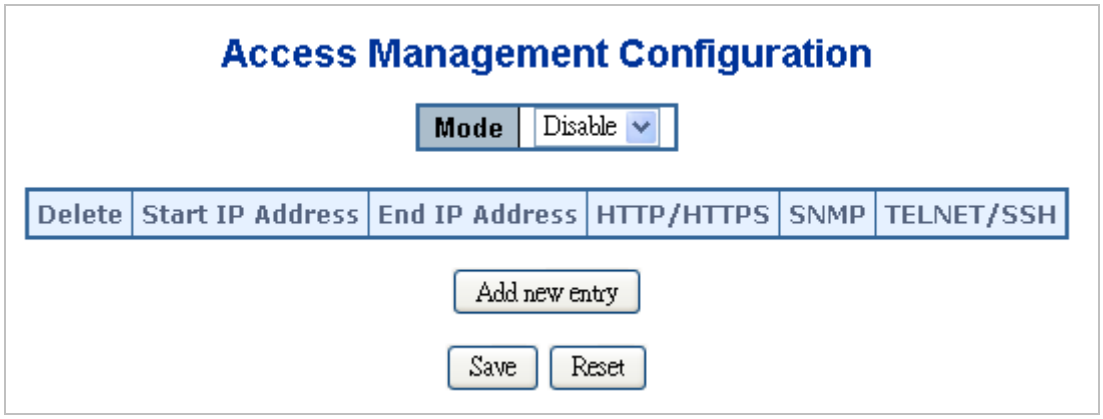


Figure 4-12-2 Access Management Configuration Overview page screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the access management mode operation. Possible modes are: **Enabled**: Enable access management mode operation. **Disabled**: Disable access management mode operation.
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Start IP address**	Indicates the start IP address for the access management entry.
• **End IP address**	Indicates the end IP address for the access management entry.
• **HTTP/HTTPS** •	Indicates the host can access the switch from HTTP/HTTPS interface that the host IP address matched the entry.
• **SNMP**	Indicates the host can access the switch from SNMP interface that the host IP address matched the entry.
• **TELNET/SSH**	Indicates the host can access the switch from TELNET/SSH interface that the

	host IP address matched the entry.

Buttons

Add new entry: Click to add a new access management entry.

Save: Click to save changes.

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

4.12.3 Access Management Statistics

This page provides statistics for access management. The Access Management Statistics screen in Figure 4-12-3 appears.

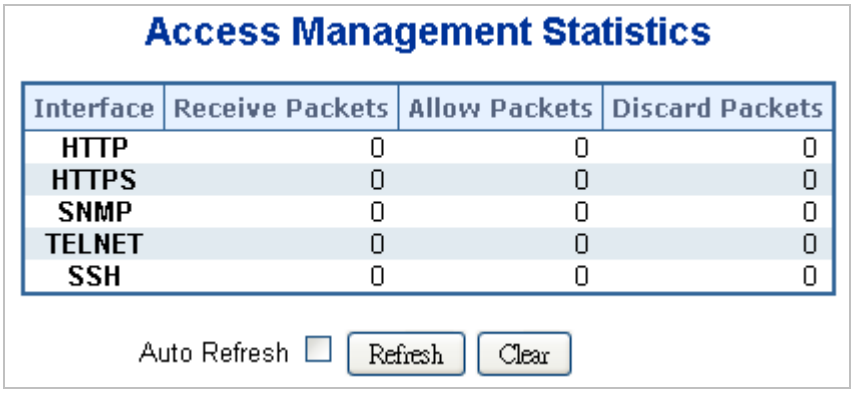


Figure 4-12-3 Access Management Statistics Overview page screenshot

The page includes the following fields:

Object	Description
• **Interface**	The interface that allowed remote host can access the switch.
• **Receive Packets**	The received packets number from the interface under access management mode is enabled.
• **Allow Packets**	The allowed packets number from the interface under access management mode is enabled.
• **Discard Packets**	The discarded packets number from the interface under access management mode is enabled.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clear all statistics.

4.12.4 HTTPs

Configure HTTPS on this page. The HTTPS Configuration screen in Figure 4-12-4 appears.

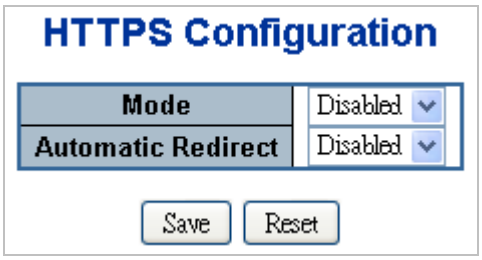


Figure 4-12-4 HTTPS Configuration screen page screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the HTTPS mode operation. Possible modes are: **Enabled**: Enable HTTPS mode operation. **Disabled**: Disable HTTPS mode operation.
• **Automatic Redirect**	Indicates the HTTPS redirect mode operation. Automatic redirect web browser to HTTPS during HTTPS mode enabled. Possible modes are: **Enabled**: Enable HTTPS redirect mode operation. **Disabled**: Disable HTTPS redirect mode operation.

Buttons

Save: Click to save changes.

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

4.12.5 SSH

Configure SSH on this page. This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status. The SSH Configuration screen in Figure 4-12-5 appears.

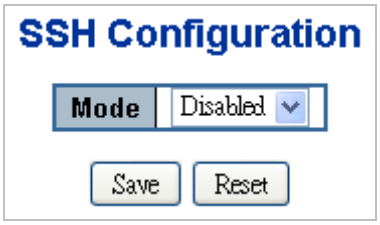


Figure 4-12-5 SSH Configuration screen page screenshot

The page includes the following fields:

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

Buttons

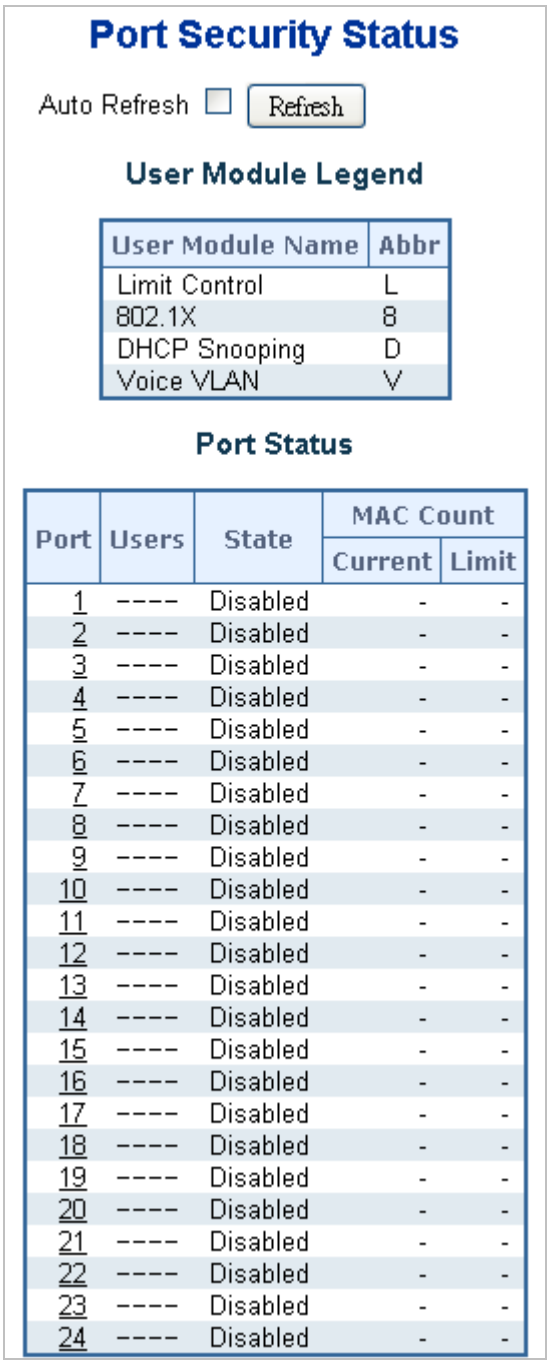
Save: Click to save changes.

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

4.12.6 Port Security Status

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status. The Port Security Status screen in Figure 4-12-6 appears.



Port Security Status

Auto Refresh ☐ Refresh

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-
9	----	Disabled	-	-
10	----	Disabled	-	-
11	----	Disabled	-	-
12	----	Disabled	-	-
13	----	Disabled	-	-
14	----	Disabled	-	-
15	----	Disabled	-	-
16	----	Disabled	-	-
17	----	Disabled	-	-
18	----	Disabled	-	-
19	----	Disabled	-	-
20	----	Disabled	-	-
21	----	Disabled	-	-
22	----	Disabled	-	-
23	----	Disabled	-	-
24	----	Disabled	-	-

Figure 4-12-6 Port Security Status screen page screenshot

The page includes the following fields:

User Module Legend

The legend shows all user modules that may request Port Security services.

Object	Description
• **User Module Name**	The full name of a module that may request Port Security services.
• **Abbr**	A one-letter abbreviation of the user module. This is used in the Users column in

	the port status table.

Port Status

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

Object	Description
• **Port**	The port number for which the status applies. Click the port number to see the status for this particular port.
• **Users**	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
• **State**	Shows the current state of the port. It can take one of four values: **Disabled**: No user modules are currently using the Port Security service. **Ready**: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. **Limit Reached**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. **Shutdown**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.
• **MAC Count (Current, Limit)**	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

Refresh: Click to refresh the page immediately.

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

4.12.7 Port Security Detail

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The Port Security Detail screen in Figure 4-12-7 appears.

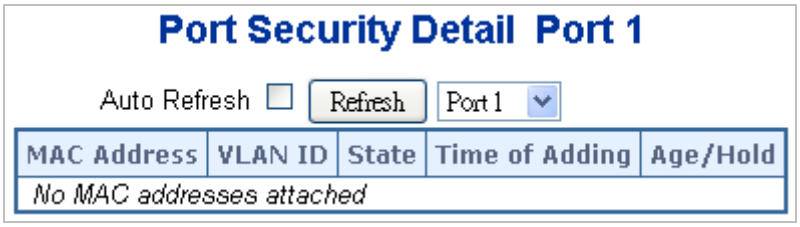


Figure 4-12-7 Port Security Detail screen page screenshot

The page includes the following fields:

Object	Description
• **MAC Address & VLAN ID**	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
• **State**	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
• **Time of Adding**	Shows the date and time when this MAC address was first seen on the port.
• **Age/Hold**	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

Refresh: Click to refresh the page immediately.

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

4.12.8 DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of DUT when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server. Configure DHCP Snooping on this page. The DHCP Snooping Configuration screen in Figure 4-12-8 appears.

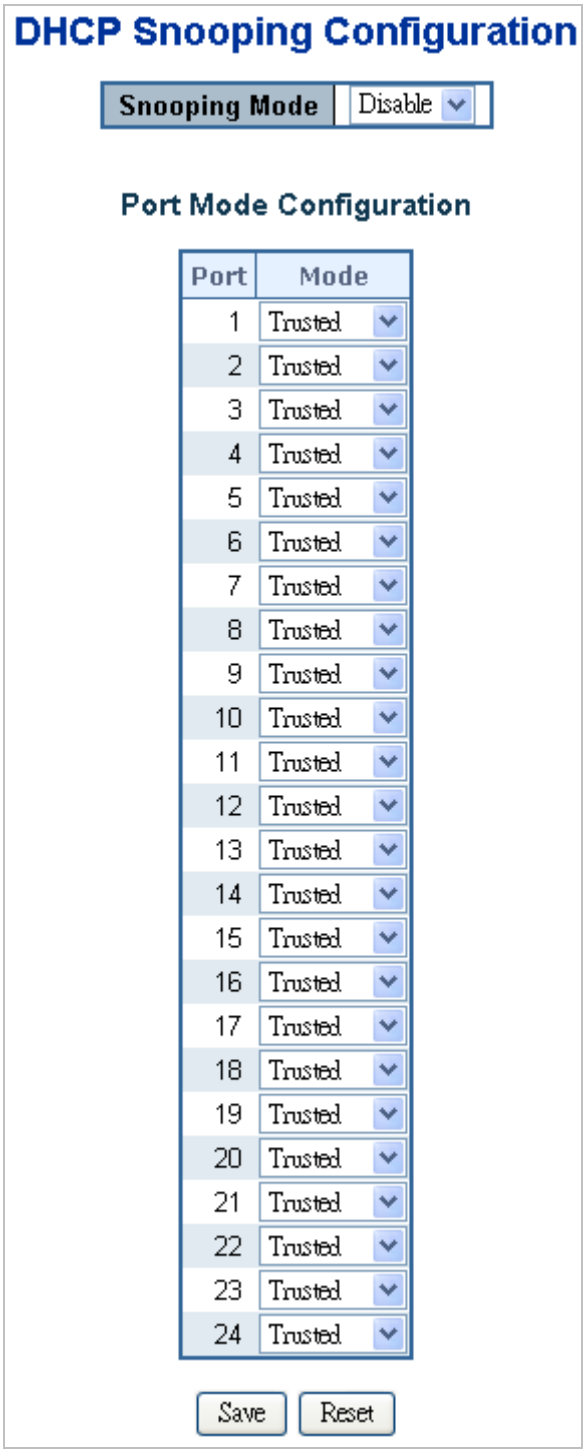


Figure 4-12-8 DHCP Snooping Configuration screen page screenshot

The page includes the following fields:

Object	Description
• **Snooping Mode**	Indicates the DHCP snooping mode operation. Possible modes are: **Enabled**: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. **Disabled**: Disable DHCP snooping mode operation.
• **Port Mode**	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted sources of the DHCP message. **Untrusted**: Configures the port as untrusted sources of the DHCP message.

Buttons

Save: Click to save changes.

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

4.12.9 DHCP Snooping Statistics

This page provides statistics for DHCP snooping. The statistics only counter packet under DHCP snooping mode is enabled and relay mode is disabled. And it doesn't count the DHCP packets for system DHCP client. The DHCP Snooping Port Statistics screen in Figure 4-12-9 appears.

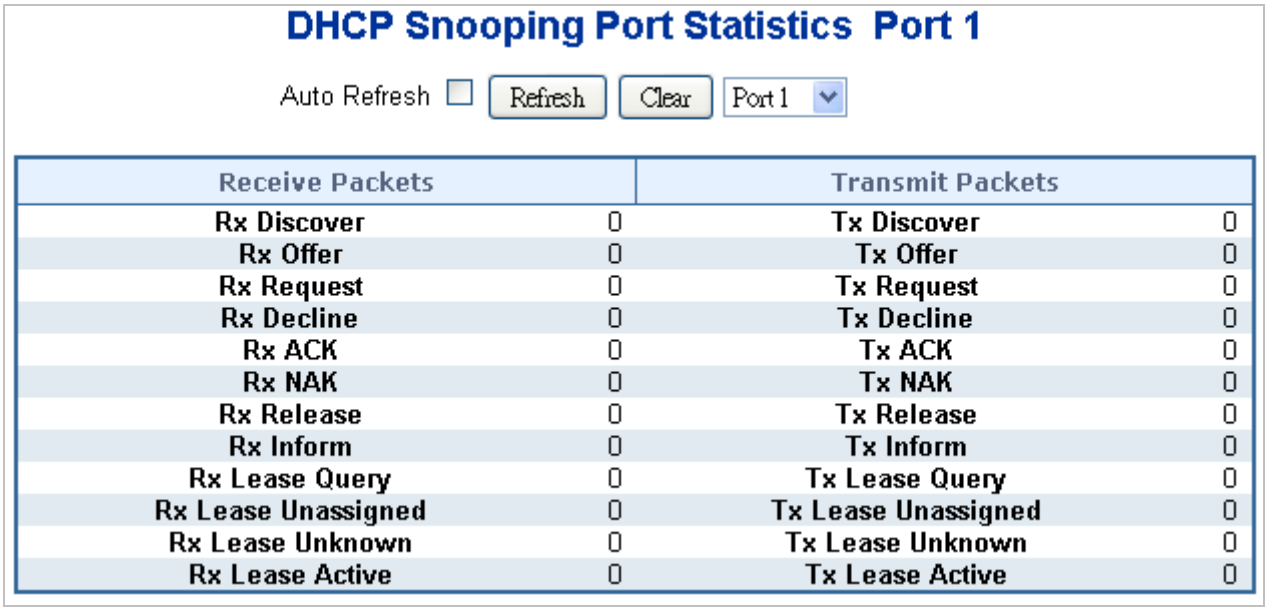


Figure 4-12-9 DHCP Snooping Port Statistics screen page screenshot

The page includes the following fields:

Object	Description
• **Rx and Tx Discover**	The number of discover (option 53 with value 1) packets received and transmitted.
• **Rx and Tx Offer**	The number of offer (option 53 with value 2) packets received and transmitted.
• **Rx and Tx Request**	The number of request (option 53 with value 3) packets received and transmitted.
• **Rx and Tx Decline**	The number of decline (option 53 with value 4) packets received and transmitted.
• **Rx and Tx ACK**	The number of ACK (option 53 with value 5) packets received and transmitted.
• **Rx and Tx NAK**	The number of NAK (option 53 with value 6) packets received and transmitted.
• **Rx and Tx Release**	The number of release (option 53 with value 7) packets received and transmitted.
• **Rx and Tx Inform**	The number of inform (option 53 with value 8) packets received and transmitted.
• **Rx and Tx Lease Query**	The number of lease query (option 53 with value 10) packets received and transmitted.
• **Rx and Tx Lease Unassigned**	The number of lease unassigned (option 53 with value 11) packets received and transmitted.
• **Rx and Tx Lease Unknown**	The number of lease unknown (option 53 with value 12) packets received and transmitted.
• **Rx and Tx Lease Active**	The number of lease active (option 53 with value 13) packets received and transmitted.

Buttons

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

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

4.12.10 IP Source Guard Configuration

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. This page provides IP Source Guard related configuration. The IP Source Guard Configuration screen in Figure 4-12-10 appears.

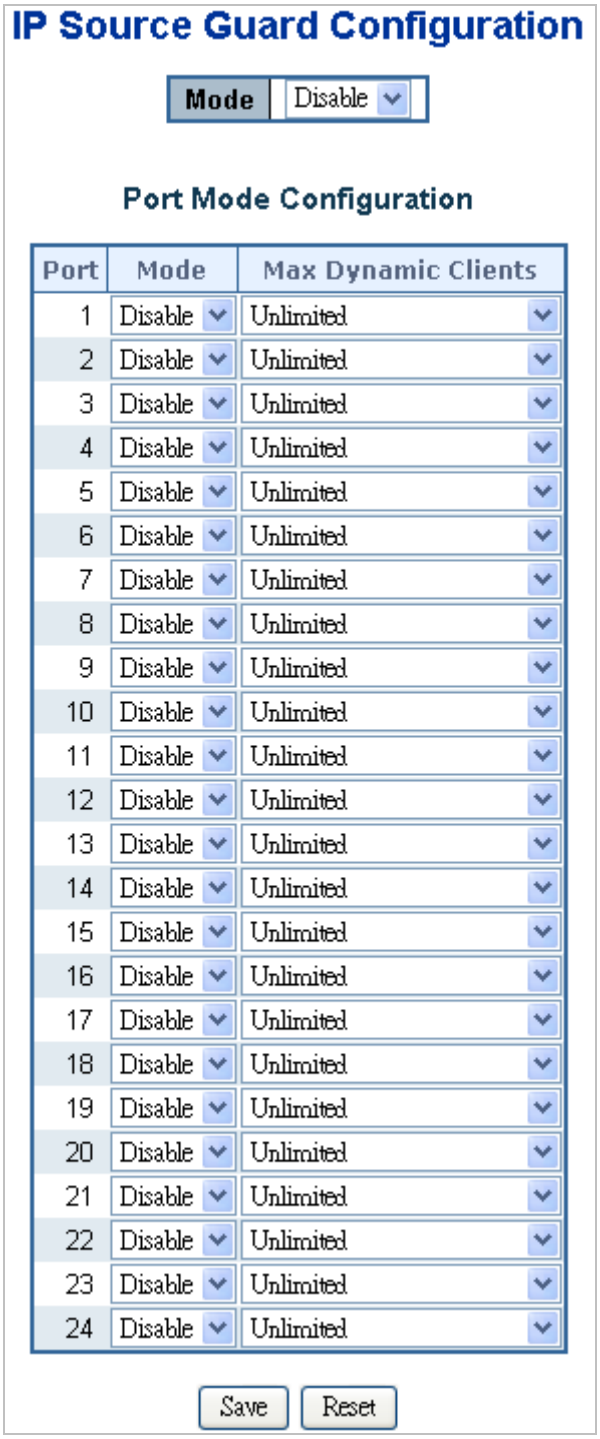


Figure 4-12-10 IP Source Guard Configuration screen page screenshot

The page includes the following fields:

Object	Description
• **Mode of IP Source Guard Configuration**	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
• **Port Mode Configuration**	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this

	given port.
• **Max Dynamic Clients**	Specify the maximum number of dynamic clients can be learned on given ports. This value can be 0, 1, 2 and unlimited. If the port mode is enabled and the value of max dynamic client is equal 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

Save: Click to save changes.

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

4.12.11 IP Source Guard Static Table

This page provides Static IP Source Guard Table. The Static IP Source Guard Table screen in Figure 4-12-11 appears.

Figure 4-12-11 Static IP Source Guard Table screen page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **VLAN ID**	The VLAN ID for the settings.
• **IP Address**	Allowed Source IP address.
• **IP Mask**	It can be used for calculating the allowed network with IP address.

Buttons

Add new entry: Click to add a new entry.

Save: Click to save changes.

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

4.12.12 ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT. This page provides ARP Inspection related configuration. The ARP Inspection Configuration screen in Figure 4-12-12 appears.

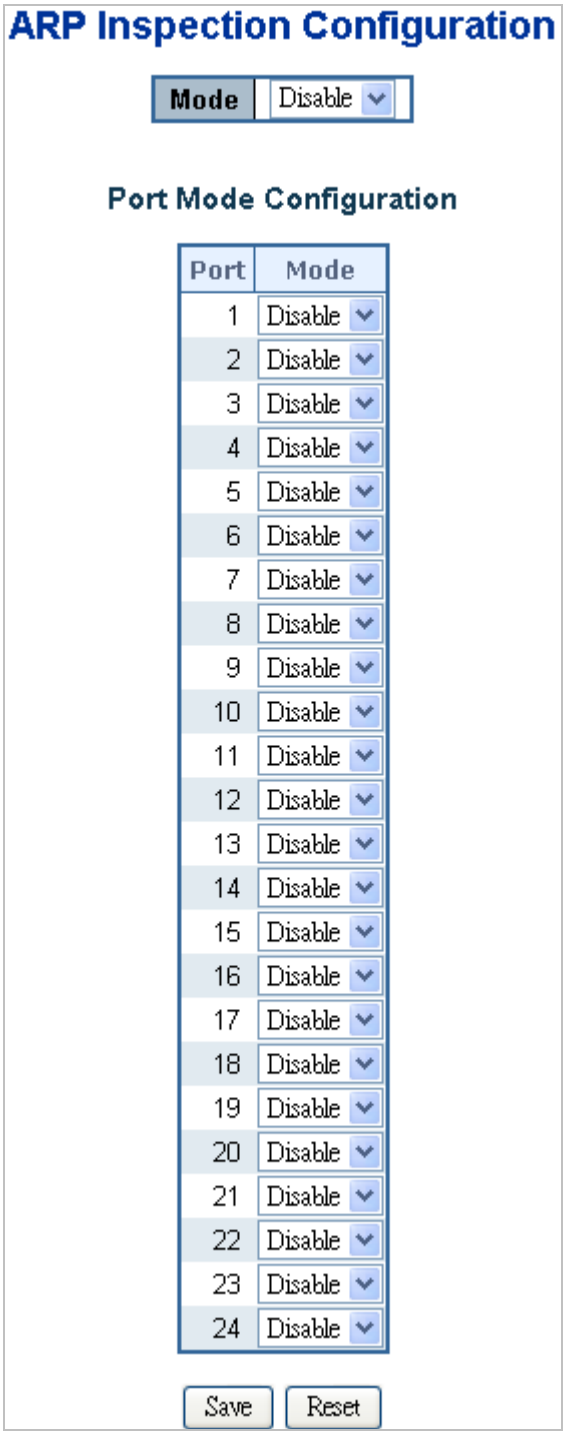


Figure 4-12-12 ARP Inspection Configuration screen page screenshot

The page includes the following fields:

Object	Description
• **Mode of ARP Inspection Configuration**	Enable the Global ARP Inspection or disable the Global ARP Inspection.
• **Port Mode Configuration**	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this

	given port.

Buttons

Save: Click to save changes.

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

4.12.13 ARP Inspection Static Table

This page provides Static ARP Inspection Table. The Static ARP Inspection Table screen in Figure 4-12-13 appears.

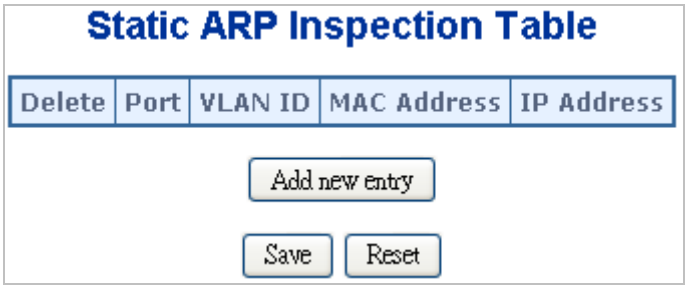


Figure 4-12-13 Static ARP Inspection Table screen page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **VLAN ID**	The VLAN ID for the settings.
• **MAC Address**	Allowed Source MAC address in ARP request packets.
• **IP Address**	Allowed Source IP address in ARP request packets.

Buttons

Add new entry: Click to add a new entry.

Save: Click to save changes.

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

4.13 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.

4.13.1 MAC Address Table Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here. The MAC Address Table Configuration screen in Figure 4-13-1 appears.

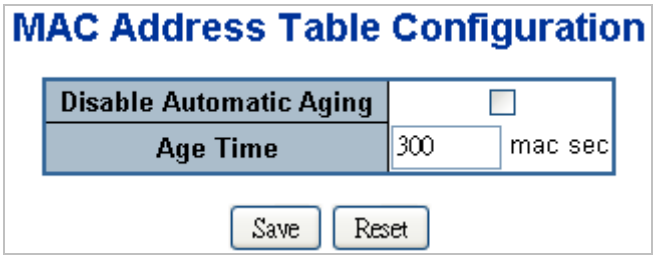


Figure 4-13-1 MAC Address Table Configuration page screenshot

The page includes the following fields:

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

Buttons

Save: Click to save changes.

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

4.13.2 Static MAC Table Configuration

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

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

The MAC table is sorted first by VLAN ID and then by MAC address. The Static MAC Table Configuration screen in Figure 4-13-2 appears.

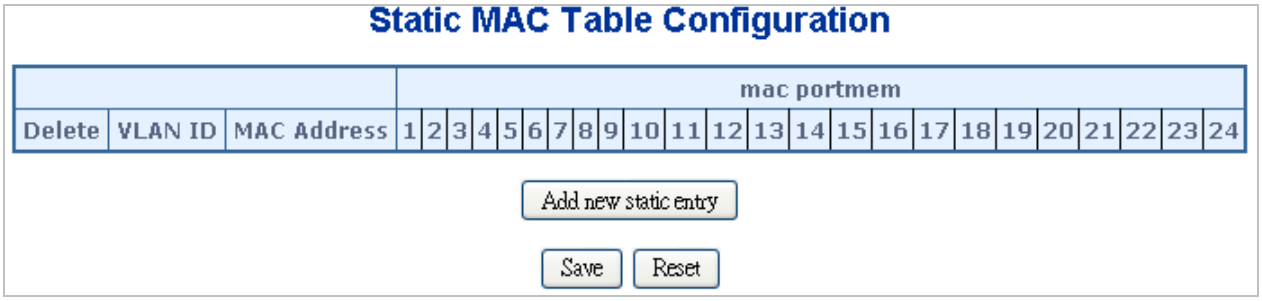


Figure 4-13-2 Static MAC Table Configuration page screenshot

The page includes the following fields:

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

Buttons

Add new static entry: Click to add new entry.

Save: Click to save changes.

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

4.13.3 MAC Address Table Status

Dynamic MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to **8192** entries, and is sorted first by VLAN ID, then by MAC address. The MAC Address Table screen in Figure 4-13-3 appears.

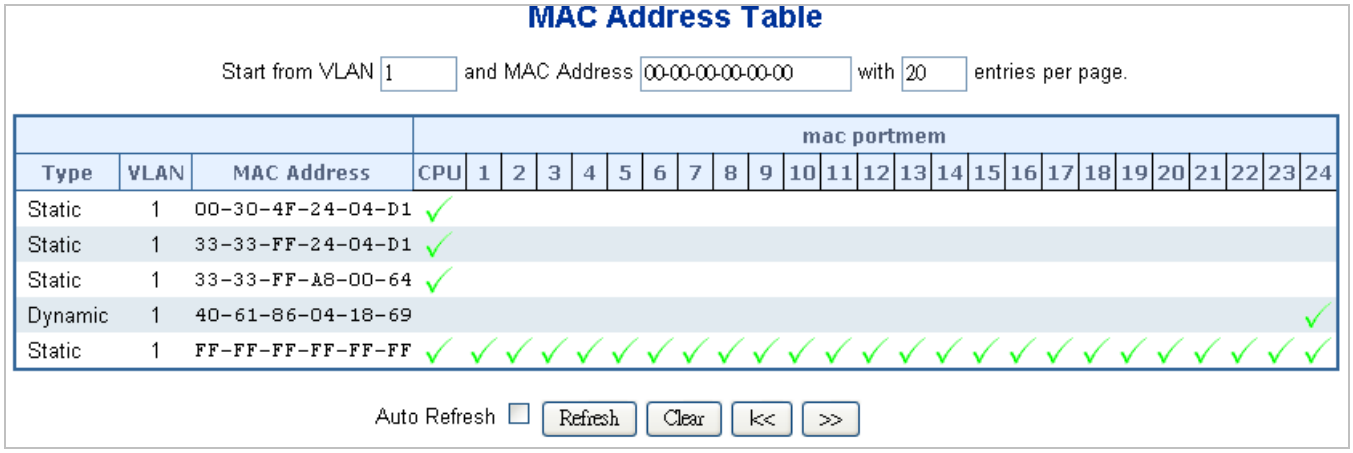


Figure 4-13-3 MAC Address Table Status

Navigating the MAC Table

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

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

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

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

The page includes the following fields:

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

Buttons

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

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

Clear: Flushes all dynamic entries.

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

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

4.13.4 MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:

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

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

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

Note that you can also manually add secure addresses to the port using the Static Address Table. The selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch. The MAC Table Learning screen in Figure 4-13-4 appears.

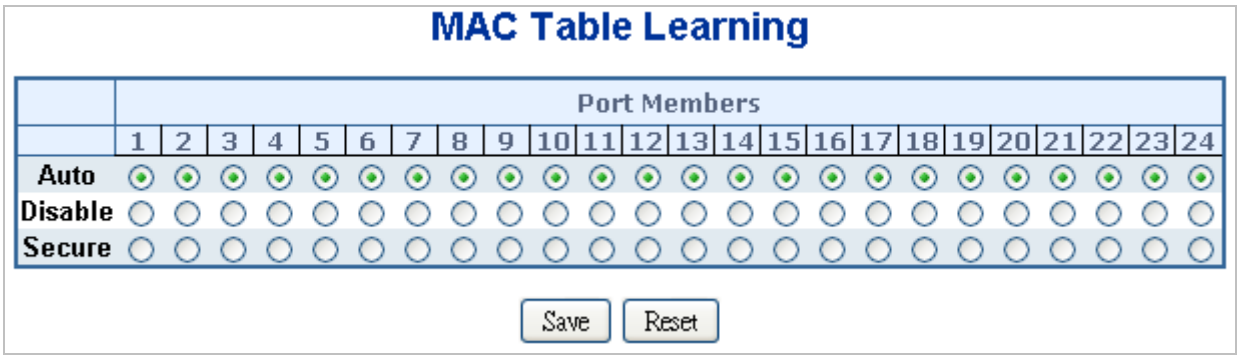


Figure 4-13-4 MAC Table Learning screenshot

The page includes the following fields:

Object	Description
• **Auto**	Learning is done automatically as soon as a frame with unknown SMAC is received.
• **Disable**	No learning is done.

• **Secure**	Only static MAC entries are learned, all other frames are dropped.

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

Buttons

Save: Click to save changes.

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

4.13.5 Dynamic ARP Inspection Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. The Dynamic ARP Inspection Table screen in Figure 4-13-5 appears.

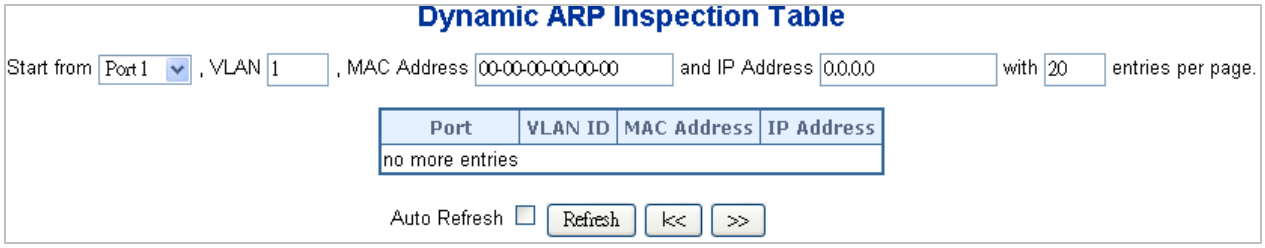


Figure 4-13-5 Dynamic ARP Inspection Table screenshot

Navigating the ARP Inspection Table

Each page shows up to 999 entries from the Dynamic ARP Inspection table, default being 20, selected through the "**entries per page**" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "**Start from port address**", "**VLAN**", "**MAC address**" and "**IP address**" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

The page includes the following fields:

Object	Description

• **Port**	The port number for which the status applies. Click the port number to see the status for this particular port.
• **VLAN ID**	The VLAN ID of the entry.
• **MAC address**	The MAC address of the entry.
• **IP Address**	The IP address of the entry.

Buttons

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

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

Clear: Flushes all dynamic entries.

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

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

4.13.6 Dynamic IP Source Guard Table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by IP mask. The Dynamic IP Source Guard Table screen in Figure 4-13-6 appears.

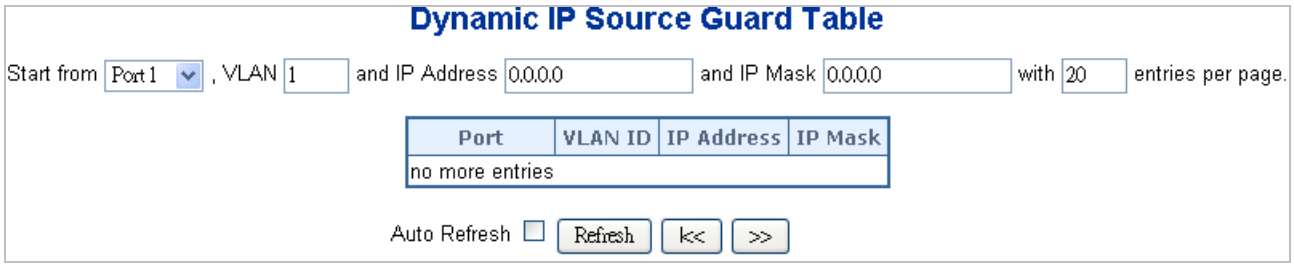


Figure 4-13-6 Dynamic IP Source Guard Table screenshot

Navigating the ARP Inspection Table

Each page shows up to 999 entries from the Dynamic IP Source Guard table, default being 20, selected through the "**entries per page**" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table.

The "**Start from port address**", "**VLAN**", "**IP address**" and "**IP mask**" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The "**>>**" will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached the text "No

more entries" is shown in the displayed table. Use the "|<<" button to start over.

The page includes the following fields:

Object	Description
• **Port**	The port number for which the status applies. Click the port number to see the status for this particular port.
• **VLAN ID**	The VLAN ID of the entry.
• **MAC address**	The MAC address of the entry.
• **IP Address**	The IP address of the entry.

Buttons

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

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

Clear: Flushes all dynamic entries.

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

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

4.14 LLDP

4.14.1 Link Layer Discovery Protocol

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

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

4.14.2 LLDP Configuration

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

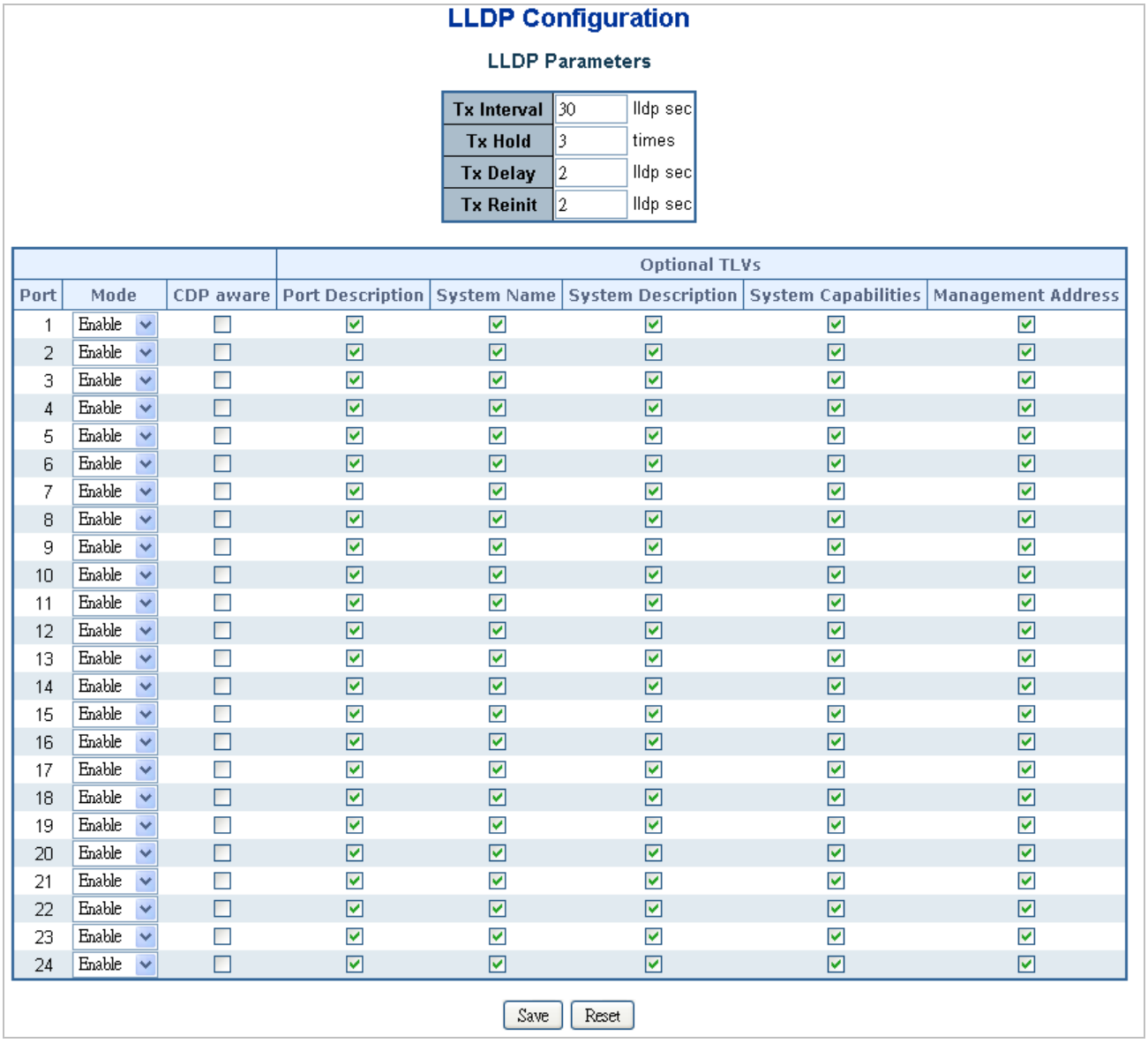


Figure 4-14-1 LLDP Configuration page screenshot

The page includes the following fields:

LLDP Parameters

Object	Description
• **Tx Interval**	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds. Default: **30** seconds This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)

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

LLDP Port Configuration

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

Object	Description
• **Port**	The switch port number of the logical LLDP port.
• **Mode**	Select LLDP mode. **Rx only** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. **Tx only** The switch will drop LLDP information received from neighbors, but will send out LLDP information. **Disabled** The switch will not send out LLDP information, and will drop LLDP information received from neighbors. **Enabled** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
• **CDP Aware**	Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP for the port is enabled.

	Only CDP TLVs that can be mapped into a corresponding field in the LLDP neighbors table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frame are not shown in the LLDP statistic. Only). CDP TLVs are mapped into LLDP neighbors table as shown below. CDP TLV "Device ID" is mapped into the LLDP "Chassis ID" field. CDP TLV "Address" is mapped into the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table. CDP TLV "Port ID" is mapped into the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped into the LLDP "System Description" field. Both the CDP and LLDP supports "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors table. If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch. Note: When CDP awareness for a port is disabled the CDP information isn't removed immediately, but will be removed when the hold time is exceeded.
• **Port Descr**	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
• **Sys Name**	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
• **Sys Descr**	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
• **Sys Capa**	Optional TLV: When checked the "system capability" is included in LLDP information transmitted. The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.
• **Mgmt Addr**	Optional TLV: When checked the "management address" is included in LLDP information transmitted. The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address

Buttons

Save: Click to save changes.

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

4.14.3 LLDPMED Configuration

This page allows you to configure the LLDP-MED. The LLDPMED Configuration screen in Figure 4-14-2 appears.

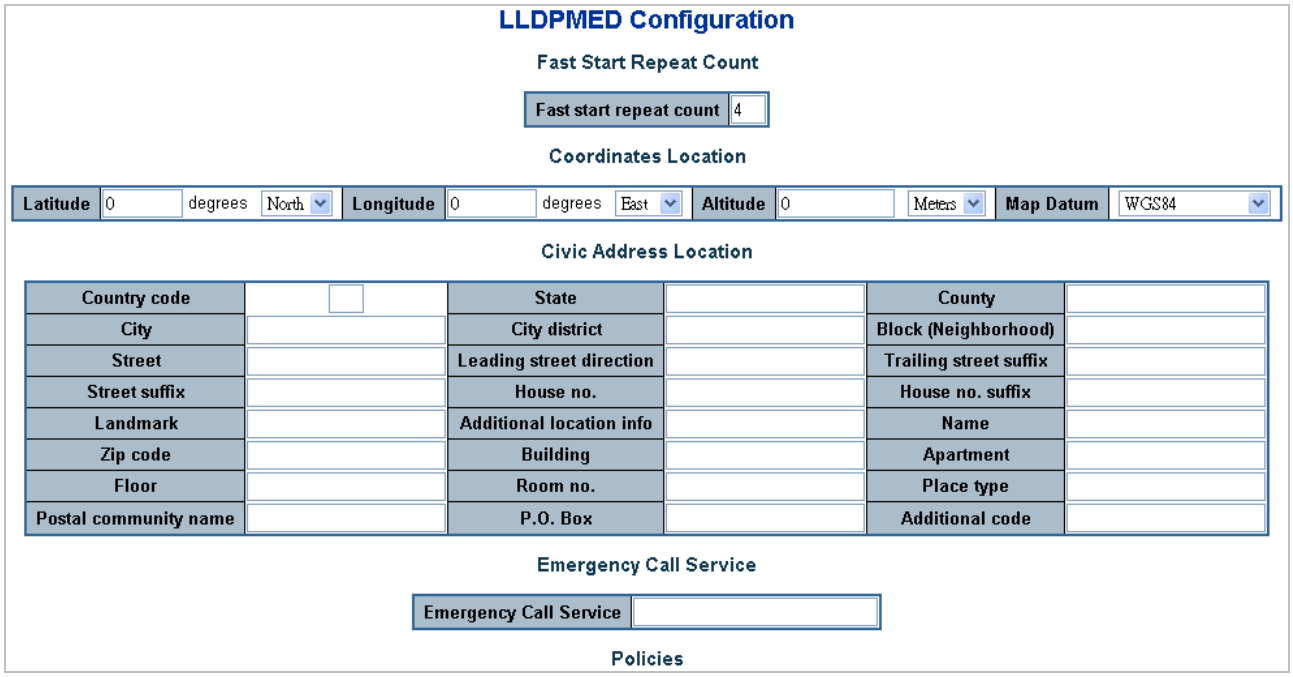


Figure 4-14-2 LLDPMED Configuration page screenshot

The page includes the following fields:

Fast start repeat count

Object	Description
• **Fast start repeat count**	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general.In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is

	detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors. Because there is a risk that a LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility for that the neighbors has received the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.

Coordinates Location

Object	Description
• **Latitude**	Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.
• **Longitude**	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.
• **Altitude**	Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). **Meters**: Representing meters of Altitude defined by the vertical datum specified. **Floors**: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

• **Map Datum**	The Map Datum used for the coordinates given in this Option **WGS84**: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. **NAD83/NAVD88**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). **NAD83/MLLW**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Object	Description
• **Country code**	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
• **State**	National subdivisions (state, canton, region, province, prefecture).
• **County**	County, parish, gun (Japan), district.
• **City**	City, township, shi (Japan) - Example: Copenhagen
• **City district**	City division, borough, city district, ward, chou (Japan)
• **Block (Neighborhood)**	Neighborhood, block
• **Street**	Street - Example: Poppelvej
• **Leading street direction**	Leading street direction - Example: N
• **Trailing street suffix**	Trailing street suffix - Example: SW
• **Street suffix**	Street suffix - Example: Ave, Platz
• **House no.**	House number - Example: 21
• **House no. suffix**	House number suffix - Example: A, 1/2
• **Landmark**	Landmark or vanity address - Example: Columbia University
• **Additional location info**	Additional location info - Example: South Wing
• **Name**	Name (residence and office occupant) - Example: Flemming Jahn
• **Zip code**	Postal/zip code - Example: 2791

• **Building**	Building (structure) - Example: Low Library
• **Apartment**	Unit (Apartment, suite) - Example: Apt 42
• **Floor**	Floor - Example: 4
• **Room no.**	Room number - Example: 450F
• **Place type**	Place type - Example: Office
• **Postal community name**	Postal community name - Example: Leonia
• **P.O. Box**	Post office box (P.O. BOX) - Example: 12345
• **Additional code**	Additional code - Example: 1320300003

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Object	Description
• **Emergency Call Service**	Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port.

The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice

4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Object	Description
• **Delete**	Check to delete the policy. It will be deleted during the next save.
• **Policy ID**	ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.
• **Application Type**	Intended use of the application types: **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. **Voice Signaling (conditional)** - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. **Guest Voice Signaling (conditional)** - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. **Video Conferencing** **Streaming Video** - for use by broadcast or multicast based video content

	distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. **Video Signaling (conditional)** - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
• **Tag**	Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
• **VLAN ID**	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003
• **L2 Priority**	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
• **DSCP**	DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Port Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Object	Description
• **Port**	The port number for which the configuration applies.
• **Policy ID**	The set of policies that shall apply for a given port. The set of policies is selected by checkmarking the checkboxes that corresponds to the policies

Buttons

Add new policy: click to add new policy.

Save: Click to save changes.

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

4.14.4 LLDP-MED Neighbor

This page provides a status overview for all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP-MED Neighbor Information screen in Figure 4-14-3 appears. The columns hold the following information:

Figure 4-14-3 LLDP-MED Neighbor Information page screenshot

The page includes the following fields:

Fast start repeat count

Object	Description
• **Port**	The port on which the LLDP frame was received.
• **Device Type**	LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. **LLDP-MED Network Connectivity Device Definition** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. **LLDP-MED Endpoint Device Definition**

	Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. Fore-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I). **LLDP-MED Generic Endpoint (Class I)** The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management. **LLDP-MED Media Endpoint (Class II)** The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery. **LLDP-MED Communication Endpoint (Class III)** The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management

• **LLDP-MED Capabilities**	LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are: 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE 5. Extended Power via MDI - PD 6. Inventory 7. Reserved
• **Application Type**	Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The poosible application types are shown below. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. **Voice Signaling** - for use in network topologies that require a different policy for the voice signaling than for the voice media. **Guest Voice** - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. **Video Signaling** - for use in network topologies that require a separate policy for the video signaling than for the video media.
• **Policy**	Policy **Unknown**: The network policy for the specified application type is currently unknown. **Defined**: The network policy is defined.
• **TAG**	TAG is indicating whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged ot Untagged **Untagged**: The device is using an untagged frame format and as such does not

	include a tag header as defined by IEEE 802.1Q-2003. **Tagged**: The device is using the IEEE 802.1Q tagged frame format
• **VLAN ID**	VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
• **Priority**	Priority is the Layer 2 priority to be used for the specified application type.One of eight priority levels (0 through 7)
• **DSCP**	DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

Buttons

Refresh: Click to refresh the page immediately.

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

4.14.5 Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP Neighbor Information screen in Figure 4-14-4 appears. The columns hold the following information:

Figure 4-14-4 LLDP Neighbor Information page screenshot

The page includes the following fields:

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

• **Port Description**	Port Description is the port description advertised by the neighbor unit.
• **System Capabilities**	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
• **Management Address**	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.

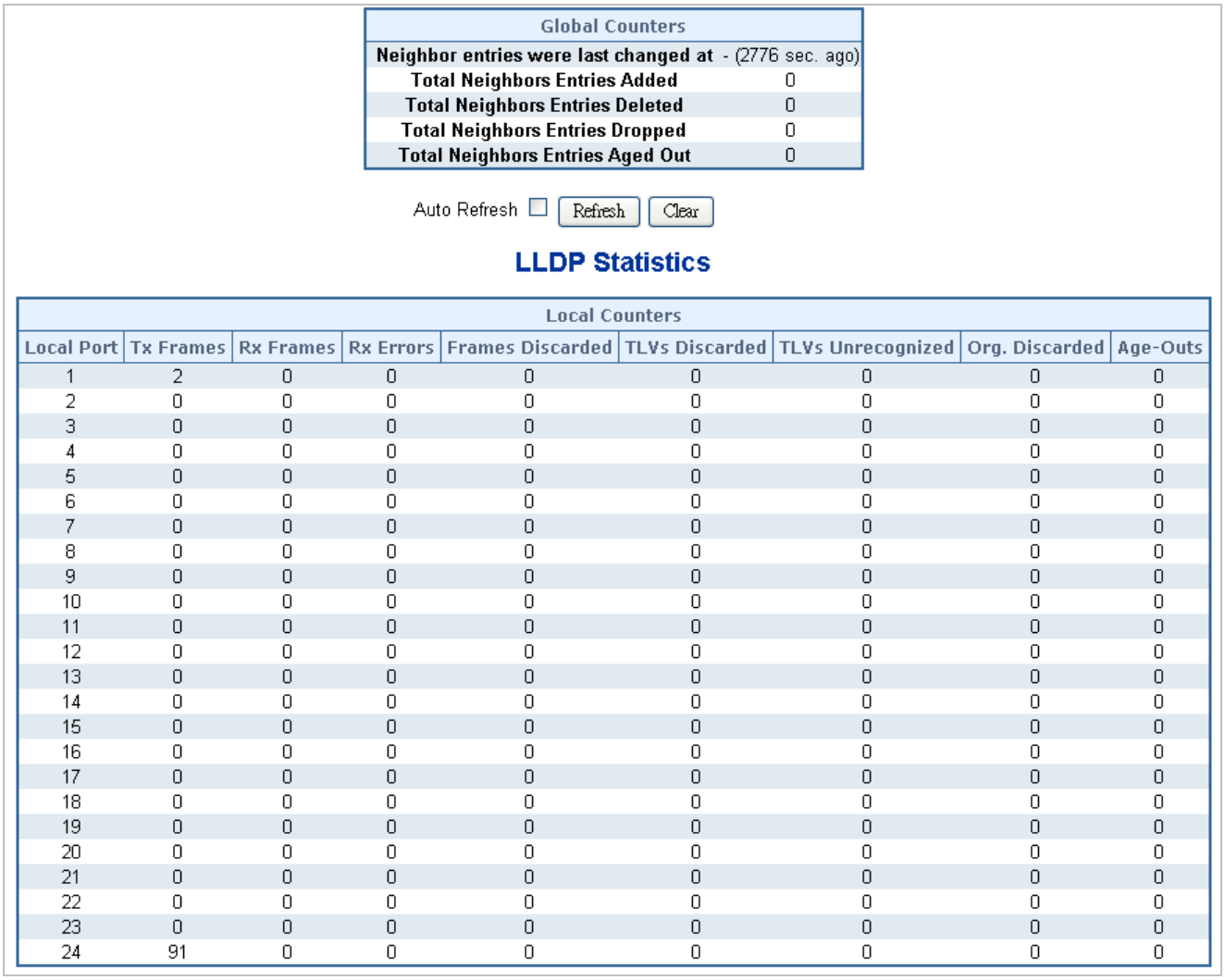
Buttons

Refresh: Click to refresh the page immediately.

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

4.14.6 Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refers to counters for the currently selected switch. The LLDP Statistics screen in Figure 4-14-5 appears.



Global Counters	
Neighbor entries were last changed at	- (2776 sec. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

Auto Refresh ☐ Refresh Clear

LLDP Statistics

Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	2	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	91	0	0	0	0	0	0	0

Figure 4-14-5 LLDP Statistics page screenshot

The page includes the following fields:

Global Counters

Object	Description
• **Neighbor entries were last changed at**	Shows the time for when the last entry was last deleted or added. It is also shows the time elapsed since last change was detected.
• **Total Neighbors Entries Added**	Shows the number of new entries added since switch reboot.
• **Total Neighbors Entries Deleted**	Shows the number of new entries deleted since switch reboot.
• **Total Neighbors Entries Dropped**	Shows the number of LLDP frames dropped due to that the entry table was full.
• **Total Neighbors Entries Aged Out**	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

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

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

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the local counters. All counters (including global counters) are cleared upon reboot.

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

4.15 Network 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**
- **IPv6 Ping**
- **Cable Diagnostic**

PING

The ping and IPv6 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.

Cable Diagnostics

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

- If the link is established on the twisted-pair interface in 1000Base-T mode, the Cable Diagnostics can run without disruption of the link or of any data transfer.
- If the link is established in 100Base-TX or 10Base-T, the Cable Diagnostics cause the link to drop while the diagnostics are running.

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

- Coupling between cable pairs.
- Cable pair termination
- Cable Length

Buttons

: Click to start to transmit ICMP packets.

4.15.1 Ping

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

After you press "**Start**", 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The

ICMP Ping screen in Figure 4-15-1 appears.

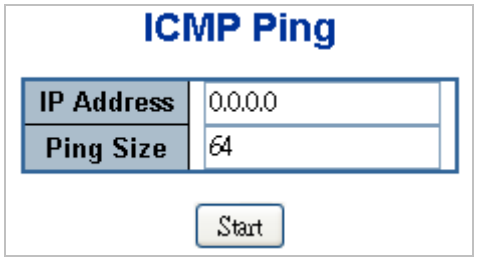


Figure 4-15-1 ICMP Ping page screenshot

The page includes the following fields:

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

Note

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

Buttons

Start: Click to transmit ICMP packets.

4.15.2 IPv6 Ping

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press "**Start**", 5 ICMPv6 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 ICMPv6 Ping screen in Figure 4-15-2 appears.

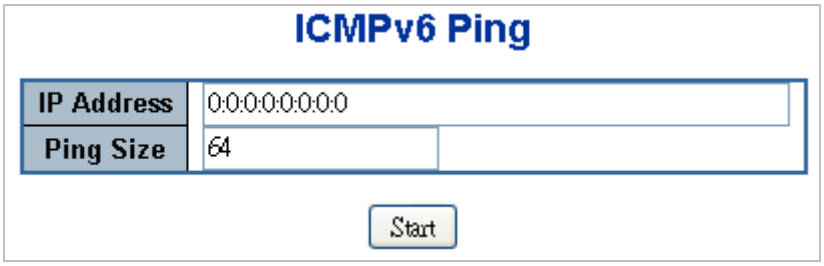


Figure 4-15-2 ICMPv6 Ping page screenshot

The page includes the following fields:

Object	Description
• **IPv6 Address**	The destination IPv6 Address.
• **Ping Size**	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

Buttons

Start: Click to transmit ICMP packets.

4.15.3 Cable Diagnostics

This page is used for running the Cable Diagnostics.

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

10 and 100 Mbps ports will be linked down while running cable diagnostic. Therefore, running cable diagnastic on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete. The ports belong to the currently selected stack unit, as reflected by the page header. The VeriPHY Cable Diagnostics screen in Figure 4-15-3 appears.

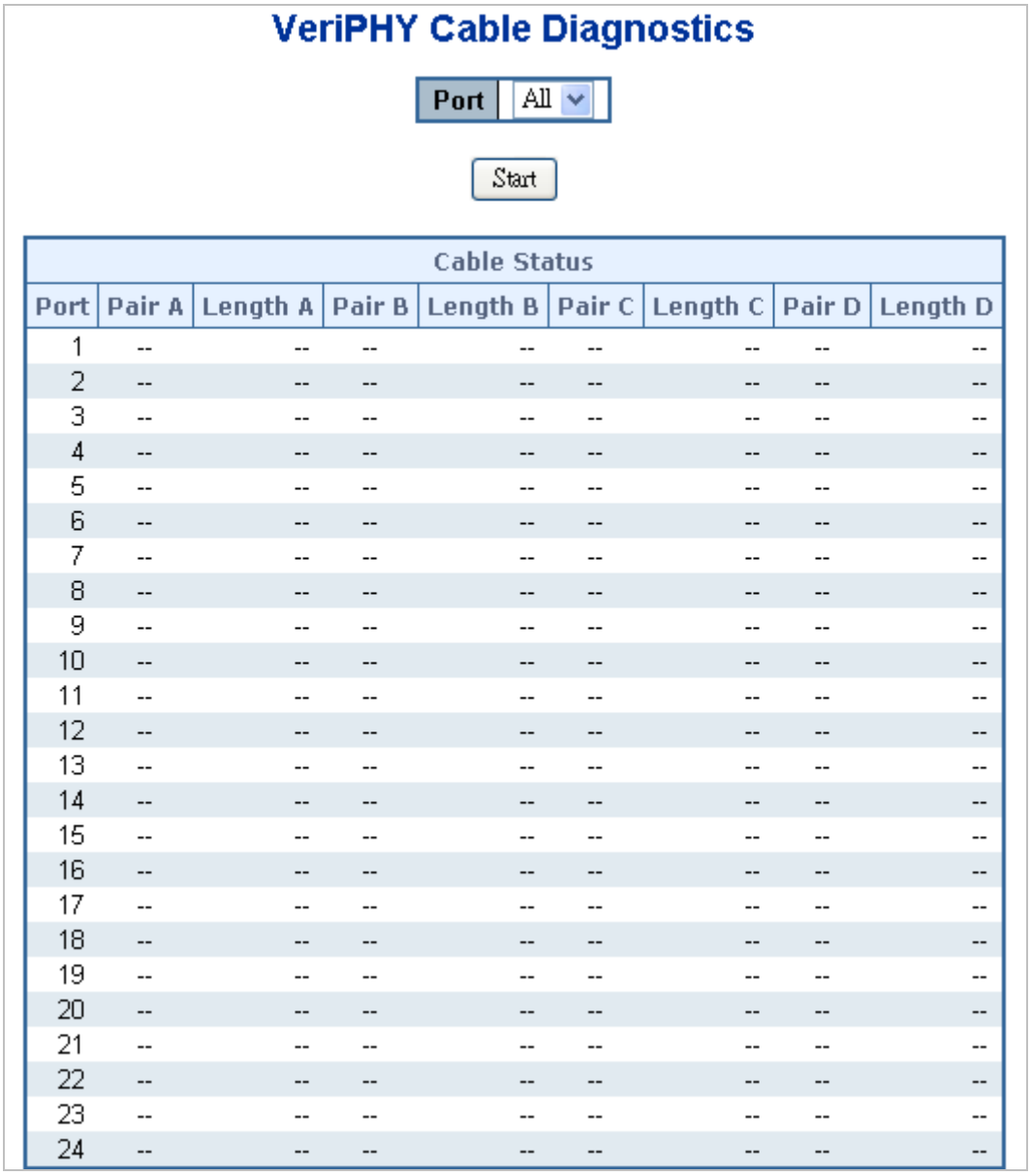


Figure 4-15-3 VeriPHY Cable Diagnostics page screenshot

The page includes the following fields:

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

Buttons

Start: Click to run the diagnostics.

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**

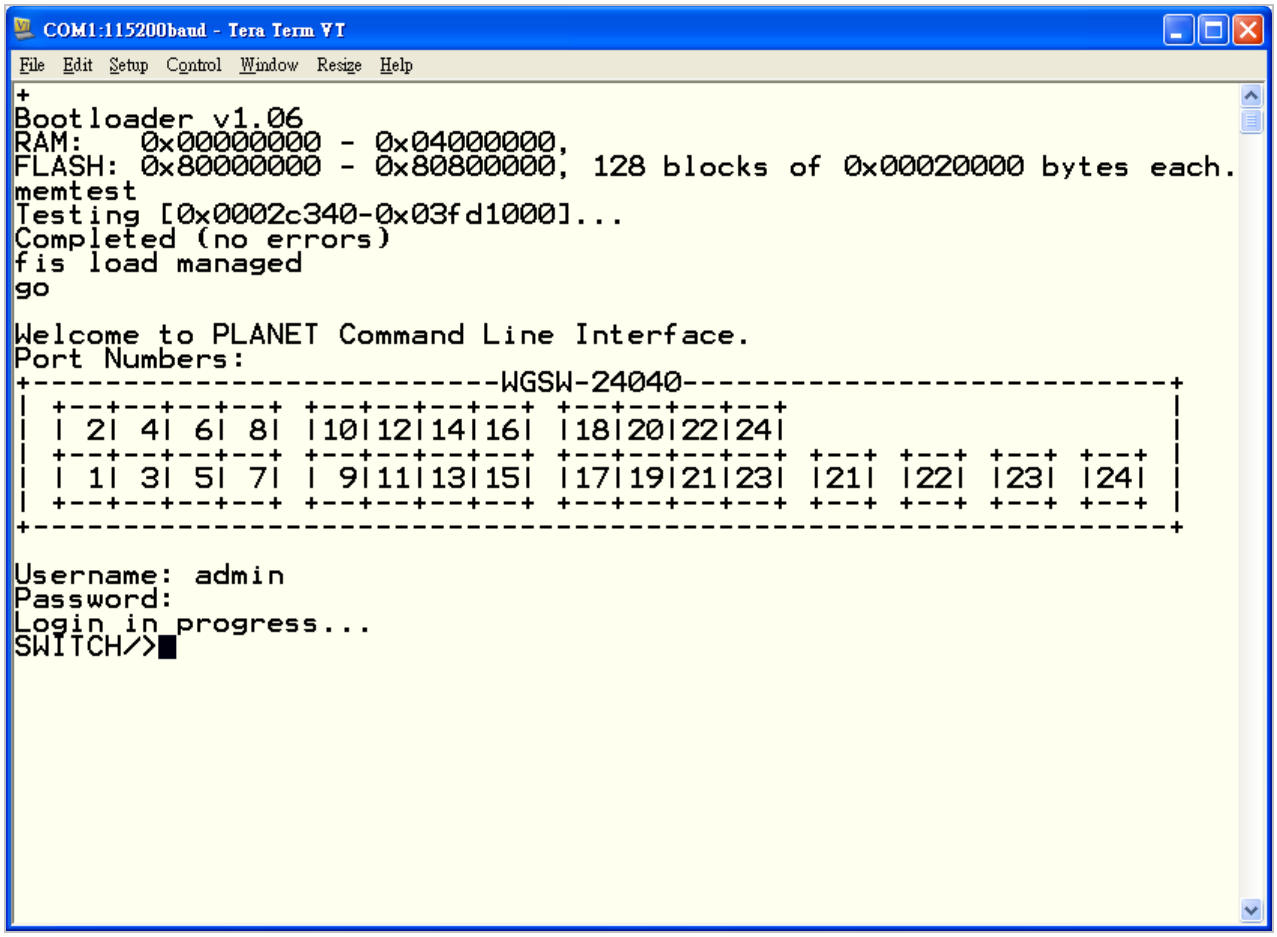


Figure 5-1 WGSW Managed Switch Console Login screen

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 WGSW Managed Switch is shipped with default IP address as following.

IP Address: **192.168.0.100**

Subnet Mask: **255.255.255.0**

To check the current IP address or modify a new IP address for the Switch, please use the procedures as follow:

■ **Show the current IP address**

1. On "**Switch/>** " prompt, enter "**ip configuration**".

2. The screen displays the current IP address, Subnet Mask and Gateway. As show in Figure 5-2.

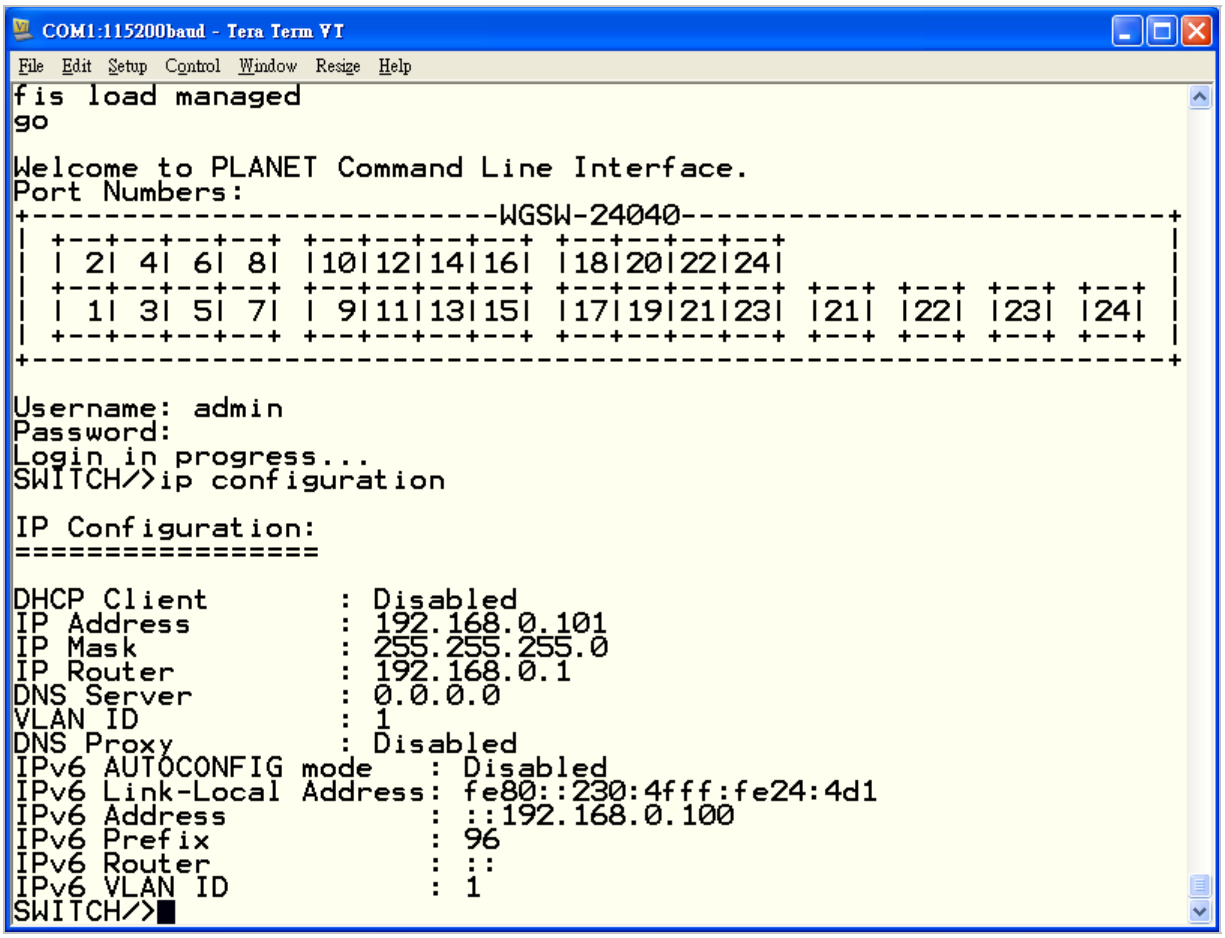


Figure 5-2 Show IP information screen

■ **Configure IP address**

3. On "**Switch/>** " prompt, enter the following command and press **<Enter>.** As show in Figure 5-3.

```
Switch/> ip setup 192.168.0.100 255.255.255.0 192.168.0.1 1
```

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

IP: 192.168.0.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.1
VLAN ID: 1

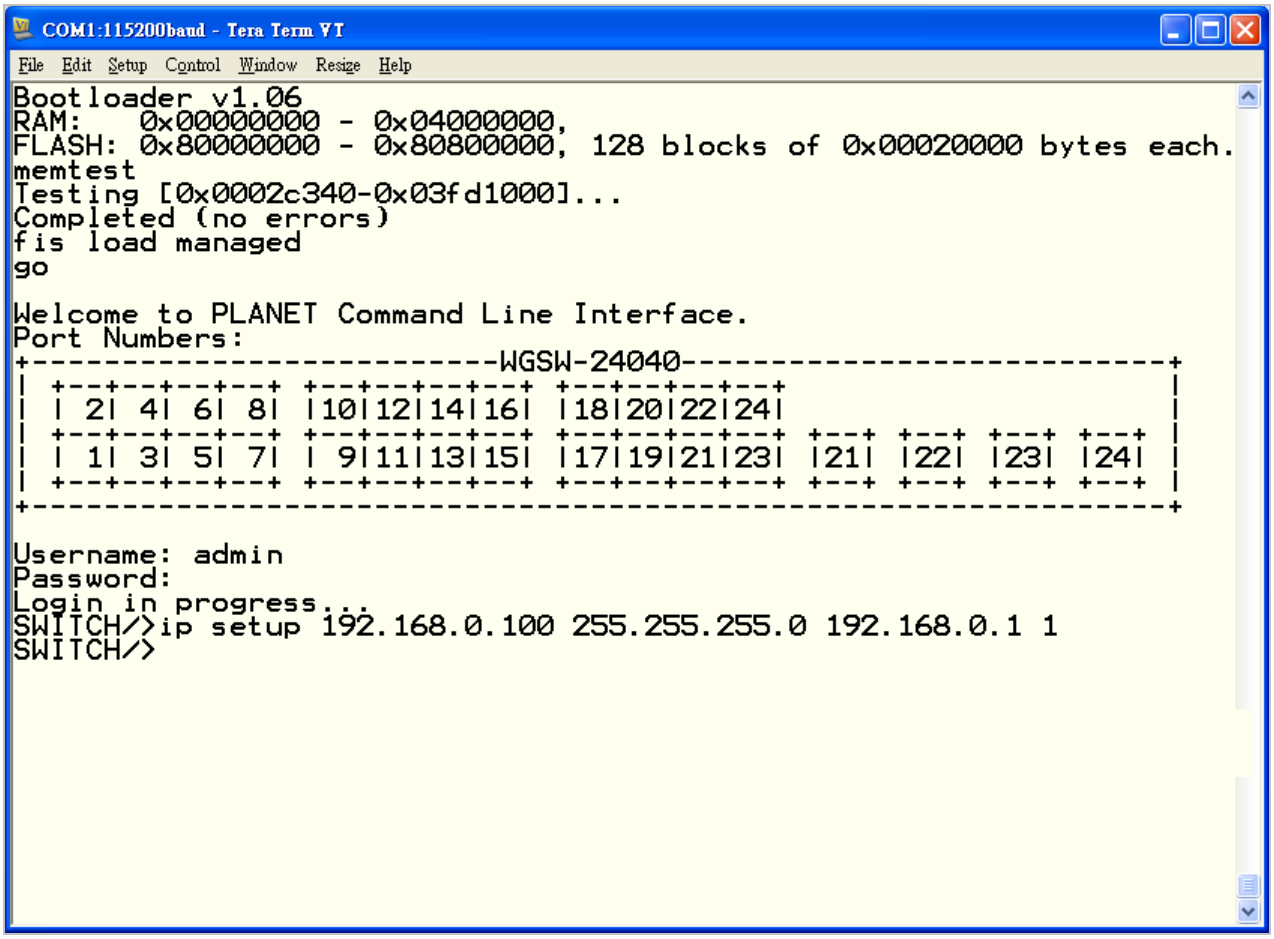


Figure 5-3 Set IP address screen

4. 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

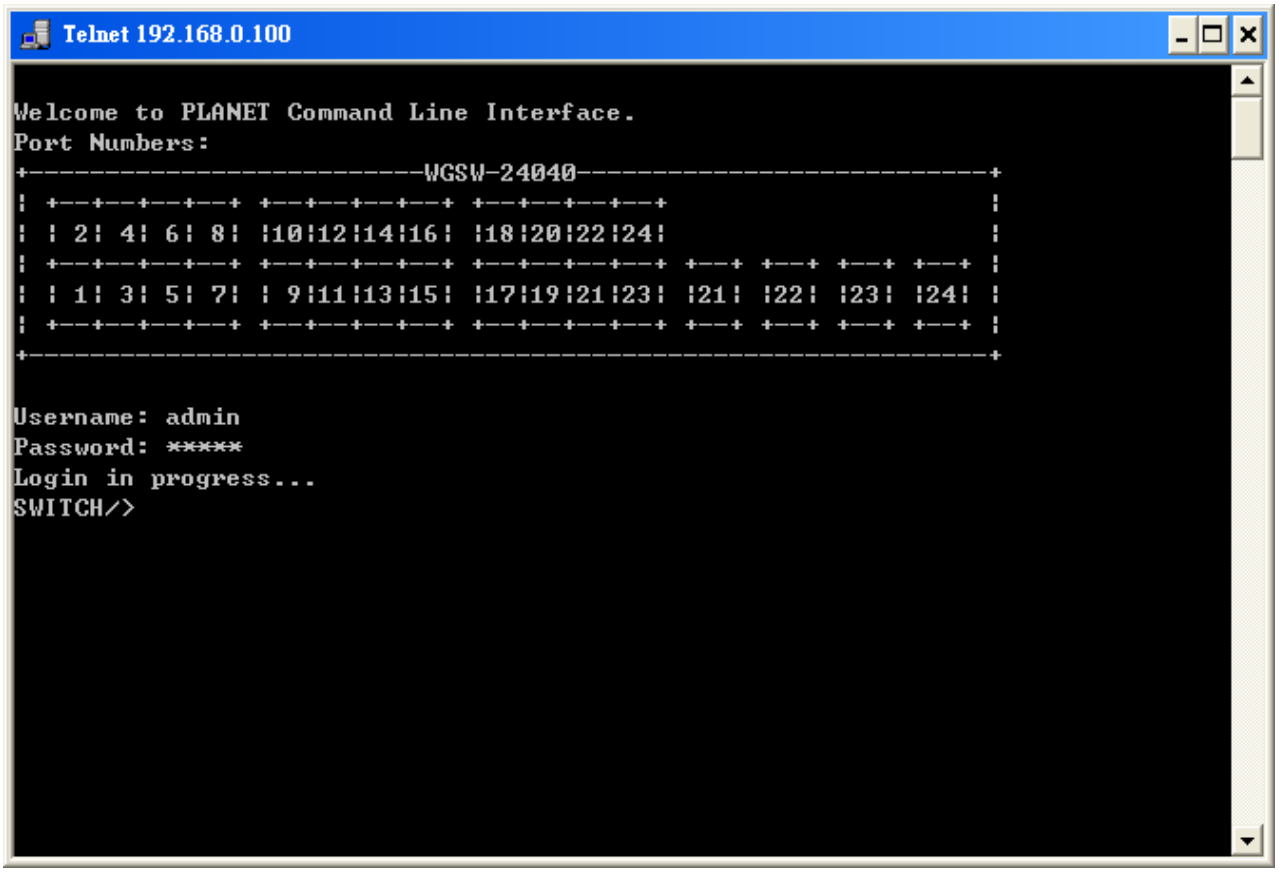
If you do not familiar with console command or the related parameter, enter "**help**" anytime in console to get the help description.

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

such as TIP

5.2 Telnet login

The Managed Switch also supports telnet for remote management. The switch asks for user name and password for remote login when using telnet, please use **"admin"** for 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.

Command Groups:

System	System settings and reset options
IP	IP configuration and Ping
Port	Port management
MAC	MAC address table
VLAN	Virtual LAN
PVLAN	Private VLAN
Security	Security management
STP	Spanning Tree Protocol
IGMP	Internet Group Management Protocol snooping
Aggr	Link Aggregation
LACP	Link Aggregation Control Protocol
LLDP	Link Layer Discovery Protocol
LLDPMED	Link Layer Discovery Protocol Media
QoS	Quality of Service
Mirror	Port mirroring
Config	Load/Save of configuration via TFTP
Firmware	Download of firmware via TFTP
UPnP	Universal Plug and Play
MVR	Multicast VLAN Registration
Voice VLAN	Specific VLAN for voice traffic

6.1 System Command

System Configuration

Description:

Show system configuration.

Syntax:

System Configuration [all] [<port_list>]

Parameters:

all : Show all switch configuration, default: Show system configuration

<port_list>: Port list or 'all', default: All ports

Example:

To display system information:

```
SWITCH/>System configuration
System Contact    :
System Name       : WGSW-24040
System Location :
Timezone Offset : 0
CLI Prompt        : SWITCH
MAC Address       : 00-30-4f-24-04-d1
Power Status      : AC,DC Power
Temperature       : 54.0 C - 129.2 F
System Time       : 1970-01-01 Thu 00:15:53 +0000
System Uptime     : 00:15:53
Software Version: Beta100601
Software Date     : 2010-06-01 18:08:32 +0800
Previous Restart: Cold
SWITCH/>
```

System Name

Description:

Set or show the system name.

Syntax:

System Name [<name>]

Parameters:

<name>: System name or 'clear' to clear

System name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No blank or space characters are permitted as part of a name. The first character must be an alpha character, and the first or last character must not be a minus sign.

Default Setting:

WGSW-24040

Example:

To set device title:

```
Switch/>System name WGSW-24040-LAB
```

System Contact

Description:

Set or show the system contact.

Syntax:

System Contact [<contact>]

Parameters:

<contact>: System contact string. Use 'clear' or "" to clear the string.

No blank or space characters are permitted as part of a contact. (only in CLI)

Default Setting:

empty

Example:

To set device contact:

```
Switch/>System contact WGSW-24040-Test
```

System Location

Description:

Set or show the system location.

Syntax:

System Location [<location>]

Parameters:

<location>: System location string. Use 'clear' or "" to clear the string

In CLI, no blank or space characters are permitted as part of a contact.

Default Setting:

empty

Example:

To set device location:

```
Switch/>System location 9F-LAB
```

System Timezone

Description:

Set or show the system timezone offset.

Syntax:

System Timezone [<offset>]

Parameters:

<offset>: Time zone offset in minutes (-720 to 720) relative to UTC

Default Setting:

0

Example:

To set timezone:

```
Switch/>system timezone 0
```

System Prompt

Description:

Set the CLI prompt string.

Syntax:

System Prompt <prompt>

Parameters:

<prompt>: CLI prompt string

Default Setting:

CLI Prompt: SWITCH

Example:

To change CLI title:

```
Switch/>system prompt WGSW-24040
WGSW-24040/>
```

System Reboot

Description:

Reboot the system.

Syntax:

System Reboot

Example:

To reboot device without changing any of the settings:

```
Switch/>system reboot
```

System Restore Default

Description:

Restore factory default configuration.

Syntax:

System Restore Default [keep_ip]

Parameters:

keep_ip: Keep IP configuration, default: Restore full configuration

Example:

To restore default value but not reset IP address:

```
Switch/>system restore default keep_ip
```

System Load

Description:

Show current CPU load: 100ms, 1s and 10s running average (in percent, zero is idle).

Syntax:

System Load

Example:

To show current CPU load:

```
Switch/>system load
Load average(100ms, 1s, 10s):     1%,     1%,     1%
```

System Log

Description:

Show or clear the system log.

Syntax:

System Log [<log_id>] [all|info|warning|error] [clear]

Parameters:

<log_id>: System log ID or range (default: All entries)

all : Show all levels (default)

info : Show informations

warning : Show warnings

error : Show errors

clear : Clear log

Example:

To show system log:

```
Switch/>system log
Number of entries:
Info     : 2
Warning: 0
Error    : 0
All      : 2

ID      Level     Time                            Message
----    ------    -------------------------    -------
    1   Info      -   Switch just made a cold boot.
    2   Info      1970-01-01 Thu 00:00:04 +0000   Link up on port 10
```

6.2 IP Command

IP Configuration

Description:

Show IP configuration.

Syntax:

IP Configuration

Example:

Show IP configuration:

```
Switch/>ip configuration
IP Configuration:
=================

DHCP Client          : Disabled
IP Address           : 192.168.0.100
IP Mask              : 255.255.255.0
IP Router            : 192.168.0.1
DNS Server           : 0.0.0.0
VLAN ID              : 1
DNS Proxy            : Disabled
IPv6 AUTOCONFIG mode     : Disabled
IPv6 Link-Local Address: fe80::230:4fff:fe24:4d1
IPv6 Address             : ::192.168.0.100
IPv6 Prefix              : 96
IPv6 Router              : ::
IPv6 VLAN ID             : 1
```

IP DHCP

Description:

Set or show the DHCP client mode.

Syntax:

IP DHCP [enable|disable]

Parameters:

enable : Enable or renew DHCP client

disable: Disable DHCP client

Default Setting:

Disable

Example:

Disable DHCP sever:

```
SWITCH/>ip dhcp disable
```

IP Setup

Description:

Set or show the IP setup.

Syntax:

IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

Parameters:

<ip_addr> : IP address (a.b.c.d), default: Show IP address

<ip_mask> : IP subnet mask (a.b.c.d), default: Show IP mask

<ip_router>: IP router (a.b.c.d), default: Show IP router

<vid> : VLAN ID (1-4095), default: Show VLAN ID

Default Setting:

IP Address : 192.168.0.100

IP Mask : 255.255.255.0

IP Router : 192.168.0.1

DNS Server : 0.0.0.0

VLAN ID : 1

Example:

Set IP address:

```
SWITCH/>ip setup 192.168.0.100 255.255.255.0
```

IP Ping

Description:

Ping IP address (ICMP echo).

Syntax:

IP Ping <ip_addr_string> [<ping_length>]

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

<ping_length> : Ping data length (8-1400), excluding MAC, IP and ICMP headers

Example:

```
SWITCH/>ip ping 192.168.0.21
PING server 192.168.0.21
60 bytes from 192.168.0.21: icmp_seq=0, time=0ms
60 bytes from 192.168.0.21: icmp_seq=1, time=0ms
60 bytes from 192.168.0.21: icmp_seq=2, time=0ms
60 bytes from 192.168.0.21: icmp_seq=3, time=10ms
60 bytes from 192.168.0.21: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

IP DNS

Description:

Set or show the DNS server address.

Syntax:

IP DNS [<ip_addr>]

Parameters:

<ip_addr>: IP address (a.b.c.d), default: Show IP address

Default Setting:

0.0.0.0

Example:

Set DNS IP address:

```
SWITCH/>ip dns 168.95.1.1
```

IP DNS Proxy

Description:

Set or show the IP DNS Proxy mode.

Syntax:

IP DNS_Proxy [enable|disable]

Parameters:

enable : Enable DNS Proxy

disable: Disable DNS Proxy

Default Setting:

disable

Example:

Enable DNS proxy function:

```
SWITCH/>ip dns_proxy enable
```

IPv6 AUTOCINFIG

Description:

Set or show the IPv6 AUTOCONFIG mode.

Syntax:

IP IPv6 AUTOCONFIG [enable|disable]

Parameters:

enable : Enable IPv6 AUTOCONFIG mode

disable: Disable IPv6 AUTOCONFIG mode

Default Setting:

disable

Example:

Enable IPv6 autoconfig function:

```
SWITCH/>ip ipv6 autoconfig enable
```

IPv6 Setup

Description:

Set or show the IPv6 setup.

Syntax:

IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>] [<vid>]

Parameters:

<ipv6_addr> : 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'.

<ipv6_prefix>: IPv6 subnet mask , default: Show IPv6 prefix

<ipv6_router>: 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'.

<vid> : VLAN ID (1-4095), default: Show VLAN ID

Default Setting:

IPv6 AUTOCONFIG mode : Disabled

IPv6 Link-Local Address: fe80::230:4fff:fe24:4d1

IPv6 Address : ::192.168.0.100

IPv6 Prefix : 96

IPv6 Router : ::

IPv6 VLAN ID : 1

Example:

Set IPv6 address:

```
SWITCH/>ip ipv6 setup 2001::0002 64 2100::0001 1
```

IPv6 Ping

Description:

Ping IPv6 address (ICMPv6 echo).

Syntax:

IP IPv6 Ping6 <ipv6_addr> [<ping_length>]

Parameters:

<ipv6_addr> : 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'.

<ping_length>: Ping data length (8-1400), excluding MAC, IP and ICMP headers

Example:

```
SWITCH/>ip ipv6 ping 2001::0002
PING6 server 2001::2
68 bytes from 2001::2: icmp_seq=0, time=0ms
68 bytes from 2001::2: icmp_seq=1, time=0ms
68 bytes from 2001::2: icmp_seq=2, time=0ms
68 bytes from 2001::2: icmp_seq=3, time=0ms
68 bytes from 2001::2: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

IP NTP Configuration

Description:

Show NTP configuration.

Syntax:

IP NTP Configuration

Default Setting:

IP NTP Configuration:

==========

NTP Mode : Disabled

Idx Server IP host address (a.b.c.d) or a host name string

--- ----------

1 pool.ntp.org

2 europe.pool.ntp.org

3 north-america.pool.ntp.org

4 asia.pool.ntp.org

5 oceania.pool.ntp.org

IP NTP Mode

Description:

Set or show the NTP mode.

Syntax:

IP NTP Mode [enable|disable]

Parameters:

enable : Enable NTP mode

disable : Disable NTP mode

(default: Show NTP mode)

Default Setting:

disable

Example:

Enable NTP mode:

```
SWITCH/>ip ntp mode enable
```

IP NTP Server Add

Description:

Add NTP server entry.

Syntax:

IP NTP Server Add <server_index> <ip_addr_string>

Parameters:

<server_index> : The server index (1-5)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Example:

To add NTP server:

```
SWITCH/>ip ntp server add 1 60.249.136.151
```

IP NTP Server IPv6 Add

Description:

Add NTP server IPv6 entry.

Syntax:

IP NTP Server Ipv6 Add <server_index> <server_ipv6>

Parameters:

<server_index>: The server index (1-5)

<server_ipv6> : IPv6 server 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, '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 add IPv6 NTP server:

```
SWITCH/>ip ntp server ipv6 add 1 2001:7b8:3:2c::123
```

IP NTP Server Delete

Description:

Delete NTP server entry.

Syntax:

IP NTP Server Delete <server_index>

Parameters:

<server_index>: The server index (1-5)

Example:

To delete NTP server:

```
SWITCH/>ip ntp server delete 1
```

6.3 Port Management Command

Port Configuration

Description:

Show port configuration.

Syntax:

Port Configuration [<port_list>] [up|down]

Parameters:

<port_list>: Port list or 'all', default: All ports

up : Show ports, which are up

down **:** Show ports, which are down

(default: Show all ports)

Example:

Display port1~4 status

```
SWITCH/>port configuration 1-4

Port Configuration:
==================


Port   State       Mode      Flow Control   MaxFrame   Power      Excessive   Link
----    --------     ------      ------------    --------    --------     ---------    ----
1       Enabled    Auto      Disabled       9600       Enabled    Discard     Down
2       Enabled    Auto      Disabled       9600       Enabled    Discard     Down
3       Enabled    Auto      Disabled       9600       Enabled    Discard     Down
4       Enabled    Auto      Disabled       9600       Enabled    Discard     Down
```

Port Mode

Description:

Set or show the port speed and duplex mode.

Syntax:

Port Mode [<port_list>] [10hdx|10fdx|100hdx|100fdx|1000fdx|auto]

Parameters:

<port_list>: Port list or 'all', default: All ports

10hdx : 10 Mbps, half duplex

10fdx : 10 Mbps, full duplex

100hdx : 100 Mbps, half duplex

100fdx : 100 Mbps, full duplex

1000fdx : 1 Gbps, full duplex

auto : Auto negotiation of speed and duplex

(default: Show configured and current mode)

Default Setting:

Auto

Example:

Set 10Mbps (half duplex) speed for port1

```
SWITCH/>port mode 1 10hdx
```

Port Flow Control

Description:

Set or show the port flow control mode.

Syntax:

Port Flow Control [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable flow control

disable : Disable flow control

(default: Show flow control mode)

Default Setting:

Disable

Example:

Enable flow control function for port1

```
SWITCH/>port flow control 1 enable
```

Port State

Description:

Set or show the port administrative state.

Syntax:

Port State [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port

disable : Disable port

(default: Show administrative mode)

Default Setting:

Enable

Example:

Disable port1

```
SWITCH/>port state 1 disable
```

Port Maximum Frame

Description:

Set or show the port maximum frame size.

Syntax:

Port MaxFrame [<port_list>] [<max_frame>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<max_frame>: Port maximum frame size (1518-9600), default: Show maximum frame size

Default Setting:

9600

Example:

Set 2048 frame size for port1

```
SWITCH/>port maxframe 1 2048
```

Port Power

Description:

Set or show the port PHY power mode.

Syntax:

Port Power [<port_list>] [enable|disable|actiphy|dynamic]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable all power control

disable: Disable all power control

actiphy: Enable ActiPHY power control

dynamic: Enable Dynamic power control

Default Setting:

Enable

Example:

Disable port power function for port1-4

```
SWITCH/>port power 1-4 disable
```

Port SFP

Description:

Show SFP port information.

Syntax:

Port SFP [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show SFP information for port21-24

```
SWITCH/>port sfp

Port   Type              Speed        Wave Length(nm)   Distance(m)
----   --------------    --------     ---------------   -----------
21     1000Base-LX       1000-Base    1310              10000
22     1000Base-LX       1000-Base    1310              10000
23     --                --           --                --
24     --                --           --                --
```

Port Excessive

Description:

Set or show the port excessive collision mode.

Syntax:

Port Excessive [<port_list>] [discard|restart]

Parameters:

<port_list>: Port list or 'all', default: All ports

discard : Discard frame after 16 collisions

restart : Restart backoff algorithm after 16 collisions

(default: Show mode)

Default Setting:

Discard

Example:

```
SWITCH/>port excessive 1 restart
```

Port Statistics

Description:

Show port statistics.

Syntax:

Port Statistics [<port_list>] [<command>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<command> : The command parameter takes the following values:

clear : Clear port statistics

packets : Show packet statistics

bytes : Show byte statistics

errors : Show error statistics

discards : Show discard statistics

filtered : Show filtered statistics

low : Show low priority statistics

normal : Show normal priority statistics

medium : Show medium priority statistics

high : Show high priority statistics

(default: Show all port statistics)

up : Show ports, which are up

down : Show ports, which are down

(default: Show all ports)

Port VeriPHY

Description:

Run cable diagnostics.

Syntax:

Port VeriPHY [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

6.4 MAC Address Table Command

MAC Configuration

Description:

Show MAC address table configuration.

Syntax:

MAC Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show Mac address state

```
SWITCH/>mac configuration

MAC Configuration:
==================

MAC Address       : 00-30-4f-24-04-d1
MAC Age Time: 300

Port   Learning
----   --------
1       Auto
2       Auto
3       Auto
4       Auto
5       Auto
6       Auto
7       Auto
8       Auto
9       Auto
10      Auto
11      Auto
12      Auto
13      Auto
14      Auto
15      Auto
```

16	**Auto**
17	**Auto**
18	**Auto**
19	**Auto**
20	**Auto**
21	**Auto**
22	**Auto**
23	**Auto**
24	**Auto**

Mac Add

Description:

Add MAC address table entry.

Syntax:

MAC Add <mac_addr> <port_list> [<vid>]

Parameters:

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)

<port_list>: Port list or 'all' or 'none'

<vid> : VLAN ID (1-4095), default: 1

Example:

Add Mac address 00-30-4F-01-01-02 in port1 and vid1

```
SWITCH/>mac add 00-30-4f-01-01-02 1 1
```

MAC Delete

Description:

Delete MAC address entry.

Syntax:

MAC Delete <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

<vid> : VLAN ID (1-4095), default: 1

Example:

Delete Mac address 00-30-4F-01-01-02 in vid1

```
SWITCH/>mac delete 00-30-4f-01-01-02 1
```

MAC Lookup

Description:

Lookup MAC address entry.

Syntax:

MAC Lookup <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

<vid> : VLAN ID (1-4095), default: 1

Example:

Lookup state of Mac address 00-30-4F-01-01-02

```
SWITCH/>mac lookup 00-30-4f-01-01-02
```

MAC Age Time

Description:

Set or show the MAC address age timer.

Syntax:

MAC Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (10-1000000), default: Show age time

Default Setting:

300

Example:

Set agetime value in 30

```
SWITCH/>mac agetime 30
```

MAC Learning

Description:

Set or show the port learn mode.

Syntax:

MAC Learning [<port_list>] [auto|disable|secure]

Parameters:

<port_list>: Port list or 'all', default: All ports

auto : Automatic learning

disable: Disable learning

secure : Secure learning

(default: Show learn mode)

Default Setting:

Auto

Example:

Set secure learning mode in port1

```
SWITCH/>mac learning 1 secure
```

MAC Dump

Description:

Show sorted list of MAC address entries.

Syntax:

MAC Dump [<mac_max>] [<mac_addr>] [<vid>]

Parameters:

<mac_max> : Maximum number of MAC addresses 1-8192, default: Show all addresses

<mac_addr>: First MAC address (xx-xx-xx-xx-xx-xx), default: MAC address zero

<vid> : First VLAN ID (1-4095), default: 1

Example:

Show all of MAC table

```
SWITCH/>mac dump
Type      VID    MAC Address           Ports
------    ---    -----------------     -----
Static     1     00-30-00-33-22-55     1
Static     1     00-30-4f-24-04-d1     None,CPU
Static     1     33-33-ff-24-04-d1     None,CPU
Static     1     33-33-ff-a8-00-64     None,CPU
Dynamic    1     40-61-86-04-18-69     10
Static     1     ff-ff-ff-ff-ff-ff     1-24,CPU
```

MAC Statistics

Description:

Show MAC address table statistics.

Syntax:

MAC Statistics [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Set all of MAC statistics

```
SWITCH/>mac statistics
Port   Dynamic Addresses
----   -----------------
1      0
2      0
3      0
4      0
5      0
6      0
7      0
8      0
9      0
```

```
10      1
11      0
12      0
13      0
14      0
15      0
16      0
17      0
18      0
19      0
20      0
21      0
22      0
23      0
24      0

Total Dynamic Addresses: 1
Total Static Addresses : 5
```

MAC Flush

Description:

Flush all learned entries.

Syntax:

MAC Flush

6.5 VLAN Configuration Command

VLAN Configuration

Description:

Show VLAN configuration.

Syntax:

VLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show VLAN status of port1

```
SWITCH/>vlan configuration 1

VLAN Configuration:
====================



Mode : IEEE 802.1Q
Port   PVID   IngrFilter   FrameType    LinkType   Q-in-Q Mode   Eth type
----    ----   ----------    ----------    --------    -----------    --------
1       1      Disabled     All          UnTag      Disable       N/A

VID    Ports
----    -----
1      1-24
```

VLAV PVID

Description:

Set or show the port VLAN ID.

Syntax:

VLAN PVID [<port_list>] [<vid>|none]

Parameters:

<port_list>: Port list or 'all', default: All ports

<vid>|none : Port VLAN ID (1-4095) or 'none', default: Show port VLAN ID

Default Setting:

1

Example:

Set PVID2 for port20

```
SWITCH/>vlan pvid 20 2
```

VLAN Frame Type

Description:

Set or show the port VLAN frame type.

Syntax:

VLAN FrameType [<port_list>] [all|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports

all : Allow tagged and untagged frames

tagged : Allow tagged frames only

(default: Show accepted frame types)

Default Setting:

All

Example:

Set port20 that allow tagged frames only

```
SWITCH/>vlan frametype 20 tagged
```

VLAN Ingress Filter

Description:

Set or show the port VLAN ingress filter.

Syntax:

VLAN IngressFilter [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable VLAN ingress filtering

disable : Disable VLAN ingress filtering

(default: Show VLAN ingress filtering)

Default Setting:

Disable

Example:

Enable VLAN ingress filtering for port20

```
SWITCH/>vlan ingressfilter 20 enable
```

VLAN Mode

Description:

Set or show the VLAN Mode.

Syntax:

VLAN Mode [portbased|dot1q]

Parameters:

portbased : Port-Based VLAN Mode

dot1q : 802.1Q VLAN Mode

(default: Show VLAN Mode)

Default Setting:

IEEE 802.1Q

Example:

Set VLAN mode in port base

```
SWITCH/>vlan mode portbased
```

VLAN Link Type

Description:

Set or show the port VLAN link type.

Syntax:

VLAN LinkType [<port_list>] [untagged|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports

untagged : VLAN Link Type Tagged

tagged : VLAN Link Type Untagged

(default: Show VLAN link type)

Default Setting:

Un-tagged

Example:

Enable tagged frame for port2

```
SWITCH/>vlan linktype 2 tagged
```

VLAN Q-in-Q Mode

Description:

Set or show the port Q-in-Q mode.

Syntax:

VLAN Qinqmode [<port_list>] [disable|man|customer]

Parameters:

<port_list>: Port list or 'all', default: All ports

disable : Disable Q-in-Q VLAN Mode

man : Q-in-Q MAN Port Mode

customer : Q-in-Q Customer Port Mode

(default: Show VLAN QinQ Mode)

Example:

Set port2 in man port

```
SWITCH/>vlan qinq 2 man
```

VLAN Ethernet Type

Description:

Set or show out layer VLAN tag ether type in Q-in-Q VLAN mode.

Syntax:

VLAN Ethtype [<port_list>] [man|dot1q]

Parameters:

<port_list>: Port list or 'all', default: All ports

man : Set out layer VLAN tag ether type : MAN

dot1q : Set out layer VLAN tag ether type : 802.1Q

(default: Show VLAN out layer VLAN tag ether type)

Default Setting:

N/A

Example:

Set out layer VLAN tag Ethernet type for port 10 in man Ethernet type

```
SWITCH/>vlan ethtype 10 man
```

VLAN Add

Description:

Add or modify VLAN entry.

Syntax:

VLAN Add <vid> [<port_list>]

Parameters:

<vid> : VLAN ID (1-4095)

<port_list>: Port list or 'all', default: All ports

Default Setting:

1

Example:

Add port17 to port24 in VLAN10

```
SWITCH/>vlan add 10 17-24
```

VLAN Delete

Description:

Delete VLAN entry.

Syntax:

VLAN Delete <vid>

Parameters:

<vid>: VLAN ID (1-4095)

Example:

Delete port17 to port24 in VLAN10

```
SWITCH/>vlan delete 10
```

VLAN Lookup

Description:

Lookup VLAN entry.

Syntax:

VLAN Lookup [<vid>] [combined|static|nas|mvr|voice_vlan|all]

Parameters:

<vid>: VLAN ID (1-4095), default: Show all VLANs

combined : Shows All the Combined VLAN database

static : Shows the VLAN entries configured by the administrator

nas : Shows the VLANs configured by NAS

mvr : Shows the VLANs configured by MVR

voice_vlan : Shows the VLANs configured by Voice VLAN

all : Shows all VLANs' configuration

Example:

Show VLAN status

```
SWITCH/>vlan lookup

VID     Ports
----    -----
1       1-24
200     None
```

VLAN Status

Description:

VLAN Port Configuration Status.

Syntax:

VLAN Status [<port_list>] [combined|static|nas|mvr|voice_vlan|mstp|all|conflicts]

Parameters:

<port_list>: Port list or 'all', default: All ports

combined : combined VLAN Users configuration

static : static port configuration

nas : NAS port configuration

mvr : MVR port configuration

voice_vlan : Voice VLAN port configuration

mstp : MSTP port configuration

all : All VLAN Users configuration

(default: combined VLAN Users configuration)

Default Setting:

Promiscous

Example:

Show VLAN configuration of port10

```
SWITCH/>status 1

Port   VLAN User      Aware    PVID   Frame Type   Ing Filter    Tx Tag       UVID    Conflicts
----    -----------    --------   ----    ----------    -----------    -----------   -----    ---------
1       Static         Enabled    1       All           Disabled      Untag This    1
```

```
NAS                                                          No
MVR                                                          No
Voice VLAN                                                   No
MSTP                                                         No
Combined      Enabled   1      All          Disabled  Untag This  1      No
```

6.6 Private VLAN Configuration Command

PVLAN Configuration

Description:

Show Private VLAN configuration.

Syntax:

PVLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show private VLAN configuration

```
SWITCH/> pvlan configuration

Private VLAN Configuration:
===========================



Port   Isolation
----   ---------
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
9      Disabled
```

```
10      Disabled
11      Disabled
12      Disabled
13      Disabled
14      Disabled
15      Disabled
16      Disabled
17      Disabled
18      Disabled
19      Disabled
20      Disabled
21      Disabled
22      Disabled
23      Disabled
24      Disabled

PVLAN ID    Ports
--------        -----
1               1-24
```

PVLAN Add

Description:

Add or modify Private VLAN entry.

Syntax:

PVLAN Add <pvlan_id> [<port_list>]

Parameters:

<pvlan_id> : Private VLAN ID

<port_list>: Port list or 'all', default: All ports

Example:

Add port17 to port24 in PVLAN10

```
SWITCH/>pvlan add 10 17-24
```

PVLAN Delete

Description:

Delete Private VLAN entry.

Syntax:

PVLAN Delete <pvlan_id>

Parameters:

<pvlan_id> : Private VLAN ID

Example:

Delete PVLAN10

```
SWITCH/>pvlan delete 10
```

PVLAN Lookup

Description:

Lookup Private VLAN entry.

Syntax:

PVLAN Lookup [<pvlan_id>]

Parameters:

<pvlan_id> : Private VLAN ID

Example:

Lookup PVLAN

```
SWITCH/> lookup

PVLAN ID    Ports
--------    -----
1               1-24
```

PVLAN Isolate

Description:

Set or show the port isolation mode.

Syntax:

PVLAN Isolate [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port isolation

disable : Disable port isolation

(default: Show port isolation port list)

Default Setting:

Promiscous

Example:

Enable isolate for port10

```
SWITCH/>pvlan isolate 10 enable
```

6.7 Security Command

Security Switch User Configuration

Description:

Show users configuration.

Syntax:

Security Switch Users Configuration

Default Setting:

User Name	Privilege
admin	15
guest	5

Example:

Enable isolate for port10

```
SWITCH/>security switch user configuration

Users Configuration:
```

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

User Name                       Privilege Level
------------------------------  ---------------
admin                                       15
guest                                        5
```

Security Switch User Add

Description:

Add or modify users entry.

Syntax:

Security Switch Users Add <user_name> <password> <privilege_level>

Parameters:

<user_name> : A string identifying the user name that this entry should belong to

<password> : The password for this user name. Use 'clear' or "" as null string

<privilege_level>: User privilege level (1-(15))

Example:

Add new user: username: test, password: test & privilege: 10

```
SWITCH/>security switch users add test test 10
```

Security Switch User Delete

Description:

Delete users entry.

Syntax:

Security Switch Users Delete <user_name>

Parameters:

<user_name> : A string identifying the user name that this entry should belong to

Example:

Delete test account.

```
SWITCH/>security switch users delete user
```

Security Switch Privilege Level Configuration

Description:

Show privilege configuration.

Syntax:

Security Switch Privilege Level Configuration

Example:

Show privilege level

```
SWITCH/>security switch privilege level configuration

Privilege Level Configuration:
==============================

Privilege Current Level: 15
Group Name                       Privilege Level
                                 CRO CRW SRO SRW
-------------------------------- --- --- --- ---
Aggregation                       5   10   5   10
Debug                            15   15  15   15
Diagnostics                       5   10   5   10
IGMP_Snooping                      5   10   5   10
IP                               5   10   5   10
LACP                              5   10   5   10
LLDP                              5   10   5   10
LLDP-MED                           5   10   5   10
MAC_Table                         5   10   5   10
MVR                               5   10   5   10
Maintenance                      15   15  15   15
Mirroring                        5   10   5   10
Port_Security                    5   10   5   10
Ports                            5   10   1   10
Private_VLANs                     5   10   5   10
QoS                              5   10   5   10
SNMP                              5   10   5   10
```

Security	**5**	**10**	**5**	**10**
Spanning_Tree	**5**	**10**	**5**	**10**
System	**5**	**10**	**1**	**10**
UPnP	**5**	**10**	**5**	**10**
VLANs	**5**	**10**	**5**	**10**
Voice_VLAN	**5**	**10**	**5**	**10**

Security Switch Privilege Level Group

Description:

Configure a privilege level group.

Syntax:

Security Switch Privilege Level Group <group_name> [<cro>] [<crw>] [<sro>] [<srw>]

Parameters:

<group_name>: Privilege group name, default: Show all group privilege level

<cro> : Configuration read-only privilege level (1-(15))

<crw> : Configuration/Execute read-write privilege level (1-(15))

<sro> : Status/Statistics read-only privilege level (1-(15))

<srw> : Status/Statistics read-write privilege level (1-(15))

Example:

Change privilege level of MVR group.

```
SWITCH/>security switch privilege level group mvr 15 15 15 15
```

Security Switch Auth Configuration

Description:

Show Auth configuration.

Syntax:

Security Switch Auth Configuration

Default Setting:

Authentication Method: local

Fallback: disable

Example:

Show authentication configuration.

```
SWITCH/>security switch auth configuration

Auth Configuration:
====================

Client     Authentication Method     Local Authentication Fallback
-------    ----------------------    -----------------------------
console    local                     Disabled
telnet     local                     Disabled
ssh        local                     Disabled
web        local                     Disabled
```

Security Switch Auth Method

Description:

Set or show Auth method.

Syntax:

Security Switch Auth Method [console|telnet|ssh|web] [none|local|radius|tacacs+] [enable|disable]

Parameters:

console : Settings for console

telnet : Settings for telnet

ssh : Settings for ssh

web : Settings for web

none : Authentication disabled

local : Use local authentication

radius : Use remote RADIUS authentication

tacacs+ : Use remote TACACS+ authentication

(default: Show client authentication method)

enable : Enable local authentication if remote authentication fails

disable : Disable local authentication if remote authentication fails

(default: Show backup client authentication configuration)

Default Setting:

Authentication Method: local

Fallback: disable

Example:

Use RADIUS authentication method for telnet.

```
SWITCH/>security switch auth method telnet radius enable
```

Security Switch SSH Configuration

Description:

Show SSH configuration.

Syntax:

Security Switch SSH Configuration

Example:

Show SSH configuration.

```
SWITCH/>security switch ssh configuration

SSH Configuration:
==================

SSH Mode : Disabled
```

Security Switch SSH Mode

Description:

Set or show the SSH mode.

Syntax:

Security Switch SSH Mode [enable|disable]

Parameters:

enable : Enable SSH

disable: Disable SSH

(default: Show SSH mode)

Default Setting:

disable

Example:

Enable SSH function.

```
SWITCH/>security switch ssh mode enable
```

Security Switch HTTPs Configuration

Description:

Show HTTPS configuration.

Syntax:

Security Switch HTTPS Configuration

Default Setting:

disable

Example:

Show HTTPs configuration.

```
SWITCH/>security switch https configuration

HTTPS Configuration:
====================

HTTPS Mode              : Disabled
HTTPS Redirect Mode : Disabled
```

Security Switch HTTPs Mode

Description:

Set or show the HTTPS mode.

Syntax:

Security Switch HTTPS Mode [enable|disable]

Parameters:

enable : Enable HTTPs

disable: Disable HTTPs

(default: Show HTTPs mode)

Default Setting:

disable

Example:

Enable HTTPs function.

```
SWITCH/>security switch https mode enable
```

Security Switch HTTPs Redirect

Description:

et or show the HTTPS redirect mode.

Automatic redirect web browser to HTTPS during HTTPS mode enabled.

Syntax:

Security Switch HTTPS Redirect [enable|disable]

Parameters:

enable : Enable HTTPs redirect

disable: Disable HTTPs redirect

(default: Show HTTPs redirect mode)

Default Setting:

disable

Example:

Enable HTTPs redirect function.

```
SWITCH/>security switch https redirect enable
```

Security Switch Access Configuration

Description:

Show access management configuration.

Syntax:

Security Switch Access Configuration

Example:

Show access management configuration.

```
SWITCH/>security switch access configuration

Access Mgmt Configuration:
==========================

System Access Mode : Disabled
System Access number of entries: 0
```

Security Switch Access Mode

Description:

Set or show the access management mode.

Syntax:

Security Switch Access Mode [enable|disable]

Parameters:

enable : Enable access management

disable: Disable access management

(default: Show access management mode)

Default Setting:

disable

Example:

Enable access management function.

```
SWITCH/>security switch access mode enable
```

Security Switch Access Add

Description:

Add access management entry.

Syntax:

Security Switch Access Add <access_id> <start_ip_addr> <end_ip_addr> [web|snmp|telnet]

Parameters:

<access_id> : entry index (1-16)

<start_ip_addr>: Start IP address (a.b.c.d)

<end_ip_addr> : End IP address (a.b.c.d)

web : WEB/HTTPS interface

snmp : SNMP interface

telnet : TELNET/SSH interface

(default: Show configured and current mode)

Example:

Add access management list from 192.168.0.1 to 192.168.0.200 via web interface.

```
SWITCH/>security switch access add 1 192.168.0.1 192.168.0.200 web
```

Security Switch Access IPv6 Add

Description:

Add access management IPv6 entry.

Syntax:

Security Switch Access Ipv6 Add <access_id> <start_ipv6_addr> <end_ipv6_addr> [web|snmp|telnet]

Parameters:

access_id> : entry index (1-16)

<start_ipv6_addr>: Start IPv6 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, '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'.

<end_ipv6_addr> : End IPv6 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, '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'.

web : WEB/HTTPS interface

snmp : SNMP interface

telnet : TELNET/SSH interface

(default: Show configured and current mode)

Example:

Add access management list from 2001::0001 to 2001::0100 via web interface.

```
SWITCH/> security switch access add 2001::0001 2001::0100 web
```

Security Switch Access Delete

Description:

Delete access management entry.

Syntax:

Security Switch Access Delete <access_id

Parameters:

<access_id> : entry index (1-16)

Example:

Delete access management ID 1

```
SWITCH/>security switch access delete 1
```

Security Switch Access Lookup

Description:

Lookup access management entry.

Syntax:

Security Switch Access Lookup [<access_id>]

Parameters:

<access_id> : entry index (1-16)

Example:

Lookup access management entry.

```
SWITCH/>security switch access lookup 1
```

Security Switch Access Lookup

Description:

Clear access management entry.

Syntax:

Security Switch Access Clear

Example:

Clear access management entry.

```
SWITCH/>security switch access clear
```

Security Switch Access Clear

Description:

Show or clear access management statistics.

Syntax:

Security Switch Access Statistics [clear]

Parameters:

clear: Clear access management statistics

Default Setting:

disable

Example:

Show access management statistics.

```
SWITCH/>security switch access statistics

Access Management Statistics:
-----------------------------
HTTP     Receive:    79    Allow:    7    Discard:    72
HTTPS    Receive:    0     Allow:    0    Discard:    0
SNMP     Receive:    0     Allow:    0    Discard:    0
```

```
TELNET    Receive:          0     Allow:          0     Discard:          0
SSH       Receive:          0     Allow:          0     Discard:          0
```

Security Switch SNMP Configuration

Description:

Show SNMP configuration.

Syntax:

Security Switch SNMP Configuration

Example:

Show SNMP configuration.

```
SWITCH/>security switch snmp configuration

SNMP Configuration:
===================

SNMP Mode                          : Enabled
SNMP Version                       : 2c
Read Community                     : public
Write Community                    : private
Trap Mode                          : Disabled
Trap Version                       : 1
Trap Community                     : public
Trap Destination                   :
Trap IPv6 Destination              : ::
Trap Authentication Failure        : Enabled
Trap Link-up and Link-down         : Enabled
Trap Inform Mode                   : Enabled
Trap Inform Timeout (seconds)      : 1
Trap Inform Retry Times            : 5
Trap Probe Security Engine ID      : Enabled
Trap Security Engine ID            :
Trap Security Name                 : None

SNMPv3 Engine ID : 800007e5017f000001
```

```
SNMPv3 Communities Table:
Idx Community                          Source IP           Source Mask
--- ---------------------------------- --------------- ---------------
1     public                                0.0.0.0             0.0.0.0
2     private                               0.0.0.0             0.0.0.0

Number of entries: 2

SNMPv3 Users Table:
Idx Engine ID User Name                              Level              Auth Priv
--- --------- ---------------------------------- -------------- ---- ----
1     Local         default_user                          NoAuth, NoPriv None None

Number of entries: 1

SNMPv3 Groups Table;
Idx Model Security Name                          Group Name
--- ----- ---------------------------------- --------------------------------
1     v1       public                                default_ro_group
2     v1       private                               default_rw_group
3     v2c      public                                default_ro_group
4     v2c      private                               default_rw_group
5     usm      default_user                          default_rw_group

Number of entries: 5

SNMPv3 Views Table:
Idx View Name                                  View Type OID Subtree
--- ---------------------------------- --------- --------------------------------
1     default_view                           included    .1

Number of entries: 1

SNMPv3 Accesses Table:
Idx Group Name                                 Model Level
--- ---------------------------------- ----- --------------
1     default_ro_group                       any     NoAuth, NoPriv
2     default_rw_group                       any     NoAuth, NoPriv

Number of entries: 2
```

Security Switch SNMP Mode

Description:

Set or show the SNMP mode.

Syntax:

Security Switch SNMP Mode [enable|disable]

Parameters:

enable : Enable SNMP

disable: Disable SNMP

(default: Show SNMP mode)

Default Setting:

enable

Example:

Disable SNMP mode.

```
SWITCH/>security switch snmp mode disable
```

Security Switch SNMP Version

Description:

Set or show the SNMP protocol version.

Syntax:

Security Switch SNMP Version [1|2c|3]

Parameters:

1 : SNMP version 1

2c: SNMP version 2c

3 : SNMP version 3

(default: Show SNMP version)

Default Setting:

2c

Example:

Set SNMP in version 3.

```
SWITCH/>security switch snmp version 3
```

Security Switch SNMP Read Community

Description:

Set or show the community string for SNMP read access.

Syntax:

Security Switch SNMP Read Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string

(default: Show SNMP read community)

Default Setting:

public

Example:

Set SNMP read community private.

```
SWITCH/>security switch snmp read community private
```

Security Switch SNMP Write Community

Description:

Set or show the community string for SNMP write access.

Syntax:

Security Switch SNMP Write Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string

(default: Show SNMP write community)

Default Setting:

private

Example:

Set public value in SNMP write community.

```
SWITCH/>security switch snmp write community public
```

Security Switch SNMP Trap Mode

Description:

Set or show the SNMP trap mode.

Syntax:

Security Switch SNMP Trap Mode [enable|disable]

Parameters:

enable : Enable SNMP traps

disable: Disable SNMP traps

(default: Show SNMP trap mode)

Default Setting:

disable

Example:

Enable SNMP trap mode.

```
SWITCH/>security switch snmp trap mode enable
```

Security Switch SNMP Trap Version

Description:

Set or show the SNMP trap protocol version.

Syntax:

Security Switch SNMP Trap Version [1|2c|3]

Parameters:

1 : SNMP version 1

2c: SNMP version 2c

3 : SNMP version 3

(default: Show SNMP trap version)

Default Setting:

1

Example:

Set SNMP trap version in version 2c.

```
SWITCH/>security switch snmp trap version 2c
```

Security Switch SNMP Trap Community

Description:

Set or show the community string for SNMP traps.

Syntax:

Security Switch SNMP Trap Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string

(default: Show SNMP trap community)

Default Setting:

public

Example:

Set private value for SNMP trap community.

```
SWITCH/>security switch snmp trap community private
```

Security Switch SNMP Trap Destination

Description:

Set or Show the SNMP trap destination address.

Syntax:

Security Switch SNMP Trap Destination [<ip_addr_string>]

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Example:

Set SNMP trap destination address for 192.168.0.20

```
SWITCH/>security switch snmp trap destination 192.168.0.20
```

Security Switch SNMP Trap IPv6 Destination

Description:

Set or Show the SNMP trap destination IPv6 address.

Syntax:

Security Switch SNMP Trap IPv6 Destination [<ipv6_addr>]

Parameters:

<ipv6_addr>: 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'.

Example:

Set SNMP trap IPv6 destination address for 2001::0001

```
SWITCH/>security switch snmp trap ipv6 destination 2001::0001
```

Security Switch SNMP Trap Authentication Failure

Description:

Set or show the SNMP authentication failure trap mode.

Syntax:

Security Switch SNMP Trap Authentication Failure [enable|disable]

Parameters:

enable : Enable SNMP trap authentication failure

disable: Disable SNMP trap authentication failure

(default: Show SNMP trap authentication failure mode)

Default Setting:

enable

Example:

Disable SNMP trap authentication failure

```
SWITCH/>security switch snmp trap authentication failure disable
```

Security Switch SNMP Trap Link-up

Description:

Set or show the port link-up and link-down trap mode.

Syntax:

Security Switch SNMP Trap Link-up [enable|disable]

Parameters:

enable : Enable SNMP trap link-up and link-down

disable: Disable SNMP trap link-up and link-down

(default: Show SNMP trap link-up and link-down mode)

Default Setting:

enable

Example:

Disable SNMP trap link-up

```
SWITCH/>security switch snmp trap link-up disable
```

Security Switch SNMP Trap Inform Mode

Description:

Set or show the SNMP trap inform mode.

Syntax:

Security Switch SNMP Trap Inform Mode [enable|disable]

Parameters:

enable : Enable SNMP trap inform

disable: Disable SNMP trap inform

(default: Show SNMP inform mode)

Default Setting:

enable

Example:

Disable SNMP trap inform mode.

```
SWITCH/>security switch snmp trap inform mode disable
```

Security Switch SNMP Trap Inform Timeout

Description:

Set or show the SNMP trap inform timeout (usecs).

Syntax:

Security Switch SNMP Trap Inform Timeout [<timeout>]

Parameters:

<timeout>: SNMP trap inform timeout (0-2147 seconds)

(default: Show SNMP trap inform timeout)

Default Setting:

1

Example:

Set SNMP trap inform timeout in 20sec.

```
SWITCH/>security switch snmp trap inform timeout 20
```

Security Switch SNMP Trap Retry Times

Description:

Set or show the SNMP trap inform retry times.

Syntax:

Security Switch SNMP Trap Inform Retry Times [<retries>]

Parameters:

<retries>: SNMP trap inform retransmited times (0-255)

(default: Show SNMP trap inform retry times)

Default Setting:

5

Example:

Set SNMP trap inform retry times in 10.

```
SWITCH/>security switch snmp trap inform retry times 10
```

Security Switch SNMP Trap Probe Security Engine ID

Description:

Show SNMP trap security engine ID probe mode.

Syntax:

Security Switch SNMP Trap Probe Security Engine ID [enable|disable]

Parameters:

enable : Enable SNMP trap security engine ID probe

disable: Disable SNMP trap security engine ID probe

(default: Show SNMP trap security engine ID probe mode)

Default Setting:

enable

Example:

Disable SNMP trap probe security engine ID

```
SWITCH/>security switch snmp trap probe security engine id disable
```

Security Switch SNMP Trap Security Engine ID

Description:

Set or show SNMP trap security engine ID.

Syntax:

Security Switch SNMP Trap Security Engine ID [<engineid>]

Parameters:

<engineid>: Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

Example:

Set the SNMP trap security engine ID

```
SWITCH/>security switch snmp trap security engine id 800007e5017f000011
```

Security Switch SNMP Trap Security Name

Description:

Set or show SNMP trap security name.

Syntax:

Security Switch SNMP Trap Security Name [<security_name>]

Parameters:

<security_name>: A string representing the security name for a principal

(default: Show SNMP trap security name)

Example:

Set the SNMP trap security name

```
SWITCH/>security switch snmp trap security name 12345678
```

Security Switch SNMP Engine ID

Description:

Set or show SNMPv3 local engine ID.

Syntax:

Security Switch SNMP Engine ID [<engineid>]

Parameters:

<engineid>: Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

Default Setting:

800007e5017f000001

Example:

Set 800007e5017f000002 for SNMPv3 local engine ID

```
SWITCH/>security switch snmp engine id 800007e5017f000002
```

Security Switch SNMP Community Add

Description:

Add or modify SNMPv3 community entry.

The entry index key is <community>.

Syntax:

Security Switch SNMP Community Add <community> [<ip_addr>] [<ip_mask>]

Parameters:

<community>: Community string

<ip_addr> : IP address (a.b.c.d), default: Show IP address

<ip_mask> : IP subnet mask (a.b.c.d), default: Show IP mask

Example:

Add SNMPv3 community entry.

```
SWITCH/>security switch snmp community add public 192.168.0.20 255.255.255.0
```

Security Switch SNMP Community Delete

Description:

Delete SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 community entry

```
SWITCH/>security switch snmp community delete 3
```

Security Switch SNMP Community Lookup

Description:

Lookup SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 community entry

```
SWITCH/>security switch snmp community lookup
Idx Community                        Source IP          Source Mask
--- -------------------------------- ---------------    ---------------
1   public                           192.168.0.20       255.255.255.0
2   private                          0.0.0.0            0.0.0.0

Number of entries: 2
```

Security Switch SNMP User Add

Description:

Add SNMPv3 user entry.

The entry index key are <engineid> and <user_name> and it doesn't allow modify.

Syntax:

Security Switch SNMP User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]

Parameters:

<engineid> : Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

<user_name> : A string identifying the user name that this entry should belong to

md5: An optional flag to indicate that this user using MD5 authentication protocol

sha: An optional flag to indicate that this user using SHA authentication protocol

<auth_password>: A string identifying the authentication pass phrase

des: An optional flag to indicate that this user using DES privacy protocol privacy protocol should belong to

<priv_password>: A string identifying the privacy pass phrase

Example:

Add SNMPv3 user entry

```
SWITCH/>security switch snmp user add 800007e5017f000003 admin_snmpv3 md5
12345678 des abcdefgh
```

Security Switch SNMP User Delete

Description:

Delete SNMPv3 user entry.

Syntax:

Security Switch SNMP User Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 user entry

```
SWITCH/>security switch snmp user delete 1
```

Security Switch SNMP User Changekey

Description:

Change SNMPv3 user password.

Syntax:

Security Switch SNMP User Changekey <engineid> <user_name> <auth_password> [<priv_password>]

Parameters:

<engineid> : Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

<user_name> : A string identifying the user name that this entry should belong to

<auth_password>: A string identifying the authentication pass phrase

<priv_password>: A string identifying the privacy pass phrase

Example:

Delete SNMPv3 user entry

```
SWITCH/>security switch snmp user changekey 800007e5017f000003 admin_snmpv3
```

```
87654321 12345678
```

Security Switch SNMP User Lookup

Description:

Lookup SNMPv3 user entry.

Syntax:

Security Switch SNMP User Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 user entry

```
SWITCH/>security switch snmp user lookup
Idx Engine ID    User Name                       Level          Auth   Priv
---  ---------   ------------------------------  -------------  ----   ----
1    Remote      admin_snmpv3                     Auth, Priv     MD5   DES

Number of entries: 1
```

Security Switch SNMP Group Add

Description:

Add or modify SNMPv3 group entry.

The entry index key are <security_model> and <security_name>.

Syntax:

Security Switch SNMP Group Add <security_model> <security_name> <group_name>

Parameters:

<security_model>: v1 - Reserved for SNMPv1
v2c - Reserved for SNMPv2c
usm - User-based Security Model (USM)

<security_name> : A string identifying the security name that this entry should belong to

<group_name> : A string identifying the group name that this entry should belong to

Example:

Add SNMPv3 group entry

```
SWITCH/>security switch snmp group add usm admin_snmpv3 group_snmpv3
```

Security Switch SNMP Group Delete

Description:

Delete SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 group entry

```
SWITCH/>security switch snmp group delete 1
```

Security Switch SNMP Group Lookup

Description:

Lookup SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 group entry

```
SWITCH/>security switch snmp group lookup
Idx   Model   Security Name                    Group Name
---   -----   -----------------------------   -----------------------------
2     v1      private                         default_rw_group
```

```
3     v2c     public                          default_ro_group
4     v2c     private                         default_rw_group
5     usm     default_user                    default_rw_group

Number of entries: 4
```

Security Switch SNMP View Add

Description:

Add or modify SNMPv3 view entry.

The entry index key are <view_name> and <oid_subtree>.

Syntax:

Security Switch SNMP View Add <view_name> [included|excluded] <oid_subtree>

Parameters:

<view_name> : A string identifying the view name that this entry should belong to

included: An optional flag to indicate that this view subtree should included

excluded: An optional flag to indicate that this view subtree should excluded

<oid_subtree>: The OID defining the root of the subtree to add to the named view

Example:

Add SNMPv3 view entry

```
SWITCH/>security switch snmp view add snmpv3_view include .1
```

Security Switch SNMP View Delete

Description:

Delete SNMPv3 view entry.

Syntax:

Security Switch SNMP View Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 view entry

```
SWITCH/>security switch snmp view delete 3
```

Security Switch SNMP View Lookup

Description:

Lookup SNMPv3 view entry.

Syntax:

Security Switch SNMP View Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 view entry

```
SWITCH/>security switch snmp view lookup
Idx   View Name                        View Type   OID Subtree
---   ------------------------------  ---------   ------------------------------
1     default_view                    included    .1
2     snmpv3_viwe                     included    .1

Number of entries: 2
```

Security Switch SNMP Access Add

Description:

Add or modify SNMPv3 access entry.

The entry index key are <group_name>, <security_model> and <security_level>.

Syntax:

Security Switch SNMP Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]

Parameters:

<group_name> : A string identifying the group name that this entry should belong to

<security_model> : any - Accepted any security model (v1|v2c|usm)

v1 - Reserved for SNMPv1

v2c - Reserved for SNMPv2c

usm - User-based Security Model (USM)

<security_level> : noAuthNoPriv - None authentication and none privacy

AuthNoPriv - Authentication and none privacy

AuthPriv - Authentication and privacy

<read_view_name> : The name of the MIB view defining the MIB objects for which this request may request the current values

<write_view_name>: The name of the MIB view defining the MIB objects for which this request may potentially SET new values

Example:

Add SNMPv3 access entry

```
SWITCH/>security switch snmp access add group_snmpv3 usm authpriv snmpv3_view snmpv3_view
```

Security Switch SNMP Access Delete

Description:

Delete SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 access entry

```
SWITCH/>security switch snmp access delete 3
```

Security Switch SNMP Access Lookup

Description:

Lookup SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 access entry

```
SWITCH/>security switch snmp access lookup
Idx Group Name                          Model Level
--- ----------------------------------- ----- --------------
1     default_ro_group                  any     NoAuth, NoPriv
2     default_rw_group                  any     NoAuth, NoPriv

Number of entries: 2
```

Security Network Psec Switch

Description:

Show Port Security status.

Syntax:

Security Network Psec Switch [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Default Setting:

800007e5017f000001

Example:

Show port security status.

```
SWITCH/>security network psec switch
Users:
L = Limit Control
8 = 802.1X
D = DHCP Snooping
V = Voice VLAN
```

Port	Users	State	MAC Cnt
1	----	No users	0
2	----	No users	0
3	----	No users	0
4	----	No users	0
5	----	No users	0
6	----	No users	0
7	----	No users	0
8	----	No users	0
9	----	No users	0
10	----	No users	0
11	----	No users	0
12	----	No users	0
13	----	No users	0
14	----	No users	0
15	----	No users	0
16	----	No users	0
17	----	No users	0
18	----	No users	0
19	----	No users	0
20	----	No users	0
21	----	No users	0
22	----	No users	0
23	----	No users	0
24	----	No users	0

Security Network Psec Port

Description:

Show MAC Addresses learned by Port Security.

Syntax:

Security Network Psec Port [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show MAC address learned on port 1

```
SWITCH/>security network psec port 1

Port 1:
-------

MAC Address          VID    State         Added                        Age/Hold Time
-----------------    ----   ----------    -------------------------    -------------
<none>
```

Security Network Limit Configuration

Description:

Show Limit Control configuration.

Syntax:

Security Network Limit Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show Limit Control configuration.

```
SWITCH/>security network limit configuration

Port Security Limit Control Configuration:
==========================================

Mode         : Disabled
Aging        : Disabled
Age Period: 3600

Port   Mode          Limit   Action
----   --------      -----   ---------------
1      Disabled        4     None
2      Disabled        4     None
3      Disabled        4     None
4      Disabled        4     None
```

5	**Disabled**	**4**	**None**
6	**Disabled**	**4**	**None**
7	**Disabled**	**4**	**None**
8	**Disabled**	**4**	**None**
9	**Disabled**	**4**	**None**
10	**Disabled**	**4**	**None**
11	**Disabled**	**4**	**None**
12	**Disabled**	**4**	**None**
13	**Disabled**	**4**	**None**
14	**Disabled**	**4**	**None**
15	**Disabled**	**4**	**None**
16	**Disabled**	**4**	**None**
17	**Disabled**	**4**	**None**
18	**Disabled**	**4**	**None**
19	**Disabled**	**4**	**None**
20	**Disabled**	**4**	**None**
21	**Disabled**	**4**	**None**
22	**Disabled**	**4**	**None**
23	**Disabled**	**4**	**None**
24	**Disabled**	**4**	**None**

Security Network Limit Mode

Description:

Set or show global enabledness.

Syntax:

Security Network Limit Mode [enable|disable]

Parameters:

enable : Globally enable port security

disable : Globally disable port security

(default: Show current global enabledness of port security limit control)

Default Setting:

disable

Example:

Enable the limit mode

```
SWITCH/>security network limit mode enable
```

Security Network Limit Aging

Description:

Set or show aging enabledness.

Syntax:

Security Network Limit Aging [enable|disable]

Parameters:

enable : Enable aging

disable : Disable aging

(default: Show current enabledness of aging)

Default Setting:

disable

Example:

Enable limit aging

```
SWITCH/>security network limit aging enable
```

Security Network Limit Agetime

Description:

Time in seconds between check for activity on learned MAC addresses.

Syntax:

Security Network Limit Agetime [<age_time>]

Parameters:

<age_time>: Time in seconds between checks for activity on a MAC address (10-10000000 seconds)

(default: Show current age time)

Default Setting:

3600

Example:

Set age time in 100sec.

```
SWITCH/>security network limit agetime 100
```

Security Network Limit Port

Description:

Set or show per-port enabledness.

Syntax:

Security Network Limit Port [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port security on this port

disable : Disable port security on this port

(default: Show current port enabledness of port security limit control)

Default Setting:

disable

Example:

Enable port limit for port 1

```
SWITCH/>security network limit port 1 enable
```

Security Network Limit Limit

Description:

Set or show the max. number of MAC addresses that can be learned on this set of ports.

Syntax:

Security Network Limit Limit [<port_list>] [<limit>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<limit> : Max. number of MAC addresses on this port

(default: Show current limit)

Default Setting:

4

Example:

Set limit in 5

```
SWITCH/>security network limit limit 1-24 5
```

Security Network Limit Action

Description:

Set or show the action involved with exceeding the limit.

Syntax:

Security Network Limit Action [<port_list>] [none|trap|shut|trap_shut]

Parameters:

<port_list> : Port list or 'all', default: All ports

none|trap|shut|trap_shut: Action to be taken in case the number of MAC addresses exceeds the limit

none : Don't do anything

trap : Send an SNMP trap

shut : Shutdown the port

trap_shut: Send an SNMP trap and shutdown the port

(default: Show current action)

Default Setting:

none

Example:

Set trap mode for limit action for port 1

```
SWITCH/>security network limit action 1 trap
```

Security Network Limit Reopen

Description:

Reopen one or more ports whose limit is exceeded and shut down.

Syntax:

Security Network Limit Reopen [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Reopen port 1

```
SWITCH/>security network limit reopen 1
```

Security Network NAS Configuration

Description:

Show 802.1X configuration.

Syntax:

Security Network NAS Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show 802.1X configuration of port 1

```
SWITCH/>security network nas configuration 1

802.1X Configuration:
=====================

Mode                  : Disabled
Reauth.               : Disabled
Reauth. Period        : 3600
EAPOL Timeout         : 30
Age Period            : 300
Hold Time             : 10
RADIUS QoS            : Disabled
RADIUS VLAN           : Disabled
Guest VLAN            : Disabled
Guest VLAN ID         : 1
```

```
Max. Reauth Count: 2
Allow Guest VLAN if EAPOL Frame Seen: Disabled

Port   Admin State          Port State           Last Source      Last ID
----   -----------------    ---------------------  ---------------  -----------------
1      Force Authorized     Globally Disabled      -                -
```

Security Network NAS Mode

Description:

Set or show the global NAS enabledness.

Syntax:

Security Network NAS Mode [enable|disable]

Parameters:

enable : Globally enable 802.1X

disable: Globally disable 802.1X

(default: Show current 802.1X global enabledness)

Default Setting:

disable

Example:

Enable IEEE802.1X function

```
SWITCH/>security network nas mode enable
```

Security Network NAS State

Description:

Set or show the port security state.

Syntax:

Security Network NAS State [<port_list>] [auto|authorized|unauthorized|single|multi|macbased]

Parameters:

<port_list>: Port list or 'all', default: All ports

auto : Port-based 802.1X Authentication

authorized : Port access is allowed

unauthorized: Port access is not allowed

single : Single Host 802.1X Authentication

multi : Multiple Host 802.1X Authentication

macbased : Switch authenticates on behalf of the client

(default: Show 802.1X state)

Default Setting:

none

Example:

Show the port 1 security state.

```
SWITCH/>security network nas state 1

Port   Admin State          Port State           Last Source        Last ID
----   -----------------    ------------------   ----------------   -----------------
1      Force Authorized     Link Down              -                  -
```

Security Network NAS Reauthentication

Description:

Set or show Reauthentication enabledness.

Syntax:

Security Network NAS Reauthentication [enable|disable]

Parameters:

enable : Enable reauthentication

disable: Disable reauthentication

(default: Show current reauthentication mode)

Default Setting:

disable

Example:

Enable reauthentication function.

```
SWITCH/>security network nas reauthentication enable
```

Security Network NAS ReauthPeriod

Description:

Set or show the period between reauthentications.

Syntax:

Security Network NAS ReauthPeriod [<reauth_period>]

Parameters:

<reauth_period>: Period between reauthentications (1-3600 seconds)

(default: Show current reauthentication period)

Default Setting:

3600

Example:

Set reauthentication period in 3000sec.

```
SWITCH/>security network nas reauthperiod 3000
```

Security Network NAS EapolTimeout

Description:

Set or show the time between EAPOL retransmissions.

Syntax:

Security Network NAS EapolTimeout [<eapol_timeout>]

Parameters:

<eapol_timeout>: Time between EAPOL retransmissions (1-65535 seconds)

(default: Show current EAPOL retransmission timeout)

Default Setting:

30

Example:

Set the time between EAPOL retransmissions for 100sec.

```
SWITCH/>security network nas eapoltimeout 100
```

Security Network NAS Agetime

Description:

Time in seconds between check for activity on successfully authenticated MAC addresses.

Syntax:

Security Network NAS Agetime [<age_time>]

Parameters:

<age_time>: Time between checks for activitiy on a MAC address that succeeded autentication

(default: Show current age time)

Default Setting:

300

Example:

Set NAS age time in 1000sec

```
SWITCH/>security network nas agetime 1000
```

Security Network NAS Holdtime

Description:

Time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Syntax:

Security Network NAS Holdtime [<hold_time>]

Parameters:

<hold_time>: Hold time before MAC addresses that failed authentication expire

(default: Show current hold time)

Default Setting:

10

Example:

Set NAS hold time in 100sec

```
SWITCH/>security network nas holdtime 100
```

Security Network NAS RADIUS_QoS

Description:

Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned QoS.

Syntax:

Security Network NAS RADIUS_QoS [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned QoS setting

<port_list>: Select the per-port RADIUS-assigned QoS setting

(default: Show current per-port RADIUS-assigned QoS enabledness)

enable : Enable RADIUS-assigned QoS either globally or on one or more ports

disable: Disable RADIUS-assigned QoS either globally or on one or more ports

(default: Show current RADIUS-assigned QoS enabledness)

Default Setting:

disable

Example:

Enable NAS RADIUS QoS

```
SWITCH/>security network nas radius_qos enable
```

Security Network NAS RADIUS_VLAN

Description:

Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned VLAN.

Syntax:

Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned VLAN setting

<port_list>: Select the per-port RADIUS-assigned VLAN setting

(default: Show current per-port RADIUS-assigned VLAN enabledness)

enable : Enable RADIUS-assigned VLAN either globally or on one or more ports

disable: Disable RADIUS-assigned VLAN either globally or on one or more ports

(default: Show current RADIUS-assigned VLAN enabledness)

Default Setting:

disable

Example:

Enable NAS RADIUS VLAN

```
SWITCH/>security network nas radius_vlan enable
```

Security Network NAS Guest_VLAN

Description:

Set or show either global enabledness and parameters (use the global keyword) or per-port enabledness of Guest VLAN Unless the 'global' keyword is used, the <reauth_max> and <allow_if_eapol_seen> parameters will not be unused.

Syntax:

Security Network NAS Guest_VLAN [global|<port_list>] [enable|disable] [<vid>] [<reauth_max>] [<allow_if_eapol_seen>]

Parameters:

global : Select the global Guest VLAN setting

<port_list>: Select the per-port Guest VLAN setting

(default: Show current per-port Guest VLAN enabledness)

enable|disable : enable : Enable Guest VLAN either globally or on one or more ports

disable: Disable Guest VLAN either globally or on one or more ports

(default: Show current Guest VLAN enabledness)

<vid> : Guest VLAN ID used when entering the Guest VLAN. Use the 'global' keyword to change it

(default: Show current Guest VLAN ID)

<reauth_max> : The value can only be set if you use the 'global' keyword in the beginning of the command. The number of times a Request Identity EAPOL frame is sent without reasponse before considering entering the Guest VLAN

(default: Show current Maximum Reauth Count value)

<allow_if_eapol_seen>: The value can only be set if you use the 'global' keyword in the beginning of the command.

disable:The Guest VLAN can only be entered if no EAPOL frames have been received on a port for the lifetime of the port

enable :The Guest VLAN can be entered even if an EAPOL frame has been received during the lifetime of the port

(default: Show current setting)

Default Setting:

disable

Example:

Enable NAS guest VLAN

```
SWITCH/>security network nas guest_vlan enable
```

Security Network NAS Authenticate

Description:

Refresh (restart) 802.1X authentication process.

Syntax:

Security Network NAS Authenticate [<port_list>] [now]

Parameters:

<port_list>: Port list or 'all', default: All ports

now : Force reauthentication immediately

Example:

Start NAS authentication now for port 1.

```
SWITCH/>security network nas authenticate 1 now
```

Security Network NAS Statistics

Description:

Show or clear 802.1X statistics.

Syntax:

Security Network NAS Statistics [<port_list>] [clear|eapol|radius]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear statistics

eapol : Show EAPOL statistics

radius : Show Backend Server statistics

(default: Show all statistics)

Example:

Show 802.1X statistics in port 1

```
SWITCH/>security network nas statistics 1
Port 1 EAPOL Statistics:
```

```
Rx Total:                    0     Tx Total:                    0
Rx Response/Id:              0     Tx Request/Id:               0
Rx Response:                 0     Tx Request:                  0
Rx Start:                    0
Rx Logoff:                   0
Rx Invalid Type:             0
Rx Invalid Length:           0

Port 1 Backend Server Statistics:

Rx Access Challenges:        0     Tx Responses:                0
Rx Other Requests:           0
Rx Auth. Successes:          0
Rx Auth. Failures:           0
```

Security Network ACL Configuration

Description:

Show ACL Configuration.

Syntax:

Security Network ACL Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show ACL Configuration.

```
SWITCH/>security network acl configuration
ACL Configuration:
==================

Port   Policy   Action   Rate Limiter   Port Copy   Logging    Shutdown   Counter
----   ------   ------   ------------   ---------   --------   --------   -------
1      1        Permit   Disabled       Disabled    Disabled   Disabled   0
2      1        Permit   Disabled       Disabled    Disabled   Disabled   0
```

3	1	Permit	Disabled	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	Disabled	Disabled	0
8	1	Permit	Disabled	Disabled	Disabled	Disabled	0
9	1	Permit	Disabled	Disabled	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	Disabled	Disabled	0
11	1	Permit	Disabled	Disabled	Disabled	Disabled	0
12	1	Permit	Disabled	Disabled	Disabled	Disabled	0
13	1	Permit	Disabled	Disabled	Disabled	Disabled	0
14	1	Permit	Disabled	Disabled	Disabled	Disabled	0
15	1	Permit	Disabled	Disabled	Disabled	Disabled	0
16	1	Permit	Disabled	Disabled	Disabled	Disabled	0
17	1	Permit	Disabled	Disabled	Disabled	Disabled	0
18	1	Permit	Disabled	Disabled	Disabled	Disabled	746
19	1	Permit	Disabled	Disabled	Disabled	Disabled	0
20	1	Permit	Disabled	Disabled	Disabled	Disabled	0
21	1	Permit	Disabled	Disabled	Disabled	Disabled	0
22	1	Permit	Disabled	Disabled	Disabled	Disabled	0
23	1	Permit	Disabled	Disabled	Disabled	Disabled	0
24	1	Permit	Disabled	Disabled	Disabled	Disabled	0

Rate Limiter	Rate
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1

```
Number of ACEs: 0
```

Security Network ACL Action

Description:

Set or show the ACL port default action.

Syntax:

Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]

Parameters:

<port_list> : Port list or 'all', default: All ports

permit : Permit forwarding (default)

deny : Deny forwarding

<rate_limiter>: Rate limiter number (1-15) or 'disable'

<port_copy> : Port number for copy of frames or 'disable'

<logging> : System logging of frames: log|log_disable

<shutdown> : Shut down ingress port: shut|shut_disable

Default Setting:

300

Example:

Show ACL action in port 1

```
SWITCH/>security network acl action 1

Port   Action   Rate Limiter   Port Copy   Logging    Shutdown   Counter
----    ------     ------------      ---------       --------     --------     -------
1       Permit   Disabled        Disabled    Disabled   Disabled     0
```

Security Network ACL Policy

Description:

Set or show the ACL port policy.

Syntax:

Security Network ACL Policy [<port_list>] [<policy>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<policy> : Policy number (1-8)

Default Setting:

1

Example:

Set ACL policy 2 for port 1

```
SWITCH/>security network acl policy 1 2
```

Security Network ACL Rate

Description:

Set or show the ACL rate limiter.

Syntax:

Security Network ACL Rate [<rate_limiter_list>] [<packet_rate>]

Parameters:

<rate_limiter_list>: Rate limiter list (1-15), default: All rate limiters

<packet_rate> : Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

1

Example:

Set rate limit value in 1024k for port 1

```
SWITCH/>security network acl rate 1 1024k
```

Security Network ACL Add

Description:

Add or modify Access Control Entry (ACE).

If the ACE ID parameter <ace_id> is specified and an entry with this ACE ID already exists, the ACE will be modified. Otherwise, a new ACE will be added. If the ACE ID is not specified, the next available ACE ID will be used.

If the next ACE ID parameter <ace_id_next> is specified, the ACE will be placed before this ACE in the list. If the next ACE ID is not specified, the ACE will be placed last in the list.

If the Switch keyword is used, the rule applies to all ports. If the Port keyword is used, the rule applies to the specified port only. If the Policy keyword is used, the rule applies to all ports configured with the specified policy. The default is that the rule applies to all ports.

Syntax:

Security Network ACL Add [<ace_id>] [<ace_id_next>] [switch | (port <port>) | (policy <policy>)] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]

Parameters:

<ace_id> : ACE ID (1-128), default: Next available ID
<ace_id_next> : Next ACE ID (1-128), default: Add ACE last
switch : Switch ACE keyword
port : Port ACE keyword
<port> : Port number
policy : Policy ACE keyword
<policy> : Policy number (1-8)
<vid> : VLAN ID (1-4095) or 'any'
<tag_prio> : VLAN tag priority (0-7) or 'any'
<dmac_type> : DMAC type: any|unicast|multicast|broadcast
etype : Ethernet Type keyword
<etype> : Ethernet Type or 'any'
<smac> : Source MAC address (xx-xx-xx-xx-xx-xx) or 'any'
<dmac> : Destination MAC address (xx-xx-xx-xx-xx-xx) or 'any'
arp : ARP keyword
<sip> : Source IP address (a.b.c.d/n) or 'any'
<dip> : Destination IP address (a.b.c.d/n) or 'any'
<arp_opcode> : ARP operation code: any|arp|rarp|other
<arp_flags> : ARP flags: request|smac|tmac|len|ip|ether [0|1|any]
ip : IP keyword
<protocol> : IP protocol number (0-255) or 'any'
<ip_flags> : IP flags: ttl|options|fragment [0|1|any]

icmp : ICMP keyword

<icmp_type> : ICMP type number (0-255) or 'any'

<icmp_code> : ICMP code number (0-255) or 'any'

udp : UDP keyword

<sport> : Source UDP/TCP port range (0-65535) or 'any'

<dport> : Destination UDP/TCP port range (0-65535) or 'any'

tcp : TCP keyword

<tcp_flags> : TCP flags: fin|syn|rst|psh|ack|urg [0|1|any]

permit : Permit forwarding (default)

deny : Deny forwarding

<rate_limiter>: Rate limiter number (1-15) or 'disable'

<port_copy> : Port number for copy of frames or 'disable'

<logging> : System logging of frames: log|log_disable

<shutdown> : Shut down ingress port: shut|shut_disable

Security Network ACL Delete

Description:

Delete ACE.

Syntax:

Security Network ACL Delete <ace_id>

Parameters:

<ace_id>: ACE ID (1-128)

Example:

Delete ACE 1

```
SWITCH/>security network acl delete 1
```

Security Network ACL Lookup

Description:

Show ACE, default: All ACEs.

Syntax:

Security Network ACL Lookup [<ace_id>]

Parameters:

<ace_id>: ACE ID (1-128)

Example:

Lookup ACE 1

```
SWITCH/>security network acl lookup 1
```

Security Network ACL Clear

Description:

Clear all ACL counters.

Syntax:

Security Network ACL Clear

Example:

Clear all ACL counters.

```
SWITCH/>security network acl clear
```

Security Network ACL Status

Description:

Show ACL status.

Syntax:

Security Network ACL Status [combined|static|dhcp|upnp|arp_inspection|ip_source_guard|conflicts]

Parameters:

combined : Shows the combined status

static : Shows the static user configured status

dhcp : Shows the status by DHCP

upnp : Shows the status by UPnP

arp_inspection : Shows the status by ARP Inspection

ip_source_guard : Shows the status by IP Source Guard

conflicts : Shows all conflict status

(default : Shows the combined status)

Example:

Show ACL status.

```
SWITCH/>security network acl status
```

Security Network DHCP Relay Configuration

Description:

Show DHCP relay configuration.

Syntax:

Security Network DHCP Relay Configuration

Example:

Show DHCP relay configuration.

```
SWITCH/>security network dhcp relay configuration

DHCP Relay Configuration:
=========================

DHCP Relay Mode                  : Disabled
DHCP Relay Server                : NULL
DHCP Relay Information Mode      : Disabled
DHCP Relay Information Policy : replace
```

Security Network DHCP Relay Mode

Description:

Set or show the DHCP relay mode.

Syntax:

Security Network DHCP Relay Mode [enable|disable]

Parameters:

enable : Enable DHCP relaly mode.

When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered.

disable: Disable DHCP relaly mode

(default: Show flow DHCP relaly mode)

Default Setting:

disable

Example:

Enable DHCP relay mode

```
SWITCH/>security network dhcp relay mode enable
```

Security Network DHCP Relay Server

Description:

Show or set DHCP relay server.

Syntax:

Security Network DHCP Relay Server [<ip_addr>]

Parameters:

<ip_addr>: IP address (a.b.c.d), default: Show IP address

Default Setting:

null

Example:

Set DHCP relay server in 192.168.0.20

```
SWITCH/>security network dhcp relay server 192.168.0.20
```

Security Network DHCP Relay Information Mode

Description:

Set or show DHCP relay agent information option mode.

When enable DHCP relay information mode operation, the agent insert specific information (option 82) into a DHCP message when forwarding to DHCP server and remote it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled.

Syntax:

Security Network DHCP Relay Information Mode [enable|disable]

Parameters:

enable : Enable DHCP relay agent information option mode

disable: Disable DHCP relay agent information option mode

(default: Show DHCP relay agent information option mode)

Default Setting:

disable

Example:

Enable DHCP relay agent information option mode.

```
SWITCH/>security network dhcp relay information mode enable
```

Security Network DHCP Relay Information Policy

Description:

Set or show the DHCP relay mode.

When enable DHCP relay information mode operation, if agent receive a DHCP message that already contains relay agent information. It will enforce the policy.

Syntax:

Security Network DHCP Relay Information Policy [replace|keep|drop]

Parameters:

replace : Replace the original relay information when receive a DHCP message that already contains it

keep : Keep the original relay information when receive a DHCP message that already contains it

drop : Drop the package when receive a DHCP message that already contains relay information

(default: Show DHCP relay information policy)

Default Setting:

replace

Example:

Keep the original relay information when receive a DHCP message that already contains it

```
SWITCH/>security network dhcp relay information policy keep
```

Security Network DHCP Relay Statistics

Description:

Show or clear DHCP relay statistics.

Syntax:

Security Network DHCP Relay Statistics [clear]

Parameters:

clear: Clear DHCP relay statistics

Example:

Show DHCP relay statistics.

```
SWITCH/>security network dhcp relay statistics
```

Security Network DHCP Snooping Configuration

Description:

Show DHCP snooping configuration.

Syntax:

Security Network DHCP Snooping Configuration

Example:

Set NAS age time in 1000sec

```
SWITCH/>security network dhcp snooping configuration

DHCP Snooping Configuration:
============================

DHCP Snooping Mode : Disabled

Port    Port Mode
----    ----------
1       trusted
2       trusted
3       trusted
4       trusted
```

5	**trusted**
6	**trusted**
7	**trusted**
8	**trusted**
9	**trusted**
10	**trusted**
11	**trusted**
12	**trusted**
13	**trusted**
14	**trusted**
15	**trusted**
16	**trusted**
17	**trusted**
18	**trusted**
19	**trusted**
20	**trusted**
21	**trusted**
22	**trusted**
23	**trusted**
24	**trusted**

Security Network DHCP Snooping Mode

Description:

Set or show the DHCP snooping mode.

Syntax:

Security Network DHCP Snooping Mode [enable|disable]

Parameters:

enable : Enable DHCP snooping mode.

When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports.

disable: Disable DHCP snooping mode

(default: Show flow DHCP snooping mode)

Default Setting:

disable

Example:

Enable DHCP snooping mode

```
SWITCH/>security network dhcp snooping mode enable
```

Security Network DHCP Snooping Port Mode

Description:

Set or show the DHCP snooping port mode.

Syntax:

Security Network DHCP Snooping Port Mode [<port_list>] [trusted|untrusted]

Parameters:

<port_list>: Port list or 'all', default: All ports

trusted : Configures the port as trusted sources of the DHCP message

untrusted: Configures the port as untrusted sources of the DHCP message

(default: Show flow DHCP snooping port mode)

Default Setting:

trusted

Example:

Set untrusted DHCP snooping port mode in port 1

```
SWITCH/>security network dhcp snooping port mode 1 untrusted
```

Security Network DHCP Snooping Statistics

Description:

Show or clear DHCP snooping statistics.

Syntax:

Security Network DHCP Snooping Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear DHCP snooping statistics

Example:

Show DHCP snooping statistics of port 1.

```
SWITCH/>security network dhcp snooping statistics 1
Port 1 Statistics:
--------------------
Rx Discover:                0     Tx Discover:                0
Rx Offer:                   0     Tx Offer:                   0
Rx Request:                 0     Tx Request:                 0
Rx Decline:                 0     Tx Decline:                 0
Rx ACK:                     0     Tx ACK:                     0
Rx NAK:                     0     Tx NAK:                     0
Rx Release:                 0     Tx Release:                 0
Rx Inform:                  0     Tx Inform:                  0
Rx Lease Query:             0     Tx Lease Query:             0
Rx Lease Unassigned:        0     Tx Lease Unassigned:        0
Rx Lease Unknown:           0     Tx Lease Unknown:           0
Rx Lease Active:            0     Tx Lease Active:            0
```

Security Network IP Source Guard Configuration

Description:

Show IP source guard configuration.

Syntax:

Security Network IP Source Guard Configuration

Example:

Show IP source guard configuration.

```
SWITCH/>security network ip source guard configuration

IP Source guard Configuration:
==============================

IP Source Guard Mode : Disabled

Port    Port Mode       Dynamic Entry Limit
----    -----------     --------------------
1       Disabled        unlimited
```

```
2       Disabled        unlimited
3       Disabled        unlimited
4       Disabled        unlimited
5       Disabled        unlimited
6       Disabled        unlimited
7       Disabled        unlimited
8       Disabled        unlimited
9       Disabled        unlimited
10      Disabled        unlimited
11      Disabled        unlimited
12      Disabled        unlimited
13      Disabled        unlimited
14      Disabled        unlimited
15      Disabled        unlimited
16      Disabled        unlimited
17      Disabled        unlimited
18      Disabled        unlimited
19      Disabled        unlimited
20      Disabled        unlimited
21      Disabled        unlimited
22      Disabled        unlimited
23      Disabled        unlimited
24      Disabled        unlimited

IP Source Guard Entry Table:

Type        Port    VLAN    IP Address          IP Mask
-------     ----    ----    ---------------     ---------------
```

Security Network IP Source Guard Mode

Description:

Set or show IP source guard mode.

Syntax:

Security Network IP Source Guard Mode [enable|disable]

Parameters:

enable : Enable IP Source Guard

disable: Disable IP Source Guard

Default Setting:

disable

Example:

Enable IP source guard mode

```
SWITCH/>security network ip source guard mode enable
```

Security Network IP Source Guard Limit

Description:

Set or show the IP Source Guard port limitation for dynamic entries.

Syntax:

Security Network IP Source Guard limit [<port_list>] [<dynamic_entry_limit>|unlimited]

Parameters:

<port_list> : Port list or 'all', default: All ports

<dynamic_entry_limit>|unlimited: dynamic entry limit (0-2) or unlimited

Default Setting:

unlimited

Example:

Set IP source guard limit

```
SWITCH/>security network ip source guard 1 1
```

Security Network IP Source Guard Entry

Description:

Add or delete IP source guard static entry.

Syntax:

Security Network IP Source Guard Entry [<port_list>] add|delete <vid> <allowed_ip> <ip_mask>

Parameters:

<port_list> : Port list or 'all', default: All ports

add : Add new port IP source guard static entry

delete : Delete existing port IP source guard static entry

<vid> : VLAN ID (1-4095)

<allowed_ip>: IP address (a.b.c.d), IP address allowed for doing ARP request

<ip_mask> : IP mask (a.b.c.d), IP mask for allowed IP address

Example:

Add IP source guard static entry.

```
SWITCH/>security network ip source guard entry 1 add 1 192.168.0.20 255.255.255.0
```

Security Network IP Source Guard Status

Description:

Show IP source guard static and dynamic entries.

Syntax:

Security Network IP Source Guard Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show IP source guard static and dynamic entries.

```
SWITCH/>security network ip source guard status
```

Security Network ARP Inspection Configuration

Description:

Show ARP inspection configuration.

Syntax:

Security Network ARP Inspection Configuration

Example:

Show ARP inspection configuration.

```
SWITCH/>security network arp inspection configuration
```

Security Network ARP Inspection Mode

Description:

Set or show ARP inspection mode.

Syntax:

Security Network ARP Inspection Mode [enable|disable]

Parameters:

enable : Enable ARP Inspection

disable: Disable ARP Inspection

Default Setting:

disable

Example:

Enable ARP inspection mode

```
SWITCH/>security network arp inspection mode enable
```

Security Network ARP Inspection Port Mode

Description:

Set or show the ARP Inspection port mode.

Syntax:

Security Network ARP Inspection Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable ARP Inspection port

disable : Disable ARP Inspection port

(default: Show ARP Inspection port mode)

Default Setting:

Disable

Example:

Enable the ARP inspection mode of port 1

```
SWITCH/>security network arp inspection port mode 1
```

Security Network ARP Inspection Entry

Description:

Add or delete ARP inspection static entry.

Syntax:

Security Network ARP Inspection Entry [<port_list>] add|delete <vid> <allowed_mac> <allowed_ip>

Parameters:

<port_list> : Port list or 'all', default: All ports

add : Add new port ARP inspection static entry

delete : Delete existing port ARP inspection static entry

<vid> : VLAN ID (1-4095)

<allowed_mac>: MAC address (xx-xx-xx-xx-xx-xx), MAC address allowed for doing ARP request

<allowed_ip> : IP address (a.b.c.d), IP address allowed for doing ARP request

Default Setting:

300

Example:

Add ARP inspection static entry.

```
SWITCH/>security network arp inspection entry 1 add 1 00-30-4f-00-00-11 192.168.0.11
```

Security Network ARP Inspection Status

Description:

Show ARP inspection static and dynamic entries.

Syntax:

Security Network ARP Inspection Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show ARP inspection static and dynamic entries.

```
SWITCH/>security network arp inspection status
```

Security AAA Configuration

Description:

Show Auth configuration.

Syntax:

Security AAA Configuration

Example:

Show Auth configuration.

```
SWITCH/>security aaa configuration

AAA Configuration:
==================



Server Timeout     : 15 seconds

Server Dead Time : 300 seconds

RADIUS Authentication Server Configuration:
=========================================
Server   Mode         IP Address          Secret                          Port
------       --------       ---------------          ------------------------------          -----
1          Disabled                                                                  1812
2          Disabled                                                                  1812
3          Disabled                                                                  1812
4          Disabled                                                                  1812
5          Disabled                                                                  1812

RADIUS Accounting Server Configuration:
=====================================
```

```
Server   Mode        IP Address         Secret                          Port
------   --------    ---------------    -----------------------------   -----
1        Disabled                                                       1813
2        Disabled                                                       1813
3        Disabled                                                       1813
4        Disabled                                                       1813
5        Disabled                                                       1813

TACACS+ Authentication Server Configuration:
==========================================
Server   Mode        IP Address         Secret                          Port
------   --------    ---------------    -----------------------------   -----
1        Disabled                                                       49
2        Disabled                                                       49
3        Disabled                                                       49
4        Disabled                                                       49
5        Disabled                                                       49
```

Security AAA Timeout

Description:

Set or show server timeout.

Syntax:

Security AAA Timeout [<timeout>]

Parameters:

<timeout>: Server response timeout (3-3600 seconds)

(default: Show server timeout configuration)

Default Setting:

15

Example:

Set 30sec for server timeout

```
SWITCH/>security aaa timeout 30
```

Security AAA Deadtime

Description:

Set or show server dead time.

Syntax:

Security AAA Deadtime [<dead_time>]

Parameters:

<dead_time>: Time that a server is considered dead if it doesn't answer a request (0-3600 seconds)

(default: Show server dead time configuration)

Default Setting:

300

Example:

Set 1000sec for server dead time

```
SWITCH/>security aaa deadtime 1000
```

Security AAA RADIUS

Description:

Set or show RADIUS authentication server setup.

Syntax:

Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)

(default: Show RADIUS authentication server configuration)

enable : Enable RADIUS authentication server

disable : Disable RADIUS authentication server

(default: Show RADIUS server mode)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

<secret> : Secret shared with external authentication server.
To set an empty secret, use two quotes ("").
To use spaces in secret, enquote the secret.
Quotes in the secret are not allowed.

<server_port> : Server UDP port. Use 0 to use the default RADIUS port (1812)

Example:

Set RADIUS authentication server configuration.

```
SWITCH/>security aaa radius 1 enable 192.168.0.20 12345678 1812
```

Security AAA ACCT_RADIUS

Description:

Set or show RADIUS accounting server setup.

Syntax:

Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)

(default: Show RADIUS accounting server configuration)

enable : Enable RADIUS accounting server

disable : Disable RADIUS accounting server

(default: Show RADIUS server mode)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

<secret> : Secret shared with external accounting server.

To set an empty secret, use two quotes ("").

To use spaces in secret, enquote the secret.

Quotes in the secret are not allowed.

<server_port> : Server UDP port. Use 0 to use the default RADIUS port (1813)

Example:

Set RADIUS accounting server configuration.

```
SWITCH/>security acct_radius 1 enable 192.168.0.20 12345678 1813
```

Security AAA TACACS+

Description:

Set or show TACACS+ authentication server setup.

Syntax:

Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)

(default: Show TACACS+ authentication server configuration)

enable : Enable TACACS+ authentication server

disable : Disable TACACS+ authentication server

(default: Show TACACS+ server mode)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

<secret> : Secret shared with external authentication server.

To set an empty secret, use two quotes ("").

To use spaces in secret, enquote the secret.

Quotes in the secret are not allowed.

<server_port> : Server TCP port. Use 0 to use the default TACACS+ port (49)

Example:

Set TACACS+ authentication server configuration.

```
SWITCH/>security aaa tacacs+ 1 enable 192.168.0.20 12345678 49
```

Security AAA Statistics

Description:

Show RADIUS statistics.

Syntax:

Security AAA Statistics [<server_index>]

Parameters:

The server index (1-5)

(default: Show statistics for all servers)

Example:

Show RADIUS statistics.

```
SWITCH/>security aaa statistics
```

6.8 Spanning Tree Protocol Command

STP Configuration

Description:

Show STP configuration.

Syntax:

STP Configuration

Example:

Show STP configuration.

```
SWITCH/>stp cofiguration

STP Configuration:
==================

Protocol Version: MSTP
Max Age              : 20
Forward Delay    : 15
Tx Hold Count    : 6
Max Hop Count    : 20
```

STP Version

Description:

Set or show the STP Bridge protocol version.

Syntax:

STP Version [<stp_version>]

Parameters:

<stp_version>: mstp|rstp|stp

Default Setting:

MSTP

Example:

Set the STP Bridge protocol version.

```
SWITCH/> stp version rstp
```

STP Tx Hold

Description:

Set or show the STP Bridge Transmit Hold Count parameter.

Syntax:

STP Txhold [<holdcount>]

Parameters:

<holdcount>: STP Transmit Hold Count (1-10)

Default Setting:

6

Example:

Set STP Tx hold in 10

```
SWITCH/>stp txhold 5
```

STP MaxHops

Description:

Set or show the MSTP Bridge Max Hop Count parameter.

Syntax:

STP MaxHops [<maxhops>]

Parameters:

<maxhops>: STP BPDU MaxHops (6-40))

Default Setting:

20

Example:

Set STP maximum hops in 25

```
SWITCH/>stp maxhops 25
```

STP MaxAge

Description:

Set or show the CIST/MSTI bridge maximum age.

Syntax:

STP MaxAge [<max_age>]

Parameters:

<max_age>: STP maximum age time (6-40, and max_age <= (forward_delay-1)*2)

Default Setting:

20

Example:

Set STP maximum age time in 10

```
SWITCH/>stp maxage 10
```

STP FwdDelay

Description:

Set or show the CIST/MSTI bridge forward delay.

Syntax:

STP FwdDelay [<delay>]

Parameters:

<delay>: MSTP forward delay (4-30, and max_age <= (forward_delay-1)*2))

Default Setting:

15

Example:

Set STP forward delay value in 25

```
SWITCH/>stp fwddelay 25
```

STP CName

Description:

Set or Show MSTP configuration name and revision.

Syntax:

STP CName [<config-name>] [<integer>]

Parameters:

<config-name>: MSTP Configuration name. A text string up to 32 characters long.

Use quotes (") to embed spaces in name.

<integer> : Integer value

Default Setting:

Configuration name: MAC address

Configuration rev.: 0

Example:

Set MSTP configuration name and revision.

```
SWITCH/>stp cname 9f_WGSW-24040 1
```

STP bpdeFilter

Description:

Set or show edge port BPDU Filtering.

Syntax:

STP bpduFilter [enable|disable]

Parameters:

enable|disable: enable or disable BPDU Filtering for Edge ports

Default Setting:

Disable

Example:

Set edge port BPDU filtering

```
SWITCH/>stp bpdufilter enable
```

STP bpduGuard

Description:

Set or show edge port BPDU Guard.

Syntax:

STP bpduGuard [enable|disable]

Parameters:

enable|disable: enable or disable BPDU Guard for Edge ports

Default Setting:

Disable

Example:

Set edge port BPDU guard

```
SWITCH/>stp bpduguard enable
```

STP Recovery

Description:

Set or show edge port error recovery timeout.

Syntax:

STP recovery [<timeout>]

Parameters:

<timeout>: Time before error-disabled ports are reenabled (30-86400 seconds, 0 disables)

(default: Show recovery timeout)

Default Setting:

Disable

Example:

Set STP recovery value in 30 sec.

```
SWITCH/>stp recovery 30
```

STP Status

Description:

Show STP Bridge status.

Syntax:

STP Status [<msti>] [<port_list>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<port_list>: Port list or 'all', default: All ports

Default Setting:

Disable

Example:

Show STP Bridge status.

```
SWITCH/>stp status
CIST Bridge STP Status
Bridge ID      : 80:00-00:30:4F:24:04:D1
Root ID        : 80:00-00:30:4F:24:04:D1
Root Port      : -
Root PathCost: 0
Regional Root: 80:00-00:30:4F:24:04:D1
Int. PathCost: 0
Max Hops       : 20
TC Flag        : Steady
TC Count       : 0
TC Last        : -
Port         Port Role         State         Pri   PathCost   Edge   P2P   Uptime
---------    ---------------   -----------   ---   --------   ----   ---   -------------
14         DesignatedPort   Forwarding   128   20000       Yes    Yes   0d 00:10:32
```

STP MSTI Priority

Description:

Set or show the CIST/MSTI bridge priority.

Syntax:

STP Msti Priority [<msti>] [<priority>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<priority> : STP bridge priority (0/16/32/48/.../224/240)

Default:

MSTI	Bridge Priority
CIST	128
MST1	128
MST2	128
MST3	128
MST4	128
MST5	128
MST6	128
MST7	128

Example:

Set MST1 priority value in 48.

```
SWITCH/>stp msti priority 1 48
```

STP MSTI Map

Description:

Show or clear MSTP MSTI VLAN mapping configuration.

Syntax:

STP Msti Map [<msti>] [clear]

Parameters:

<msti>: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

Clear : Clear VID to MSTI mapping

Example:

Add MST1 priority value in 48.

```
SWITCH/>stp msti priority 1 48
```

STP MSTI Add

Description:

Add a VLAN to a MSTI.

Syntax:

STP Msti Add <msti> <vid>

Parameters:

<msti>: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<vid> : VLAN ID (1-4095)

Example:

Add MST1 in vlan1.

```
SWITCH/>stp msti add 1 1
```

STP Port Configuration

Description:

Show STP Port configuration.

Syntax:

STP Port Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

Example:

Show STP status of Port1

```
SWITCH/>stp port configuration 1

Port   Mode       AdminEdge   AutoEdge    restrRole   restrTcn    bpduGuard   Point2point
----   --------   ---------   ---------   ---------   ---------   ---------   -----------
1      Enabled    Enabled     Enabled     Disabled    Disabled    Disabled    Auto
```

STP Port Mode

Description:

Set or show the STP enabling for a port.

Syntax:

STP Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

Enable : Enable MSTP protocol

Disable : Disable MSTP protocol

Default:

Enable

Example:

Disable STP function on port1

```
SWITCH/>stp port mode 1 disable
```

STP Port Edge

Description:

Set or show the STP adminEdge port parameter.

Syntax:

STP Port Edge [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

Enable : Configure MSTP adminEdge to Edge

Disable : Configure MSTP adminEdge to Non-edge

Default:

Enable

Example:

Disable STP edge function on port1

```
SWITCH/>stp port edge 1 disable
```

STP Port AutoEdge

Description:

Set or show the STP autoEdge port parameter.

Syntax:

STP Port AutoEdge [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

Enable : Enable MSTP autoEdge

Disable : Disable MSTP autoEdge

Default:

enable

Example:

Disable STP edge function on port1

```
SWITCH/>stp port autoedge 1 disable
```

STP Port P2P

Description:

Set or show the STP point2point port parameter.

Syntax:

STP Port P2P [<port_list>] [enable|disable|auto]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable MSTP point2point

disable : Disable MSTP point2point

auto : Automatic MSTP point2point detection

Default:

auto

Example:

Disable STP P2P function on port1

```
SWITCH/>stp port p2p 1 disable
```

STP Port RestrictedRole

Description:

Set or show the MSTP restrictedRole port parameter.

Syntax:

STP Port RestrictedRole [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable MSTP restricted role

disable : Disable MSTP restricted role

Default:

disable

Example:

Eisable STP restricted role on port1

```
SWITCH/>stp port restrictedrole 1 enable
```

STP Port RestrictedTcn

Description:

Set or show the MSTP restrictedTcn port parameter.

Syntax:

STP Port RestrictedTcn [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable MSTP restricted TCN

disable : Disable MSTP restricted TCN

Default:

disable

Example:

Eisable STP restricted TCN on port1

```
SWITCH/>stp port restrictedtcn 1 enable
```

STP Port bpduGuard

Description:

Set or show the bpduGuard port parameter.

Syntax:

STP Port bpduGuard [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port BPDU Guard

disable : Disable port BPDU Guard

Default:

disable

Example:

Eisable BPDU guard on port1

```
SWITCH/>stp port bpduguard 1 enable
```

STP Port Statistic

Description:

Show STP port statistics.

Syntax:

STP Port Statistics [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show STP port statistics.

```
SWITCH/>stp port statistics
Port Rx MSTP Tx MSTP Rx RSTP Tx RSTP Rx STP Tx STP Rx TCN Tx TCN Rx Ill. Rx Unk.
---- -------- -------- -------- -------- ------- ------- ------- ------- ------- -------
14        0      579        0        0       0       0       0       0       0       0
```

STP Port Mcheck

Description:

Set the STP mCheck (Migration Check) variable for ports.

Syntax:

STP Port Mcheck [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Set the STP mCheck (Migration Check) variable for port 1.

```
SWITCH/>stp port mcheck 1
```

STP Msti Port Configuration

Description:

Show the STP CIST/MSTI port configuration.

Syntax:

STP Msti Port Configuration [<msti>] [<port_list>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<port_list>: Port list or 'all', default: All ports

Default:

auto

Example:

Set MSTI2 in port1~2

```
SWITCH/>stp msti port configuration 2 1-2

MSTI   Port    Path Cost    Priority
----    ----   ----------    --------
MST2   Aggr   Auto          128

MSTI   Port   Path Cost    Priority
----    ----  ----------   --------
MST2    1     Auto         128
MST2    2     Auto         128
```

STP Msti Port Cost

Description:

Set or show the STP CIST/MSTI port path cost.

Syntax:

STP Msti Port Cost [<msti>] [<port_list>] [<path_cost>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<port_list> : Port list or 'all'. Port zero means aggregations.

<path_cost> : STP port path cost (1-200000000) or 'auto'

Default:

auto

Example:

Set MSTI7 in port1

```
SWITCH/>stp msti port cost 7 1

MSTI   Port   Path Cost
----    ----  ----------
```

MST7	**1**	**Auto**

STP Msti Port Priority

Description:

Set or show the STP CIST/MSTI port priority.

Syntax:

STP Msti Port Priority [<msti>] [<port_list>] [<priority>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<port_list> : Port list or 'all'. Port zero means aggregations.

<priority> : STP port priority (0/16/32/48/.../224/240)

Default:

128

6.9 Multicast Configuration Command

IGMP Configuration

Description:

Show IGMP snooping configuration.

Syntax:

IGMP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show IGMP snooping configuration.

```
SWITCH/>igmp configuration
```

IGMP Mode

Description:

Set or show the IGMP snooping mode.

Syntax:

IGMP Mode [enable|disable]

Parameters:

enable : Enable IGMP snooping

disable: Disable IGMP snooping

(default: Show IGMP snooping mode)

Default Setting:

Disabled

Example:

Enable IGMP mode

```
SWITCH/>igmp mode enable
```

IGMP Leave Proxy

Description:

Set or show the mode of IGMP Leave Proxy.

Syntax:

IGMP Leave Proxy [enable|disable]

Parameters:

enable : Enable IGMP Leave Proxy

disable: Disable IGMP Leave Proxy

(default: Show IGMP snooping mode)

Default Setting:

disable

Example:

Enable IGMP leave proxy

```
SWITCH/>igmp leave proxy enable
```

IGMP State

Description:

Set or show the IGMP snooping state for VLAN.

Syntax:

IGMP State [<vid>] [enable|disable]

Parameters:

<vid>: VLAN ID (1-4095), default: Show all VLANs

enable : Enable IGMP snooping

disable: Disable IGMP snooping

(default: Show IGMP snooping mode)

Default Setting:

enable

Example:

Disable VID 1

```
SWITCH/>igmp state 1 disable
```

IGMP Querier

Description:

Set or show the IGMP snooping querier mode for VLAN.

Syntax:

IGMP Querier [<vid>] [enable|disable]

Parameters:

<vid>: VLAN ID (1-4095), default: Show all VLANs

enable : Enable IGMP querier

disable : Disable IGMP querier

(default: Show IGMP querier mode)

Default Setting:

disable

Example:

Enable the IGMP snooping querier mode for VLAN.

```
SWITCH/>igmp querier 1 enable
```

IGMP Fastleave

Description:

Set or show the IGMP snooping fast leave port mode.

Syntax:

IGMP Fastleave [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable IGMP fast leave

disable : Disable IGMP fast leave

(default: Show IGMP fast leave mode)

Default Setting:

disable

Example:

Enable the IGMP snooping fast leave port mode.

```
SWITCH/>igmp fastleave 1 enable
```

IGMP Throttling

Description:

Set or show the IGMP port throttling status.

Syntax:

IGMP Throttling [<port_list>] [limit-group-number]

Parameters:

<port_list>: Port list or 'all', default: All ports

0 : No limit

1~10 : Group learn limit

(default: Show IGMP Port Throttling)

Default Setting:

unlimited

Example:

Set the IGMP port throttling status for port 1.

```
SWITCH/>igmp throttling 1 10
```

IGMP Filtering

Description:

Set or show the IGMP port group filtering list.

Syntax:

IGMP Filtering [<port_list>] [add|del] [group_addr]

Parameters:

<port_list>: Port list or 'all', default: All ports

add : Add new port group filtering entry

del : Del existing port group filtering entry

(default: Show IGMP port group filtering list)

IP multicast group address (a.b.c.d)

Default Setting:

No filtering

Example:

Set the IGMP port group filtering list for port 1.

```
SWITCH/>igmp filtering 1 add 239.0.0.1
```

IGMP Router

Description:

Set or show the IGMP snooping router port mode.

Syntax:

IGMP Router [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable IGMP router port

disable : Disable IGMP router port

(default: Show IGMP router port mode)

Default Setting:

disable

Example:

Enable IGMP snooping function for port1~4

```
SWITCH/>igmp router 1-4 enable
```

IGMP Flooding

Description:

Set or show the IGMP snooping unregistered flood operation.

Syntax:

IGMP Flooding [enable|disable]

Parameters:

enable : Enable IGMP flooding

disable: Disable IGMP flooding

(default: Show IGMP flood mode)

Default Setting:

disable

Example:

Enable IGMP flooding function

```
SWITCH/>igmp flooding enable
```

IGMP Groups

Description:

Show IGMP groups.

Syntax:

IGMP Groups [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

IGMP Status

Description:

Show IGMP status.

Syntax:

IGMP Status [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

Default Setting:

disable

6.10 Link Aggregation Command

Aggregation Configuration

Description:

Show link aggregation configuration.

Syntax:

Aggr Configuration

Example:

```
SWITCH/>aggr configuration
Aggregation Mode:

SMAC   : Enabled
DMAC   : Disabled
IP     : Enabled
Port   : Enabled
```

Aggregation Add

Description:

Add or modify link aggregation.

Syntax:

Aggr Add <port_list> [<aggr_id>]

Parameters:

<port_list>: Port list

<aggr_id> : Aggregation ID, global: 1-2, local: 3-14

Default Setting:

disable

Example:

Add port 1~4 in Group1

```
SWITCH/>aggr add 1-4 1
```

Aggregation Delete

Description:

Delete link aggregation.

Syntax:

Aggr Delete <aggr_id>

Parameters:

<aggr_id>: Aggregation ID

Example:

Delete Group2

```
SWITCH/>aggr delete 2
```

Aggregation Lookup

Description:

Lookup link aggregation.

Syntax:

Aggr Lookup [<aggr_id>]

Parameters:

<aggr_id>: Aggregation ID

Example:

Show aggregation status

```
SWITCH/>aggr lookup 1

Aggr ID   Name      Type      Ports
----------- -------  -------  -------
1          GLAG1    Static     1-4
```

Aggregation Mode

Description:

Set or show the link aggregation traffic distribution mode.

Syntax:

Aggr Mode [smac|dmac|ip|port] [enable|disable]

Parameters:

smac : Source MAC address

dmac : Destination MAC address

ip : Source and destination IP address

port : Source and destination UDP/TCP port

enable : Enable field in traffic distribution

disable: Disable field in traffic distribution

Default Setting:

SMAC : Enabled

DMAC : Disabled

IP : Enabled

Port : Enabled

Example:

Disable SMAC mode

```
SWITCH/>Aggr mode smac disable
```

6.11 Link Aggregation Control Protocol Command

LACP Configuration

Description:

Show LACP configuration.

Syntax:

LACP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LACP configuration

```
SWITCH/>lacp configuration

Port   Mode       Key    Role
----   --------   ----   ------
1      Disabled   Auto   Active
2      Disabled   Auto   Active
3      Disabled   Auto   Active
4      Disabled   Auto   Active
5      Disabled   Auto   Active
6      Disabled   Auto   Active
7      Disabled   Auto   Active
8      Disabled   Auto   Active
9      Disabled   Auto   Active
10     Disabled   Auto   Active
11     Disabled   Auto   Active
12     Disabled   Auto   Active
13     Disabled   Auto   Active
14     Disabled   Auto   Active
15     Disabled   Auto   Active
16     Disabled   Auto   Active
17     Disabled   Auto   Active
18     Disabled   Auto   Active
19     Disabled   Auto   Active
20     Disabled   Auto   Active
21     Disabled   Auto   Active
```

```
22      Disabled    Auto    Active
23      Disabled    Auto    Active
24      Disabled    Auto    Active
```

LACP Mode

Description:

Set or show LACP mode.

Syntax:

LACP Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable LACP protocol

disable: Disable LACP protocol

(default: Show LACP mode)

Default Setting:

disable

Example:

Enable LACP for port1~4

```
SWITCH/>lacp mode 1-4 enable
```

LACP Key

Description:

Set or show the LACP key.

Syntax:

LACP Key [<port_list>] [<key>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<key> : LACP key (1-65535) or 'auto'

Default Setting:

auto

Example:

Set key1 for port1~4

```
SWITCH/>lacp key 1-4 1
```

LACP Role

Description:

Set or show the LACP role.

Syntax:

LACP Role [<port_list>] [active|passive]

Parameters:

<port_list>: Port list or 'all', default: All ports

active : Initiate LACP negotiation

passive: Listen for LACP packets

(default: Show LACP role)

Default Setting:

active

Example:

Set passive for port1~4

```
SWITCH/>lacp role 1-4 passive
```

LACP Status

Description:

Show LACP Status.

Syntax:

LACP Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LACP status of port1~4

```
SWITCH/>status 1-4

Port   Mode        Key     Aggr ID   Partner System ID   Partner Port
----   --------    -----   -------   -----------------   ------------
1      Disabled    1       -         -                   -
2      Disabled    1       -         -                   -
3      Disabled    1       -         -                   -
4      Disabled    1       -         -                   -
```

LACP Statistics

Description:

Show LACP Statistics.

Syntax:

LACP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear **:** Clear LACP statistics

Example:

Show LACP statistics of port1~4

```
SWITCH/>lacp statistics 1-4

Port   Rx Frames     Tx Frames     Rx Unknown    Rx Illegal
------ ------------- ------------- ------------- ----------
1      0             0             0             0
2      0             0             0             0
3      0             0             0             0
4      0             0             0             0
```

6.12 LLDP Command

LLDP Configuration

Description:

Show LLDP configuration.

Syntax:

LLDP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LLDP configuration of port1~4

```
SWITCH/>lldp configuration 1-4

LLDP Configuration:
===================

Interval      : 30
Hold          : 3
Tx Delay      : 2
Reinit Delay: 2

Port Mode       Port Descr System Name System Descr System Capa Mgmt Addr CDP awareness
---- --------   ---------- ----------- ------------ ------------ --------- -------------
1    Enabled    Enabled    Enabled     Enabled      Enabled      Enabled   Disabled
2    Enabled    Enabled    Enabled     Enabled      Enabled      Enabled   Disabled
3    Enabled    Enabled    Enabled     Enabled      Enabled      Enabled   Disabled
4    Enabled    Enabled    Enabled     Enabled      Enabled      Enabled   Disabled
```

LLDP Mode

Description:

Set or show LLDP mode.

Syntax:

LLDP Mode [<port_list>] [enable|disable|rx|tx]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable LLDP reception and transmission

disable: Disable LLDP

rx : Enable LLDP reception only

tx : Enable LLDP transmission only

(default: Show LLDP mode)

Default Setting:

disable

Example:

Enable port1 LLDP function.

```
SWITCH/>lldp mode 1 enable
```

LLDP Optional TLV

Description:

Show or Set LLDP Optional TLVs.

Syntax:

LLDP Optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

port_descr : Description of the port

sysm_name : System name

sys_descr : Description of the system

sys_capa : System capabilities

mgmt_addr : Master's IP address

(default: Show optional TLV's configuration)

enable : Enables TLV

disable : Disable TLV

(default: Show optional TLV's configuration)

Default Setting:

Description of the port: Enable

System name: Enable

Description of the system: Enable

System capabilities: Enable

Master's IP address: Enable

Example:

Disable description of the port for port1

```
SWITCH/>lldp optional_tlv 1 port_descr disable
```

LLDP Interval

Description:

Set or show LLDP Tx interval.

Syntax:

LLDP Interval [<interval>]

Parameters:

<interval>: LLDP transmission interval (5-32768)

Default Setting:

30

Example:

Set transmission interval in 10

```
SWITCH/>lldp interval 10
```

LLDP Hold

Description:

Set or show LLDP Tx hold value.

Syntax:

LLDP Hold [<hold>]

Parameters:

<hold>: LLDP hold value (2-10)

Default Setting:

3

Example:

Set LLDP hold value in 10

```
SWITCH/>lldp hold 10
```

LLDP Delay

Description:

Set or show LLDP Tx delay.

Syntax:

LLDP Delay [<delay>]

Parameters:

<delay>: LLDP transmission delay (1-8192)

Default Setting:

2

Example:

Set LLDP delay value in 1

```
SWITCH/>lldp delay 1
```

LLDP Reinit

Description:

Set or show LLDP reinit delay.

Syntax:

LLDP Reinit [<reinit>]

Parameters:

<reinit>: LLDP reinit delay (1-10)

Default Setting:

2

Example:

Set LLDP reinit delay value in 3

```
SWITCH/>lldp reinit 3
```

LLDP Statistics

Description:

Show LLDP Statistics.

Syntax:

LLDP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear LLDP statistics

Example:

Show LLDP Statistics of port 1

```
SWITCH/>lldp statistics 1

LLDP global counters
Neighbor entries was last changed at - (323592 sec. ago).
Total Neighbors Entries Added      0.
Total Neighbors Entries Deleted    0.
Total Neighbors Entries Dropped    0.
Total Neighbors Entries Aged Out 0.

LLDP local counters
        Rx         Tx         Rx         Rx         Rx TLV    Rx TLV    Rx TLV
Port    Frames     Frames     Errors     Discards   Errors    Unknown   Organz.   Aged
----    ------     ------     ------     --------   ------    -------   -------   -----
1       0          0          0          0          0         0         0         0
```

LLDP Info

Description:

Show LLDP neighbor device information.

Syntax:

LLDP Info [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

6.13 LLDPMED Command

LLDPMED Configuration

Description:

Show LLDP-MED configuration.

Syntax:

LLDPMED Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LLDP-MED configuration of port1~4

```
SWITCH/>lldpmed configuration 1-4

LLDP-MED Configuration:
=======================

Fast Start Repeast Count : 4
Location Coordinates      : Latitude          - 0.0000 North
                            Longitude         - 0.0000 East
                            Altitude          - 0.0000 meter(s)
                            Map datum         - WGS84
Civic Address Location    :


Port        Policies
1           none
2           none
3           none
4           none
```

LLDPMED Civic

Description:

Set or show LLDP-MED Civic Address Location.

Syntax:

LLDPMED Civic

[country|state|county|city|district|block|street|leading_street_direction|trailing_street_suffix|str_suf|house_no|house_no_suffix|landmark|additional_info|name|zip_code|building|apartment|floor|room_number|place_type|postal_com_name|p_o_box|additional_code] [<civic_value>]

Parameters:

country : Country

state : National subdivisions (state, caton, region, province, prefecture)

county : County, parish,gun (JP), district(IN)

city : City, townchip, shi (JP)

district : City division,borough, city, district, ward,chou (JP)

block : Neighborhood, block

street : Street

leading_street_direction : Leading street direction

trailing_street_suffix : Trailing street suffix

str_suf : Street Suffix

house_no : House Number

house_no_suffix : House number suffix

landmark : Landmark or vanity address

additional_info : Additional location information

name : Bame(residence and office occupant)

zip_code : Postal/zip code

building : Building (structure)

apartment : Unit (apartment, suite)

floor : Floor

room_number : Room number

place_type : Placetype

postal_com_name : Postal community name

p_o_box : Post office box (P.O. Box)

additional_code : Addtional code

(default: Show Civic Address Location configuration)

<civic_value>: lldpmed The value for the Civic Address Location entry.

LLDPMED ECS

Description:

Set or show LLDP-MED Emergency Call Service.

Syntax:

LLDPMED ecs [<ecs_value>]

Parameters:

<ecs_value>: lldpmed The value for the Emergency Call Service

LLDPMED Policy Delete

Description:

Delete the selected policy.

Syntax:

LLDPMED policy delete [<policy_list>]

Parameters:

<policy_list>: List of policies to delete

Example:

Delete the policy 1

```
SWITCH/>lldpmed policy delete 1
```

LLDPMED Policy Add

Description:

Adds a policy to the list of polices.

Syntax:

LLDPMED policy add [voice|voice_signaling|guest_voice|guest_voice_signaling|softphone_voice|video_conferencing|streaming_video|video_signaling] [tagged|untagged] [<vlan_id>] [<l2_priority>] [<dscp>]

Parameters:

voice : Voice for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications

voice_signaling : Voice Signaling (conditional) for use in network topologies that require a different policy for the voice signaling than for the voice media.

guest_voice : Guest Voice to support a separate limited feature-set voice service for guest users and

visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

guest_voice_signaling : Guest Voice Signaling (conditional) for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.

softphone_voice : Softphone Voice for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all,and are typically configured to use an untagged VLAN or a single tagged data specific VLAN.

video_conferencing : Video Conferencing for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

streaming_video : Streaming Video for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

video_signaling : Video Signaling (conditional) for use in network topologies that require a separate policy for the video signaling than for the video media.

tagged : The device is using tagged frames

unragged : The device is using untagged frames

<vlan_id> : VLAN id

<l2_priority>: This field may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004 [3].

<dscp> : This field shall contain the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474 [5]. This 6 bit field may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

LLDPMED Port Policy

Description:

Set or show LLDP-MED port polcies.

Syntax:

LLDPMED port policies [<port_list>] [<policy_list>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<policy_list>: List of policies to delete

LLDPMED Coordinates

Description:

Set or show LLDP-MED Location.

Syntax:

LLDPMED Coordinates [latitude|longitude|altitude] [north|south|west|east|meters|floor] [coordinate_value]

Parameters:

latitude : Latitude, 0 to 90 degress with max. 4 digits (Positive numbers are north of the equator and negative numbers are south of the equator).

longitude : Longitude,0 to 180 degress with max. 4 digits (Positive values are East of the prime meridian and negative numbers are West of the prime meridian.

altitude : Altitude, Meters or floors with max. 4 digits.

(default: Show coordinate location configuration)

north|south|west|east|meters|floor:

North : North (Valid for latitude)

South : South (Valid for latitude)

West : West (Valid for longitude)

East : East (Valid for longitude)

Meters : Meters (Valid for altitude)

Floor : Floor (Valid for altitude)

lldpmed Coordinate value

coordinate_value : lldpmed Coordinate value

LLDPMED Datum

Description:

Set or show LLDP-MED Coordinates map datum.

Syntax:

LLDPMED Datum [wgs84|nad83_navd88|nad83_mllw]

Parameters:

wgs84|nad83_navd88|nad83_mllw:

wgs84 : WGS84

nad83_navd88 : NAD83_NAVD88

nad83_mllw : NAD83_MLLW

lldpmed Coordinate datum

LLDPMED Fast

Description:

Set or show LLDP-MED Fast Start Repeat Count.

Syntax:

LLDPMED Fast [<count>]

Parameters:

<count>: The number of times the fast start LLDPDU are being sent during the activation of the fast start mechanism defined by LLDP-MED (1-10).

LLDPMED Info

Description:

Show LLDP-MED neighbor device information.

Syntax:

LLDPMED Info [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

LLDPMED Debuge_med_transmit_var

Description:

Set or show if the current value of the global medTansmitEnable variable (Section Section 11.2.1, TIA 1057).

Syntax:

LLDPMED debug_med_transmit_var [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable - Set medTansmitEnable variable to true

disable: Disable - Set medTansmitEnable variable to false

(default: Show medTansmitEnable variable value)

6.14 Quality of Service Command

QoS Configuration

Description:

Show QoS Configuration.

Syntax:

QoS Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show QoS Configuration of port 1-4.

```
SWITCH/>qos configuration 1-4

QoS Configuration:
==================

Traffic Classes: 4

Storm Multicast: Disabled        1 pps
Storm Broadcast: Disabled        1 pps
Storm Unicast   : Disabled       1 pps

Port   Default   Tag Priority   QCL ID   Rate Limiter       Shaper       Mode     Weight
----   -------   ------------   ------   ------------       ---------    --------  ------
1      Low       0              1        Disabled           Disabled     Strict   1/2/4/8
2      Low       0              1        Disabled           Disabled     Strict   1/2/4/8
3      Low       0              1        Disabled           Disabled     Strict   1/2/4/8
4      Low       0              1        Disabled           Disabled     Strict   1/2/4/8
```

QoS Classes

Description:

Set or show the number of traffic classes.

Syntax:

QoS Classes [<class>]

Parameters:

<class>: Number of traffic classes (1,2 or 4)

Default Setting:

4

Example:

Set QoS classes 2

```
SWITCH/>qos classes 2
```

QoS Default

Description:

Set or show the default port priority.

Syntax:

QoS Default [<port_list>] [<class>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<class> : Traffic class low/normal/medium/high or 1/2/3/4

Default Setting:

Low

Example:

Set high priority for port5

```
SWITCH/>qos default 5 high
```

QoS Tagprio

Description:

Set or show the port VLAN tag priority.

Syntax:

QoS Tagprio [<port_list>] [<tag_prio>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<tag_prio> : VLAN tag priority (0-7)

Default Setting:

0

Example:

Set priority7 for port 3

```
SWITCH/>qos tagprio 3 7
```

QoS QCL Port

Description:

Set or show the port QCL ID.

Syntax:

QoS QCL Port [<port_list>] [<qcl_id>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<qcl_id> : QCL ID

Default Setting:

1

Example:

Set QCL ID5 for port10

```
SWITCH/>qos qcl port 10 5
```

QoS QCL Add

Description:

Add or modify QoS Control Entry (QCE).

If the QCE ID parameter <qce_id> is specified and an entry with this QCE ID already exists, the QCE will be modified. Otherwise, a new QCE will be added. If the QCE ID is not specified, the next available QCE ID will be used.

If the next QCE ID parameter <qce_id_next> is specified, the QCE will be placed before this QCE in the list. If the next QCE ID is not specified, the QCE will be placed last in the list.

Syntax:

QoS QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>]
(etype <etype>) |
(vid <vid>) |
(port <udp_tcp_port>) |
(dscp <dscp>) |
(tos <tos_list>) |
(tag_prio <tag_prio_list>)
<class>

Parameters:

<qcl_id> : QCL ID
<qce_id> : QCE ID (1-24)
<qce_id_next> : Next QCE ID (1-24)
etype : Ethernet Type keyword
<etype> : Ethernet Type
vid : VLAN ID keyword
<vid> : VLAN ID (1-4095)
port : UDP/TCP port keyword
<udp_tcp_port> : Source or destination UDP/TCP port (0-65535)
dscp : IP DSCP keyword
<dscp> : IP DSCP (0-63)
tos : IP ToS keyword
<tos_list> : IP ToS list (0-7)
tag_prio : VLAN tag priority keyword
<tag_prio_list>: VLAN tag priority list (0-7)
<class> : Traffic class low/normal/medium/high or 1/2/3/4

QoS QCL Delete

Description:

Delete QCE.

Syntax:

QoS QCL Delete <qcl_id> <qce_id>

Parameters:

<qcl_id>: QCL ID

<qce_id>: QCE ID (1-24)

QoS QCL Lookup

Description:

Lookup QCE.

Syntax:

QoS QCL Lookup [<qcl_id>] [<qce_id>]

Parameters:

<qcl_id>: QCL ID

<qce_id>: QCE ID (1-24)

QoS Mode

Description:

Set or show the port egress scheduler mode.

Syntax:

QoS Mode [<port_list>] [strict|weighted]

Parameters:

<port_list>: Port list or 'all', default: All ports

strict : Strict mode

weighted: Weighted mode

(default: Show QoS mode)

Default Setting:

Strict

Example:

Set weighted mode for port15

```
SWITCH/>qos mode 15 weighted
```

QoS Weight

Description:

Set or show the port egress scheduler weight.

Syntax:

QoS Weight [<port_list>] [<class>] [<weight>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<class> : Traffic class low/normal/medium/high or 1/2/3/4

<weight> : Traffic class weight 1/2/4/8

QoS Rate Limiter

Description:

Set or show the port rate limiter.

Syntax:

QoS Rate Limiter [<port_list>] [enable|disable] [<bit_rate>]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable rate limiter

disable : Disable rate limiter

(default: Show rate limiter mode)

<bit_rate> : Rate in 1000 bits per second (500-1000000 kbps)

Default Setting:

Disabled, 500kbps

Example:

Set 1000kbps rate limiter for port17~24

```
SWITCH/>qos rate limiter 17-24 enable 1000
```

QoS Shaper

Description:

Set or show the port shaper.

Syntax:

QoS Shaper [<port_list>] [enable|disable] [<bit_rate>]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable shaper

disable : Disable shaper

(default: Show shaper mode)

<bit_rate> : Rate in 1000 bits per second (500-1000000 kbps)

Default Setting:

Disabled, 500kbps

Example:

Set 1000kbps shaper for port 9~16

```
SWITCH/>qos shaper 9-16 enable 1000
```

QoS Storm Unicast

Description:

Set or show the unicast storm rate limiter.

Syntax:

QoS Storm Unicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable unicast storm control

disable : Disable unicast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable unicast storm rate limiter in 1kpps

```
SWITCH/>qos storm unicast enable 1k
```

QoS Strom Multicast

Description:

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Multicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable multicast storm control

disable : Disable multicast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable multicast storm rate limiter in 1kpps

```
SWITCH/>qos storm multicast enable 1k
```

QoS Strom Broadcast

Description:

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Broadcast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable broadcast storm control

disable : Disable broadcast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable broadcast storm rate limiter in 1kpps

```
SWITCH/>qos storm broadcast enable 1k
```

QoS DSCP Remarking

Description:

Set or show the status of QoS DSCP Remarking.

Syntax:

QoS DSCP Remarking [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable QoS Remarking

disable : Disable QoS Remarking

Default Setting:

Disabled

Example:

Enable the status of QoS DSCP Remarking for port 1-4

```
SWITCH/>qos dscp remarking 1-4 enable
```

QoS DSCP Queue Mapping

Description:

Set or show the default port priority.

Syntax:

QoS Default [<port_list>] [<class>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<class> : Traffic class low/normal/medium/high or 1/2/3/4

6.15 Mirror Command

Mirror Configuration

Description:

Show mirror configuration.

Syntax:

Mirror Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Default Setting:

disable

Example:

Show mirror configuration.

```
SWITCH/>mirror configuration
```

Mirror Port

Description:

Set or show the mirror port.

Syntax:

Mirror Port [<port>|disable]

Parameters:

<port>|disable: Mirror port or 'disable', default: Show port

Default Setting:

Mirror Port: 1

Example:

Set port 2 for the mirror port.

```
SWITCH/>mirror port 2
```

Mirror Mode

Description:

Set or show the mirror mode.

Syntax:

Mirror Mode [<port_list>] [enable|disable|rx|tx]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable Rx and Tx mirroring

disable: Disable Mirroring

rx : Enable Rx mirroring

tx : Enable Tx mirroring

(default: Show mirror mode)

Default Setting:

disable

Example:

Enable the mirror mode for port 1-4.

```
SWITCH/>mirror mode 1-4 enable
```

6.16 Configuration Command

Configuration Save

Description:

Save configuration to TFTP server.

Syntax:

Config Save <ip_server> <file_name>

Parameters:

<ip_server>: TFTP server IP address (a.b.c.d)

<file_name>: Configuration file name

Configuration Load

Description:

Load configuration from TFTP server.

Syntax:

Config Load <ip_server> <file_name> [check]

Parameters:

<ip_server>: TFTP server IP address (a.b.c.d)

<file_name>: Configuration file name

check : Check configuration file only, default: Check and apply file

6.17 Firmware Command

Firmware Load

Description:

Load new firmware from TFTP server.

Syntax:

Firmware Load <ip_addr_string> <file_name>

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

<file_name> : Firmware file name

Firmware IPv6 Load

Description:

Load new firmware from IPv6 TFTP server.

Syntax:

Firmware IPv6 Load <ipv6_server> <file_name>

Parameters:

<ipv6_server>: TFTP server IPv6 address

6.18 UPnP Command

UPnP Configuration

Description:

Show UPnP configuration.

Syntax:

UPnP Configuration

Example:

Show UPnP configuration.

```
SWITCH/>upnp configuration

UPnP Configuration:
===================

UPnP Mode                       : Disabled
UPnP TTL                        : 4
UPnP Advertising Duration : 100
```

UPnP Mode

Description:

Set or show the UPnP mode.

Syntax:

UPnP Mode [enable|disable]

Parameters:

enable : Enable UPnP

disable: Disable UPnP

(default: Show UPnP mode)

Default Setting:

disable

Example:

Enable the UPnP mode.

```
SWITCH/>upnp mode enable
```

UPnP TTL

Description:

Set or show the TTL value of the IP header in SSDP messages.

Syntax:

UPnP TTL [<ttl>]

Parameters:

<ttl>: ttl range (1..255), default: Show UPnP TTL

Default Setting:

4

Example:

Set the value 10 for TTL value of the IP header in SSDP messages.

```
SWITCH/>upnp ttl 10
```

UPnP Advertising Duration

Description:

Set or show UPnP Advertising Duration.

Syntax:

UPnP Advertising Duration [<duration>]

Parameters:

<duration>: duration range (100..86400), default: Show UPnP duration range

Default Setting:

100

Example:

Set value 1000 for UPnP Advertising Duration.

```
SWITCH/>upnp advertising duration 1000
```

6.19 MVR Command

MVR Configuration

Description:

Show the MVR configuration.

Syntax:

MVR Configuration

Example:

Show the MVR configuration.

```
SWITCH/>mvr configuration

MVR Configuration:
==================

MVR Mode: Disabled
Muticast VLAN ID: 100

Port   Port Mode      Port Type      Immediate Leave
----    ----------     ----------     ---------------
1       Disabled       Receive        Disabled
2       Disabled       Receive        Disabled
3       Disabled       Receive        Disabled
4       Disabled       Receive        Disabled
5       Disabled       Receive        Disabled
6       Disabled       Receive        Disabled
7       Disabled       Receive        Disabled
8       Disabled       Receive        Disabled
9       Disabled       Receive        Disabled
10      Disabled       Receive        Disabled
11      Disabled       Receive        Disabled
12      Disabled       Receive        Disabled
13      Disabled       Receive        Disabled
14      Disabled       Receive        Disabled
15      Disabled       Receive        Disabled
16      Disabled       Receive        Disabled
17      Disabled       Receive        Disabled
18      Disabled       Receive        Disabled
```

19	**Disabled**	**Receive**	**Disabled**
20	**Disabled**	**Receive**	**Disabled**
21	**Disabled**	**Receive**	**Disabled**
22	**Disabled**	**Receive**	**Disabled**
23	**Disabled**	**Receive**	**Disabled**
24	**Disabled**	**Receive**	**Disabled**

MVR Group

Description:

Show the MVR group.

Syntax:

MVR Group

MVR Status

Description:

Show the MVR status.

Syntax:

MVR Status

MVR Mode

Description:

Set or show the MVR mode.

Syntax:

MVR Mode [enable|disable]

Parameters:

enable : Enable MVR mode

disable : Disable MVR mode

(default: Show MVR mode)

Default Setting:

disable

Example:

Enable MVR mode.

```
SWITCH/>mvr mode enable
```

MVR Port Mode

Description:

Set or show the MVR port mode.

Syntax:

MVR Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable MVR mode

disable : Disable MVR mode

(default: Show MVR mode)

Default Setting:

disable

Example:

Enable the MVR port mode for port 1-4.

```
SWITCH/>mvr port mode 1-4 enable
```

MVR Multicast VLAN

Description:

Set or show MVR multicast VLAN ID.

Syntax:

MVR Multicast VLAN [<vid>]

Parameters:

<vid>: VLAN ID (1-4095), default: Show current MVR multicast VLAN ID

Default Setting:

100

Example:

Set VLAN 1000 for MVR multicast VLAN ID.

```
SWITCH/>mvr multicast vlan 1000
```

MVR Port Type

Description:

Set or show MVR port type.

Syntax:

MVR Port Type [<port_list>] [source|receiver]

Parameters:

<port_list>: Port list or 'all', default: All ports

source : Enable source mode

receiver : Disable receiver mode

(default: Show MVR port type)

Default Setting:

receive

Example:

Set source type for MVR port type of port 1.

```
SWITCH/>mvr port type 1 source
```

MVR Immediate

Description:

Set or show MVR port state about immediate leave.

Syntax:

MVR Immediate Leave [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable Immediate-leave mode

disable : Disable Immediate-leave mode

(default: Show MVR Immediate-leave mode)

Default Setting:

disable

Example:

Enable MVR port state about immediate leave for port 1.

```
SWITCH/>mvr immediate leave 1 enable
```

6.20 Voice VLAN Command

Voice VLAN Configuration

Description:

Show Voice VLAN configuration.

Syntax:

Voice VLAN Configuration

Example:

Show Voice VLAN configuration.

```
SWITCH/>voice vlan configuration

Voice VLAN Configuration:
=========================

Voice VLAN Mode                    : Disabled
Voice VLAN VLAN ID                 : 1000
Voice VLAN Age Time(seconds)   : 86400
Voice VLAN Traffic Class         : High

Voice VLAN OUI Table:
=====================

Telephony OUI Description
------------ -----------
00-30-4F         PLANET phones
00-03-6B         Cisco phones
00-0F-E2         H3C phones
00-60-B9         Philips and NEC AG phones
00-D0-1E         Pingtel phones
00-E0-75         Polycom phones
00-E0-BB         3Com phones
00-01-E3         Siemens AG phones

Voice VLAN Port Configuration:
==============================
```

Port	Mode	Security	Discovery Protocol
1	Disabled	Disabled	
2	Disabled	Disabled	
3	Disabled	Disabled	
4	Disabled	Disabled	
5	Disabled	Disabled	
6	Disabled	Disabled	
7	Disabled	Disabled	
8	Disabled	Disabled	
9	Disabled	Disabled	
10	Disabled	Disabled	
11	Disabled	Disabled	
12	Disabled	Disabled	
13	Disabled	Disabled	
14	Disabled	Disabled	
15	Disabled	Disabled	
16	Disabled	Disabled	
17	Disabled	Disabled	
18	Disabled	Disabled	
19	Disabled	Disabled	
20	Disabled	Disabled	
21	Disabled	Disabled	
22	Disabled	Disabled	
23	Disabled	Disabled	
24	Disabled	Disabled	

Voice VLAN Mode

Description:

Set or show the Voice VLAN mode.

We must disable MSTP feature before we enable Voice VLAN.

It can avoid the conflict of ingress filter.

Syntax:

Voice VLAN Mode [enable|disable]

Parameters:

enable : Enable Voice VLAN mode.

disable: Disable Voice VLAN mode

(default: Show flow Voice VLAN mode)

Default Setting:

disable

Example:

Enable the Voice VLAN mode.

```
SWITCH/>voice vlan mode enable
```

Voice VLAN ID

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN ID [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

Default Setting:

1000

Example:

Set ID 2 for Voice VLAN ID.

```
SWITCH/>voice vlan id 2
```

Voice VLAN Agetime

Description:

Set or show Voice VLAN age time.

Syntax:

Voice VLAN Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (10-10000000) default: Show age time

Default Setting:

86400sec

Example:

Set Voice VLAN age time in 100sec.

```
SWITCH/>voice valn agetime 100
```

Voice VLAN Traffic Class

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN Traffic Class [<class>]

Parameters:

<class>: Traffic class low/normal/medium/high or 1/2/3/4

Default Setting:

high

Example:

Set medium traffic class for voice VLAN

```
SWITCH/>voice vlan traffic class medium
```

Voice VLAN OUI Add

Description:

Add Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Add <oui_addr> [<description>]

Parameters:

<oui_addr> : OUI address (xx-xx-xx)

<description>: Entry description. Use 'clear' or "" to clear the string

No blank or space characters are permitted as part of a contact.(only in CLI)

Example:

Add Voice VLAN OUI entry.

```
SWITCH/>voice vlan oui add 00-11-22 test
```

Voice VLAN OUI Delete

Description:

Delete Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Delete <oui_addr>

Parameters:

<oui_addr>: OUI address (xx-xx-xx)

Example:

Delete Voice VLAN OUI entry.

```
SWITCH/>voice vlan oui delete 00-11-22
```

Voice VLAN OUI Clear

Description:

Clear Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Clear

Example:

Clear Voice VLAN OUI entry.

```
SWITCH/>voice vlan oui clear
```

Voice VLAN OUI Lookup

Description:

Lookup Voice VLAN OUI entry.

Syntax:

Voice VLAN OUI Lookup [<oui_addr>]

Parameters:

<oui_addr>: OUI address (xx-xx-xx), default: Show OUI address

Example:

Lookup Voice VLAN OUI entry.

```
SWITCH/>voice vlan oui lookup
```

Voice VLAN Port Mode

Description:

Set or show the Voice VLAN port mode.

When the port mode isn't disabled, we must disable MSTP feature

before we enable Voice VLAN. It can avoid the conflict of ingress filter.

Syntax:

Voice VLAN Port Mode [<port_list>] [disable|auto|force]

Parameters:

<port_list>: Port list or 'all', default: All ports

disable : Disjoin from Voice VLAN.

auto : Enable auto detect mode. It detects whether there is VoIP phone attached on the specific port and configure the Voice VLAN members automatically.

force : Forced join to Voice VLAN.

(default: Show Voice VLAN port mode)

Default Setting:

disable

Example:

Set auto mode for port 1-4 of Voice VLAN port mode.

```
SWITCH/>voice vlan port mode 1-4 auto
```

Voice VLAN Security

Description:

Set or show the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN will be blocked 10 seconds.

Syntax:

Voice VLAN Security [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable Voice VLAN security mode.

disable: Disable Voice VLAN security mode

(default: Show flow Voice VLAN security mode)

Default Setting:

disable

Example:

Enable the Voice VLAN port security mode for port 1-4.

```
SWITCH/>voice vlan security 1-4 enable
```

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 problems. If the Ethernet Switch is not functioning properly, make sure the Ethernet Switch was set up according to instructions in this manual.

■ **The Link LED is not lit**

Solution:

Check the cable connection and remove duplex mode of the Ethernet Switch

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

Solution:

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

■ **Performance is bad**

Solution:

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

■ **Why the Switch doesn't connect to the network**

Solution:

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

■ **100Base-TX port link LED is lit, but the traffic is irregular**

Solution:

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

■ **Switch does not power up**

Solution:

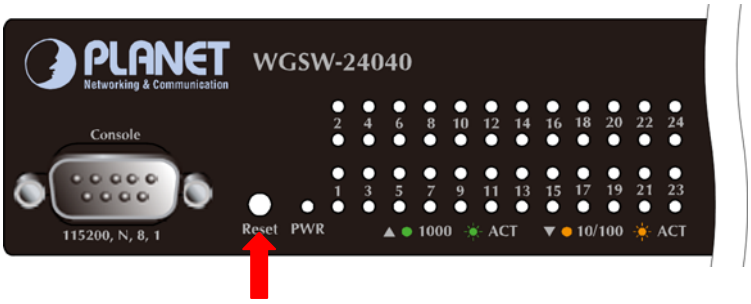
1. AC power cord not inserted or faulty
2. Check that the AC power cord is inserted correctly
3. Replace the power cord If the cord is inserted correctly, check that the AC power source is working by connecting a

different device in place of the switch.

4. If that device works, refer to the next step.
5. If that device does not work, check the AC power

■ **While IP Address be changed or forgotten admin password** –

To reset the IP address to the default IP Address "192.168.0.100" or reset the password to default value. Press the hardware **reset button** at the front panel about **10 seconds.** After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.



Reset

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.

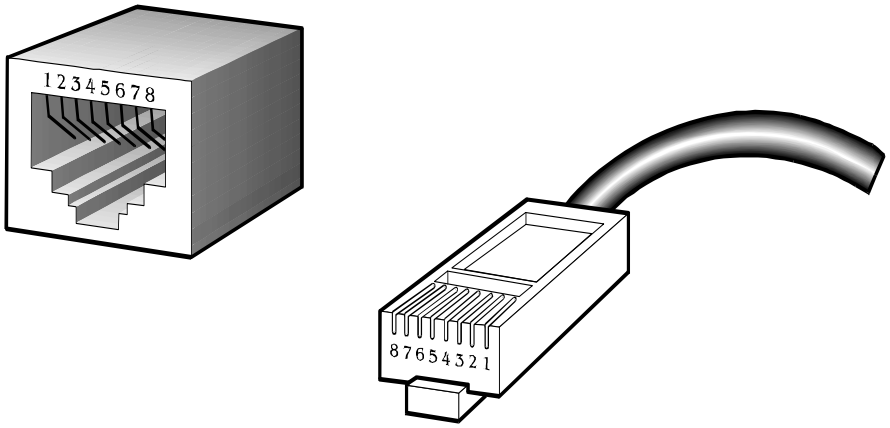
A.2 10/100Mbps, 10/100Base-TX

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:

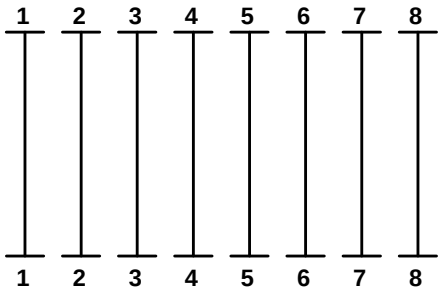
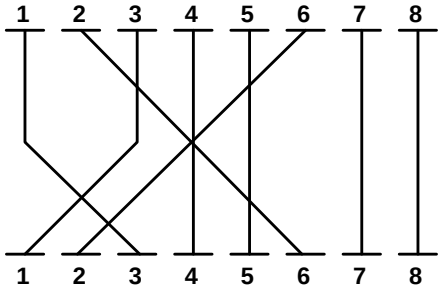
Straight Cable		**SIDE 1**	**SIDE2**
	**SIDE 1**	**1 = White / Orange**	**1 = White / Orange**
		2 = Orange	**2 = Orange**
		3 = White / Green	**3 = White / Green**
		4 = Blue	**4 = Blue**
		5 = White / Blue	**5 = White / Blue**
		6 = Green	**6 = Green**
		7 = White / Brown	**7 = White / Brown**
	SIDE 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.

APPENDEX B : GLOSSARY

A

ACE

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

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

ACL

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

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

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

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

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

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the

frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.

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

ACE

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

APS

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

Aggregation

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

(Also *Port Aggregation, Link Aggregation*).

ARP

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

ARP Inspection

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

Auto-Negotiation

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

C

CC

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

CCM

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

CDP

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

D

DEI

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

DES

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

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

DHCP

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

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

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

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

DHCP Relay

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

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

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

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

DNS

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

DoS

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

Dotted Decimal Notation

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

DSCP

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

E

EEE

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

EPS

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

Ethernet Type

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

F

FTP

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

Fast Leave

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

H

HTTP

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

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

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

HTTPS

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

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

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

I

ICMP

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

IEEE 802.1X

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

IGMP

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

IGMP Querier

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

IMAP

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

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

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from

the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

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

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

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

IPMC

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

IP Source Guard

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

L

LACP

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

LLDP

LLDP is an IEEE 802.1ab standard protocol.
The **L**ink **L**ayer **D**iscovery **P**rotocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management

System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

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

LOC

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

M

MAC Table

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

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

MEP

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

MD5

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

Mirroring

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

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

N

NAS

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

NetBIOS

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

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

NFS

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

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

NTP

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

O

OAM

OAM is an acronym for **O**peration **A**dministration and **M**aintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier ethernet functionality. MEP functionality like CC and RDI is based on this

Optional TLVs.

A LLDP frame contains multiple TLVs

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

OUI

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

P

PCP

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

PHY

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

PING

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

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

Policer

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

POP3

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

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

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

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read

using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

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

Private VLAN

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

PTP

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

Q

QCE

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

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

QCL

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

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

QL

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

QoS

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

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

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

R

RARP

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

RADIUS

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

RDI

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

Router Port

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

RSTP

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

S

SAMBA

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

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

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

SHA

SHA is an acronym for **S**ecure **H**ash **A**lgorithm. It designed by the National Security Agency (NSA) and published by

the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

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

SMTP

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

SNMP

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

SNTP

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

SPROUT

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

SSID

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

SSH

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

SSM

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

STP

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

original STP protocol is now obsoleted by RSTP.

T

TACACS+

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

Tag Priority

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

TCP

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

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

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

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

TELNET

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

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

TFTP

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

ToS

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

TLV

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

TKIP

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

U

UDP

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

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

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

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

UPnP

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

User Priority

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

V

VLAN

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

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

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

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

VLAN ID

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

Voice VLAN

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

W

WEP

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

WiFi

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

WPA

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

necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

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

WPA-Radius

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

WPS

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

WTR

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

EC Declaration of Conformity

For the following equipment:

*Type of Product: 24-Port 10/100/1000Mbps with 4 Shared SFP Managed Gigabit Switch
*Model Number: WGSW-24040 / WGSW-24040R

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

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC).
For the evaluation regarding the EMC, the following standards were applied:

Emission	EN 55022	(Class A:2006)
Harmonic	EN 61000-3-2	(2006)
Flicker	EN 61000-3-3	(1995+A1: 2001+A2:2005)
Immunity	EN 55024	(1998+A1: 2001+A2:2003)
ESD	IEC 61000-4-2	(2001)
RS	IEC 61000-4-3	(2008)
EFT/ Burst	IEC 61000-4-4	(2004)
Surge	IEC 61000-4-5	(2005)
CS	IEC 61000-4-6	(2008)
Magnetic Field	IEC 61000-4-8	(2001)
Voltage Disp	IEC 61000-4-11	(2004)

Responsible for marking this declaration if the:

☒ **Manufacturer** ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Taiwan	**29th Aug, 2008**	Kent Kang
Place	*Date*	*Legal Signature*