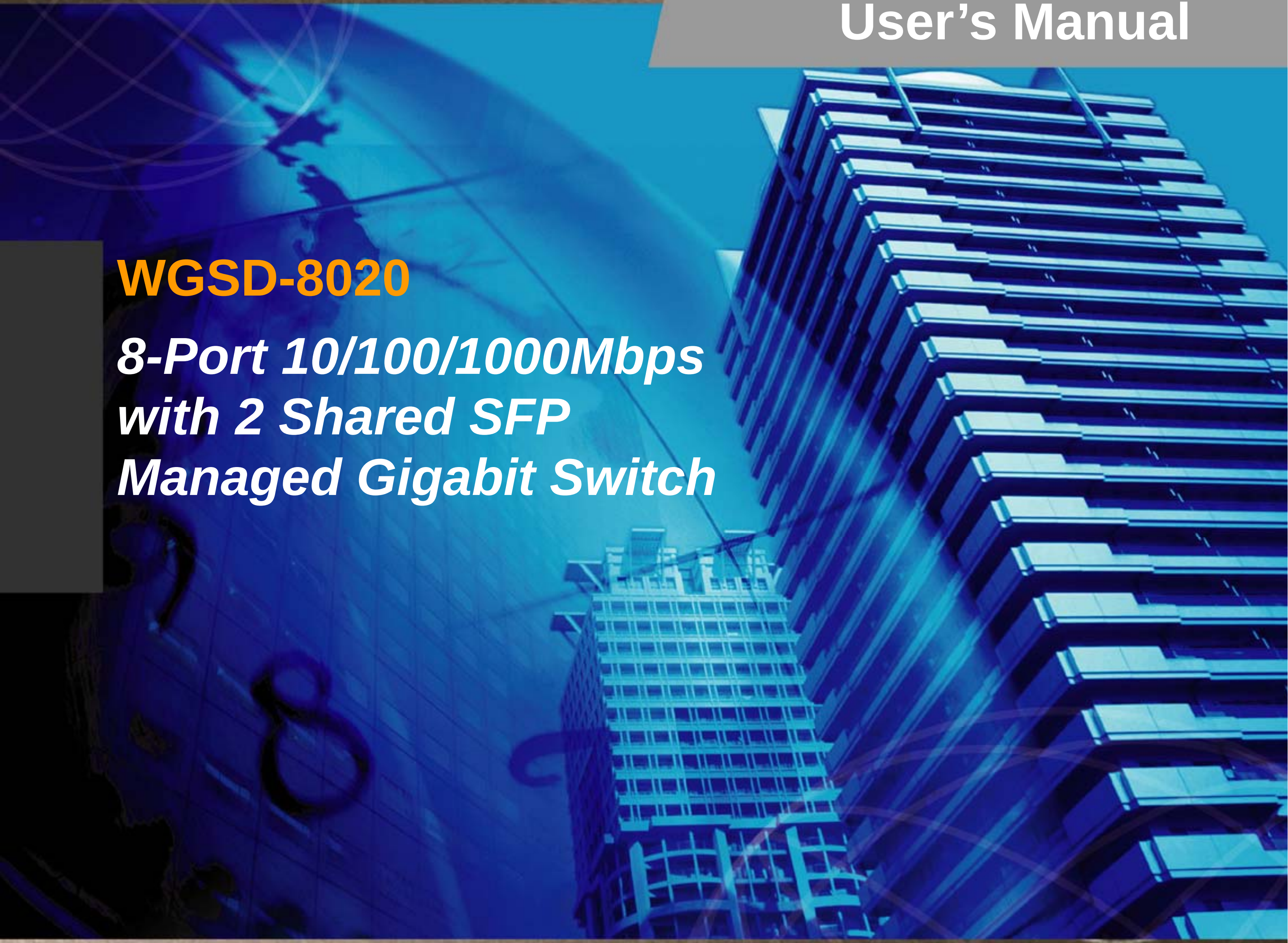
PLANET
Networking & Communication

User's Manual



WGSD-8020

8-Port 10/100/1000Mbps with 2 Shared SFP Managed Gigabit Switch

Trademarks

Copyright © PLANET Technology Corp. 2010.
Contents subject to which revision without prior notice.
PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.

Disclaimer

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

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

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

FCC Warning

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

CE Mark Warning

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

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 8-Port 10/100/1000Mbps with 2 Shared SFP Managed Gigabit Switch User's Manual

FOR MODEL: WGSD-8020

REVISION: 1.1 (February.2010)

Part No: EM-WGSD-8020 (2080-A93190-000)

TABLE OF CONETNTS

1. INTRODUTION

The PLANET WGSD-8020 is a 8-Port 10/100/1000Mbps with 2 shared 100/1000 SFP slots Gigabit Ethernet Switch. It boasts a high performance switch architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as 16Gbps. Its two built-in GbE uplink ports also offer incredible extensibility, flexibility and connectivity to the Core switch or Servers. Terms of “**Managed Switch**” means the Switches mentioned titled in the cover page of this User’s manual.

1.1 Packet Contents

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

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 female 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.

Diversity for Multiple Applications

PLANET WGSD-8020 is a desktop size, **Layer 2 / Layer 4 Full Managed** Gigabit Switch which can handle extremely large amounts of data in a secure topology linking to an Enterprise backbone or high capacity network server with 16Gbps switching fabric. The powerful features of QoS and network security offered by the WGSD-8020 provides effective data traffic control for ISPs and Enterprises VoIP, video streaming and multicast applications. It is ideal for the remote access layer of campus or enterprise networks and the aggregation layer of IP metropolitan networks.

High Performance

The WGSD-8020 provides 8 10/100/1000Mbps Gigabit Ethernet ports with 2 shared Gigabit SFP slots. It boasts high performance architecture of switch that is capable for providing the non-blocking switch fabric and wire-speed throughput as high as 16Gbps, which greatly simplifies the tasks of upgrading the LAN for catering to increasing bandwidth demands.

Robust Layer 2 Features

The WGSD-8020 can be programmed for advanced switch management functions such as dynamic Port link aggregation, **Q-in-Q VLAN**, private VLAN, **Multiple Spanning Tree protocol (MSTP)**, Layer 2 to Layer 4 QoS, bandwidth control and IGMP Snooping. The WGSD-8020 provides 802.1Q Tagged VLAN, and the VLAN groups allowed will be maximally up to 255. Via aggregation of supporting ports, the WGSD-8020 allows the operation of a high-speed trunk combining multiple ports. It enables maximum up to 4 groups of 8 ports for trunk and supports fail-over as well.

Enhanced Security

PLANET WGSD-8020 offers comprehensive **Layer 2 to Layer 4 Access Control List (ACL)** for enforcing security to the edge. It can be used to restrict network access by denying packets based on source and destination IP address, TCP/UDP ports or defined typical network applications. Its protection mechanism also comprises of **802.1x port-based** and **MAC-based** user and device authentication. With the **private VLAN** function, communication between edge ports can be prevented to ensure user privacy. New WGSD-8020 Net Security also provides **DHCP Snooping**, **IP Source Guard** 及 **Dynamic ARP Inspection** functions to prevent IP snooping attack and discard ARP packets with invalid MAC address. The network administrators can now construct highly secured corporate networks with considerably less time and effort than before.

Excellent Traffic Control

The WGSD-8020 series is loaded with powerful traffic management and QoS features to enhance services offered by telecoms. The QoS features includes wire-speed Layer 4 traffic classifiers and bandwidth limiting that are particular useful for multi-tenant unit, multi business unit, Telco, or Network Service Provider applications. The WGSD-8020 also empowers the enterprises to take full advantages of the limited network resources and guarantees the best performance in VoIP and Video conferencing transmission.

Efficient and Secure Management

For efficient management, the WGSD-8020 Managed Ethernet Switch is equipped with console, WEB and SNMP management interfaces. With the built-in Web-based management interface, the WGSD-8020 offers an easy-to-use, platform-independent management and configuration facility. The WGSD-8020 supports standard Simple Network Management Protocol (SNMP) and can be managed via any standard-based management software. For text-based management, the WGSD-8020 can be accessed via Telnet and the console port. Moreover, the WGSD-8020 offers secure remote management by supporting **SSH**, **SSL** and **SNMPv3** connection which encrypt the packet content at each session.

Flexibility and Extension Solution

The two mini-GBIC slots built in the WGSD-8020 support Dual-Speed, **100Base-FX** and **1000Base-SX/LX** SFP (Small Form-factor Pluggable) fiber-optic modules, that means, the administrator now can flexibly choose the suitable SFP transceiver according to the transmission distance or the transmission speed required. 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 applications within the enterprise data centers and distributions.

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, **INSTALLATION**

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

Section 3, **SWITCH MANAGEMENT**

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

Section 4, **WEB CONFIGURATION**

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

Section 5, **COMMAND LINE INTERFACE**

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

Section 6, **CLI CONFIGURATION**

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

Section 7, **SWITCH OPERATION**

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

Section 8, **TROUBSHOOTING**

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

Appendix A

The section contains cable information of the Managed Switch.

1.4 Product Features

- **Physical Port**
  - **8-Port 10/100/1000Base-T** RJ-45 copper
  - **2 100/1000Base-X mini-GBIC/SFP** slots, shared with Port-7 to Port-8
  - RS-232 DB9 console interface for basic management and setup

- **Layer 2 Features**
  - Prevents packet loss with back pressure (Half-Duplex) and IEEE 802.3x PAUSE frame flow control (Full-Duplex)
  - High performance of Store-and-Forward architecture and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
  - Storm Control support:
    - Broadcast / Multicast / Unknown-Unicast
  - Support **VLAN**
    - IEEE 802.1Q Tagged VLAN
    - Up to 256 VLANs groups, out of 4095 VLAN IDs
    - Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
    - Private VLAN Edge (PVE)
  - Support **Spanning Tree Protocol**
    - STP, IEEE 802.1D Spanning Tree Protocol
    - RSTP, IEEE 802.1w Rapid Spanning Tree Protocol
    - 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 4 trunk groups, up to 8 ports per trunk group
    - Up to 16Gbps bandwidth (Duplex Mode)
  - Provide Port Mirror (many-to-1)
  - Port Mirroring to monitor the incoming or outgoing traffic on a particular port

- **Quality of Service**
  - Ingress 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

- **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 and Relay Option 82
  - 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

1.5 Product Specification

Product	**WGSD-8020**
Hardware Specification	
Copper Ports	8 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports
SFP/mini-GBIC Slots	2 1000Base-SX/LX/BX SFP interfaces, shared with Port-7 and Port-8 Compatible with 100Base-FX SFP
Console	1 x RS-232 DB9 serial port (115200, 8, N, 1)
Switch Architecture	Store-and-Forward
Switch Fabric	16Gbps / non-blocking
Address Table	8K entries, automatic source address learning and ageing
Share data Buffer	1392 kilobytes
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
LED	Power, 1000 Link/Act, 100 Link/Act
Dimension (W x D x H)	330 x 155 x 43.5 mm, 13-inch, 1U height
Weight	1.26 kg
Power Requirement	100~240V AC, 50/60Hz
Power Consumption	Max. 14.5 Watts / 49.46 BTU
ESD Protection	6KV DC
Layer 2 function	
Basic Management Interfaces	Console, Telnet, Web Browser, SNMPv1, v2c
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 Power saving mode control
Port Status	Display each port's speed duplex mode, link status, Flow control status. Auto negotiation status, trunk status.
Port Mirroring	TX / RX / Both Many to 1 monitor
VLAN	802.1Q Tagged Based VLAN ,up to 256 VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE) Up to 256 VLAN groups, out of 4094 VLAN IDs
Link Aggregation	IEEE 802.3ad LACP / Static Trunk Support 4 groups of 8-Port trunk support
QoS	Traffic classification based, Strict priority and WRR 4-level priority for switching - Port Number - 802.1p priority

	- 802.1Q VLAN tag - DSCP/TOS field in IP Packet
IGMP Snooping	IGMP (v1/v2/V3) Snooping, up to 255 multicast Groups IGMP Querier mode support
Access Control List	IP-Based ACL / MAC-Based ACL Up to 123 entries
Bandwidth Control	Per port bandwidth control Ingress: 500Kbps~1000Mbps Egress: 500Kbps~1000Mbps
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-1643 Ethernet MIB RFC-2863 Interface MIB RFC-2665 Ether-Like MIB RFC-2819 RMON MIB (Group 1, 2, 3 and 9) RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC-2933 IGMP-STD-MIB RFC-3411 SNMP-Frameworks-MIB IEEE 802.1X 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 protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2
Environment	
Operating	Temperature: 0 ~ 50 Degree C Relative Humidity: 20 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 70 Degree C Relative Humidity: 20 ~ 95% (non-condensing)

2. INSTALLATION

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

2.1 Hardware Description

2.1.1 Switch Front Panel

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

WGSD-8020 Front Panel

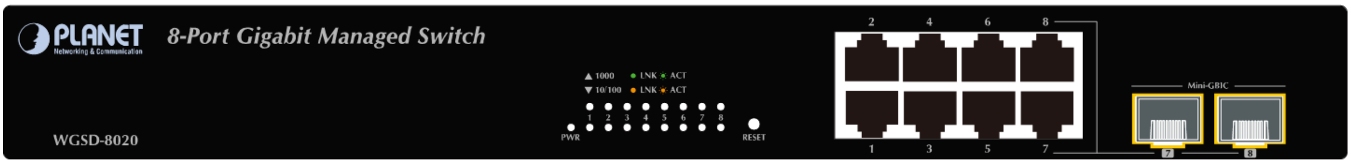


Figure 2-1-1 WGD-8020 front panel.

- **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).

- **Reset button**

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

Reset Button Pressed and Released	Function
About **1~3 second**	Reboot the Managed Switch
Until the **PWR** LED lit **off**	Reset the Managed Switch to Factory Default configuration. The Managed Switch will then reboot and load the default settings as below: ◦ Default User Name: **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, system operation, Stack status and system power, helps monitor and troubleshoot when needed.

WGSD-8020 LED indication

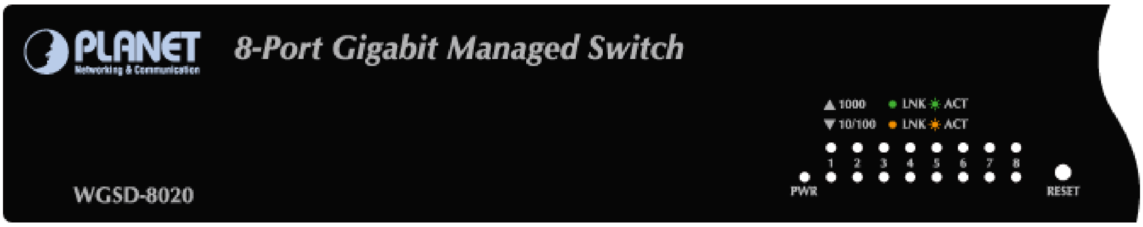


Figure 2-1-2 WGSD-8020 LED panel

- **System**

LED	Color	Function
PWR	**Green**	Lights to indicate that the Switch has power.

- **Per 10/100/1000Mbps port**

LED	Color	Function
1000 LNK/ACT	**Green**	**Lights** to indicate the port is running in **1000Mbps** speed and successfully established. **Blink**: indicate that the switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Orange**	**Lights** to indicate the port is running in **100Mbps** or **10Mbps** speed. **Blink**: indicate that the switch is actively sending or receiving data over that port.

- **Per 1000Base-SX/LX SFP interfaces (Shared Port-7 and Port-8)**

LED	Color	Function
1000	**Green**	**Lights** to indicate the link through that port is successfully established.

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 2-1-3 shows the rear panel of these Managed Switches

WGSD-8020 Rear Panel

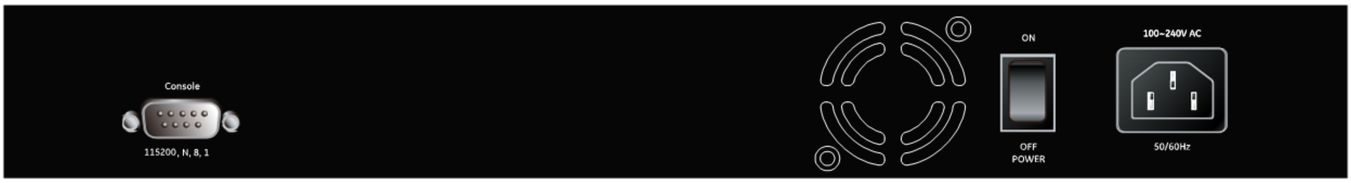


Figure 2-1-3 Rear panel of **WGSD-8020**

- **Console Port**

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

- **AC Power Receptacle**

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

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

Power Notice:

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

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

2.2 Install the Switch

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

2.2.1 Desktop Installation

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

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

Step2: Place the Managed Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-2-1.

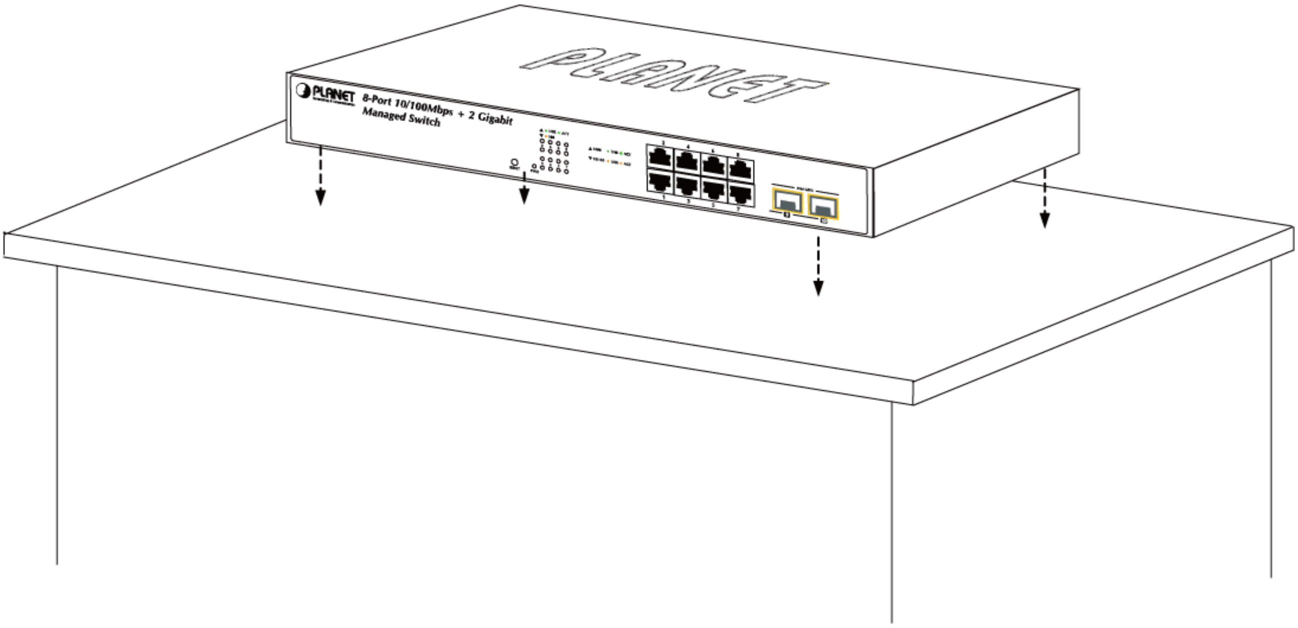


Figure 2-2-1 Place the Managed Switch on the desktop

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

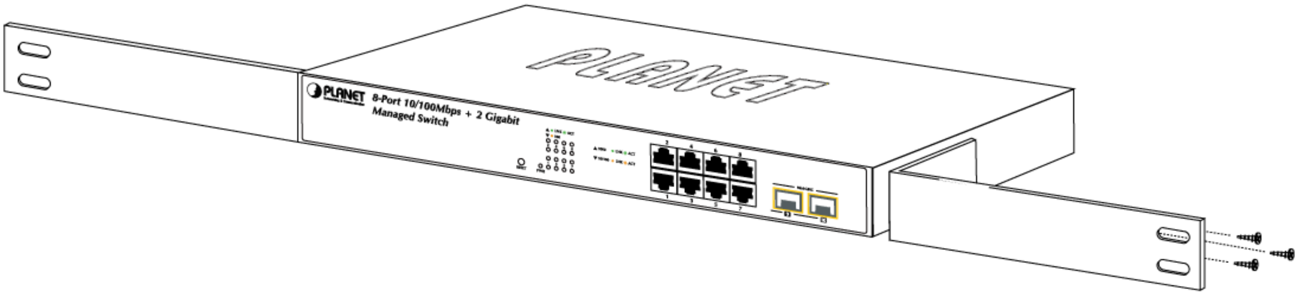


Figure 2-2-2 Attach brackets to the Managed Switch.

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

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 2-2-3.

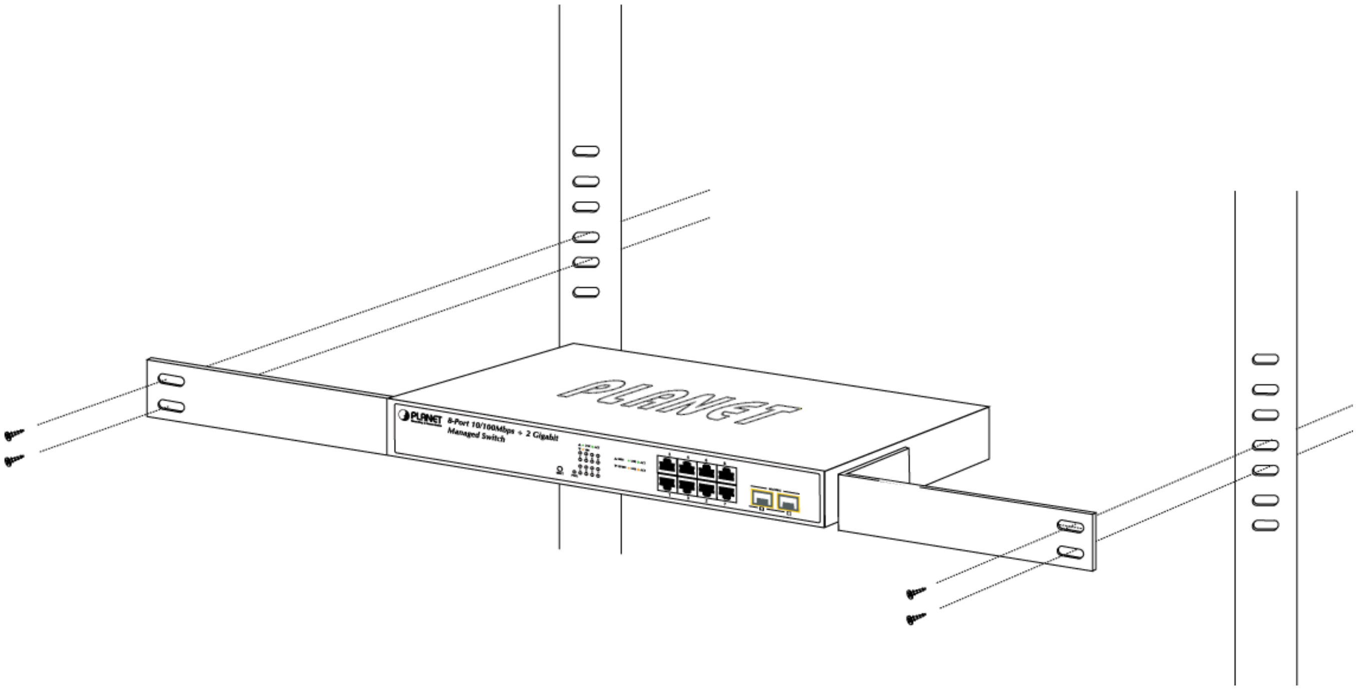


Figure 2-2-3 Mounting WGSD-8020 in a Rack

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 2-2-4 appears.

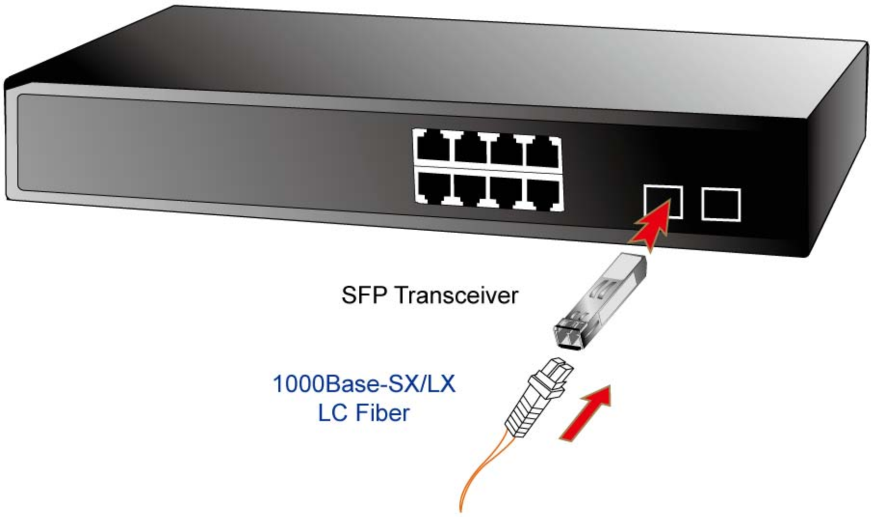


Figure 2-2-4 Plug-in the SFP transceiver

- **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:

Gigabit SFP Transceiver modules:

- **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)

100Base-FX SFP Transceiver modules:

- **MFB-FX** SFP (100BASE-FX SFP transceiver / Multi-mode / 1310nm / 2km)
- **MFB-F20** SFP (100BASE-FX SFP transceiver / Single mode / 1310nm / 20km)
- **MFB-FA20** SFP (100BASE-FX SFP transceiver / WDM Single mode / TX:1310nm, RX:1550nm / 20km)
- **MFB-FB20** SFP (100BASE-FX SFP transceiver / WDM Single mode / TX:1550nm, TX:1310nm / 20km)

Note

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

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

1. Make sure both side of the SFP transceiver are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.
2. Check the fiber-optic cable type match the SFP transceiver model.
   - To connect to 1000Base-SX SFP transceiver, use the Multi-mode fiber cable- with one side must be male duplex LC connector type.
   - To connect to 1000Base-LX SFP transceiver, use the Single-mode fiber cable-with one side must be male duplex LC connector type.

Connect the fiber cable

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

Remove the transceiver module

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

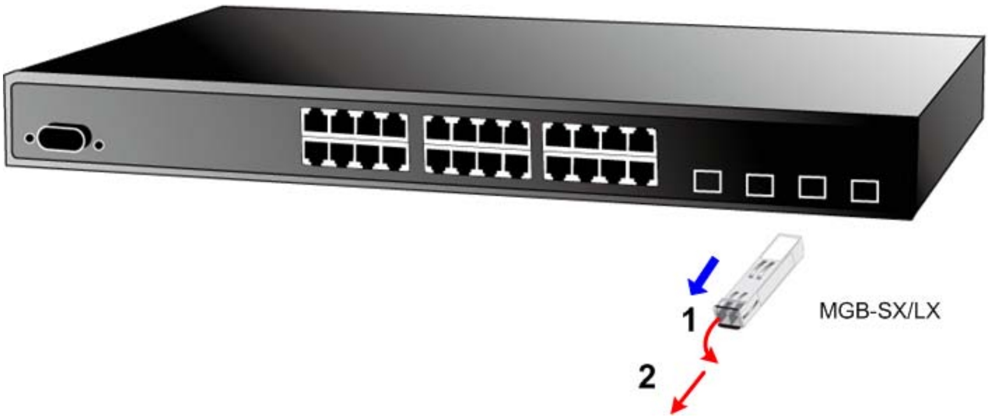


Figure 2-2-5 Pull out the SFP transceiver

Note

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

3. SWITCH MANAGEMENT

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

This chapter covers the following topics:

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

3.1 Requirements

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

Note

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

3.2 Management Access Overview

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

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

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

Method	Advantages	Disadvantages
Console	• No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems • Secure	• Must be near switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1 Management Methods Comparison

3.3 Administration Console

The administration console is an internal, character-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the switch's console (serial) port. There are two ways to use this management method: via direct access or modem port access. The following sections describe these methods. For more information about using the console, refer to **Chapter 5 Command Line Interface Console Management**.

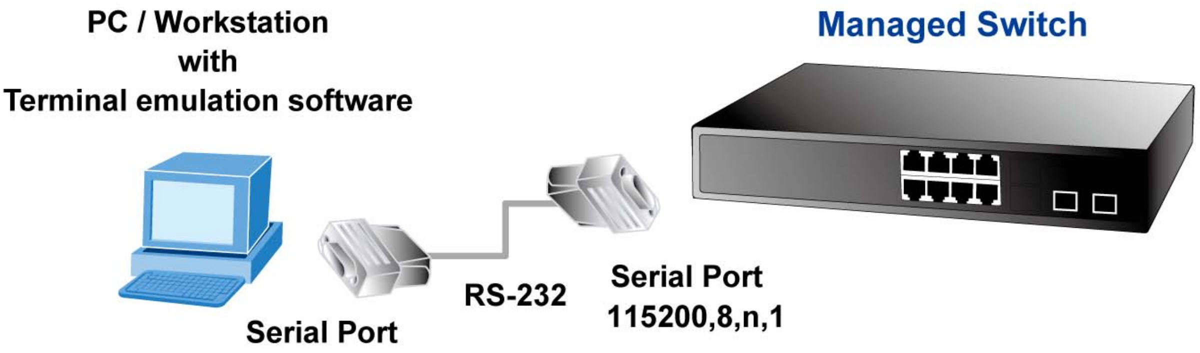


Figure 3-3-1 Console management

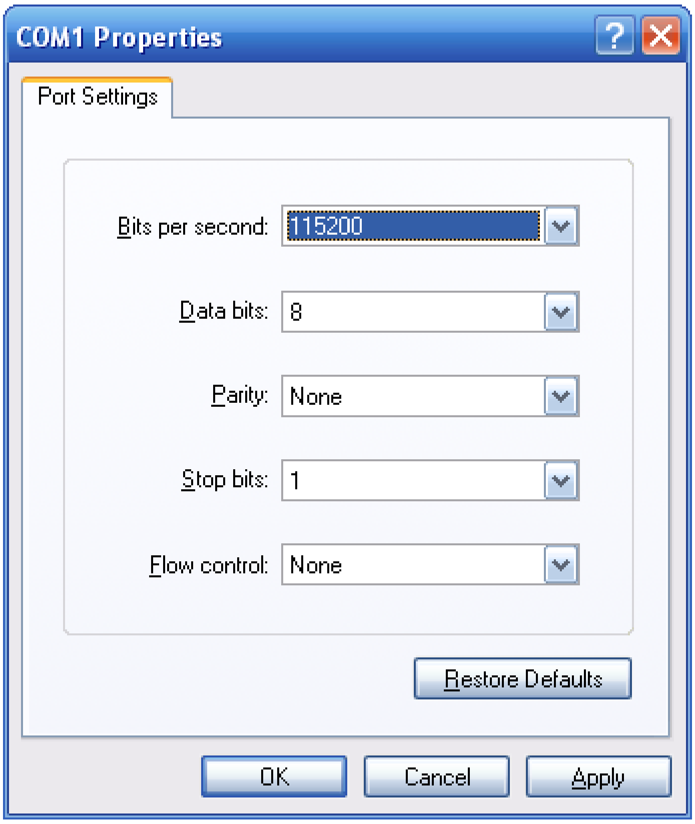
Direct Access

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**
- **No Flow Control**



Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 3-3-2 Terminal parameter settings

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.

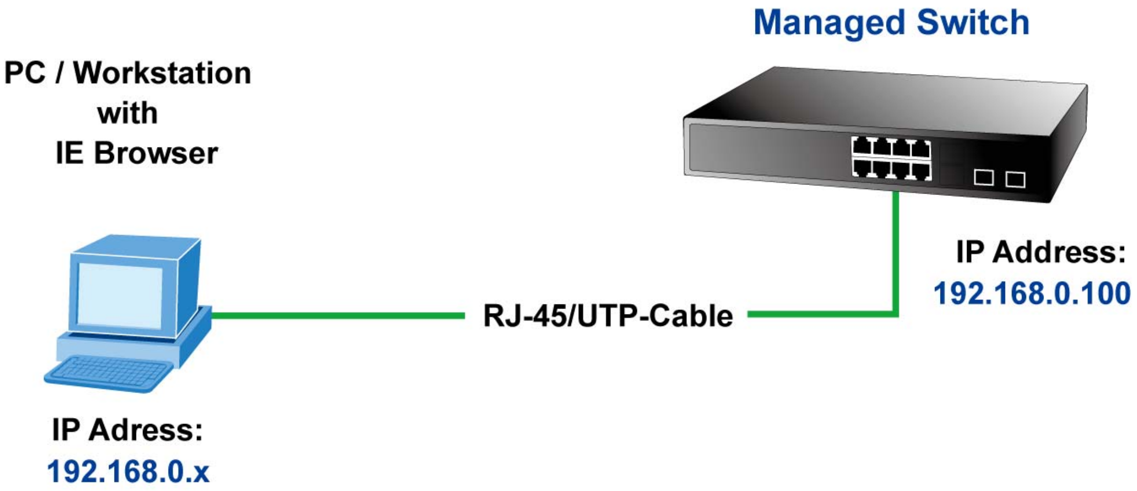
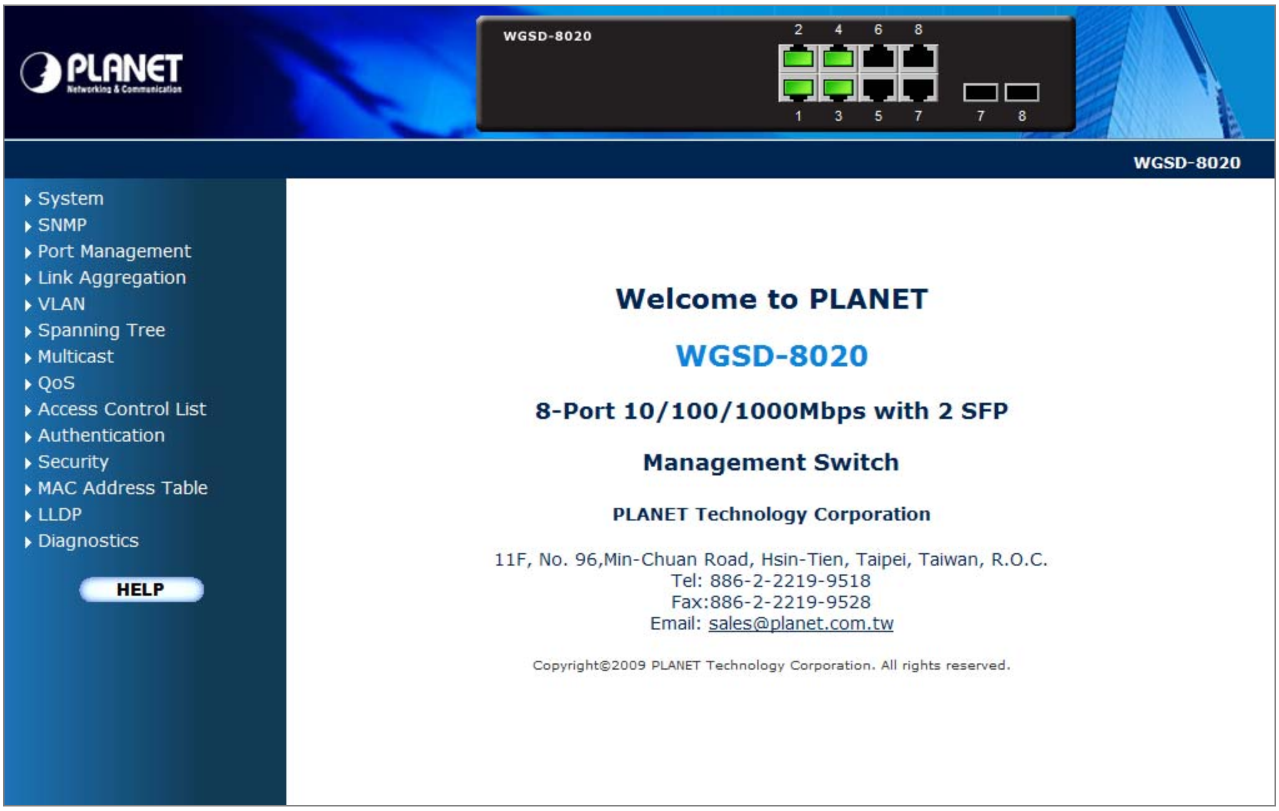


Figure 3-4-1 Web management

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.



Welcome to PLANET

WGSD-8020

8-Port 10/100/1000Mbps with 2 SFP

Management Switch

PLANET Technology Corporation

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

Copyright©2009 PLANET Technology Corporation. All rights reserved.

Figure 3-4-2 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.

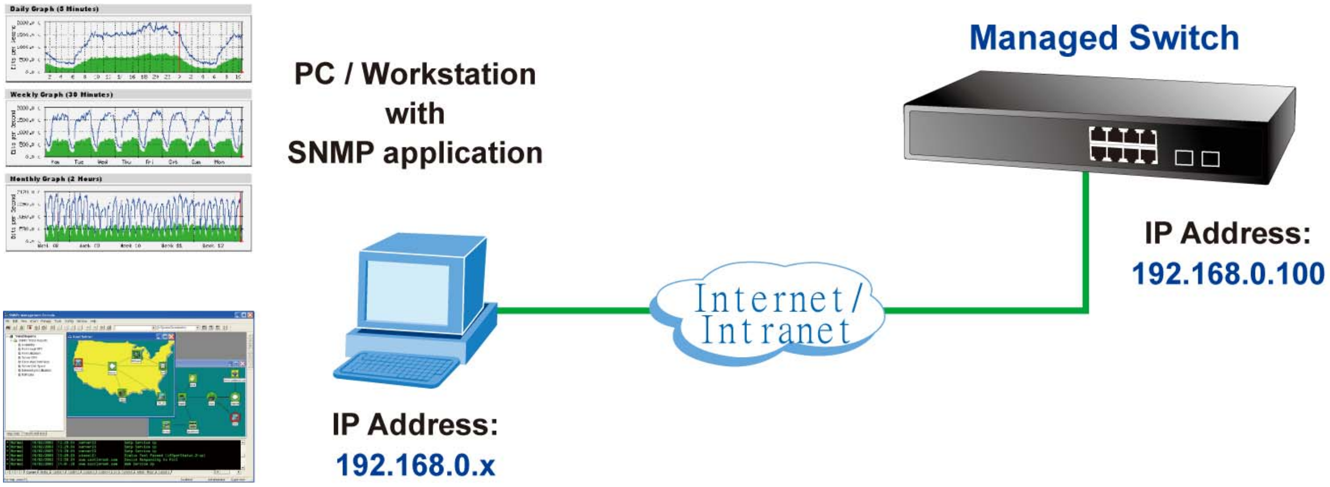


Figure 3-5-1 SNMP management

3.6 Protocols

The Managed Switch supports the following protocols:

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

3.6.1 Virtual Terminal Protocols

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

Note

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

To access the Managed Switch through a Telnet session:

1. Be Sure of the Managed Switch is configured with an IP address and the Managed Switch is reachable from a PC.
2. Start the Telnet program on a PC and connect to the Managed Switch.

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

3.6.2 SNMP Protocol

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

3.6.3 Management Architecture

All of the management application modules use the same Messaging Application Programming Interface (MAPI). By unifying management methods with a single MAPI, configuration parameters set using one method (console port, for example) are immediately displayable by the other management methods (for example, SNMP agent of Web browser).

The management architecture of the switch adheres to the IEEE open standard. This compliance assures customers that the Managed Switch is compatible with, and will interoperate with other solutions that adhere to the same open standard.

4. WEB CONFIGURATION

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

About Web-based Management

The Managed Switch offers management features that allow users to manage the Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome or Apple Safari.

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

Note

By default, IE6.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

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

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

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

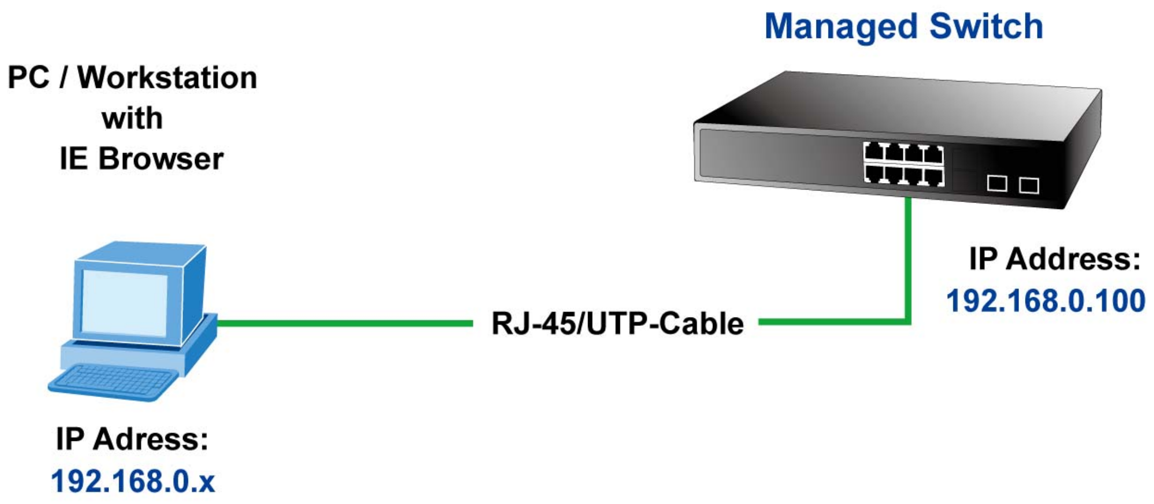


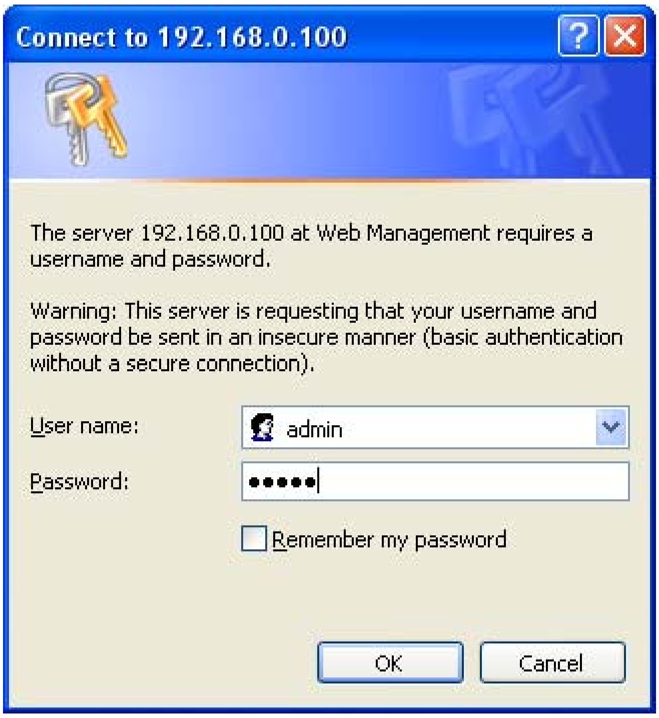
Figure 4-1-1 Web Management

- **Logging on the switch**

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

http://192.168.0.100

2. When the following login screen appears, please enter the default user name **"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.



Connect to 192.168.0.100

The server 192.168.0.100 at Web Management requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password: •••••

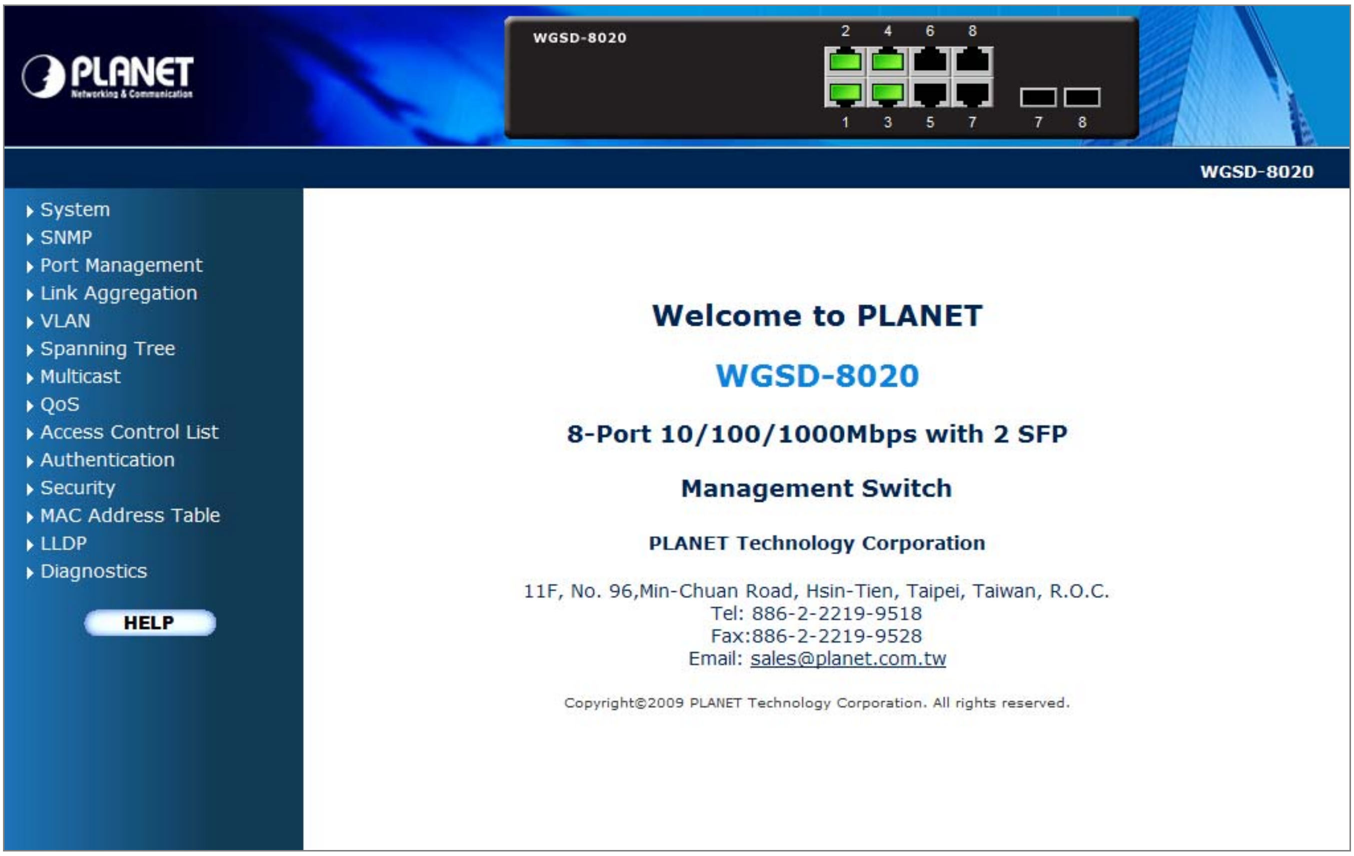
□ Remember my password

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.



Welcome to PLANET

WGSD-8020

8-Port 10/100/1000Mbps with 2 SFP

Management Switch

PLANET Technology Corporation

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

Copyright©2009 PLANET Technology Corporation. All rights reserved.

Figure 4-1-3 Default main page screenshot

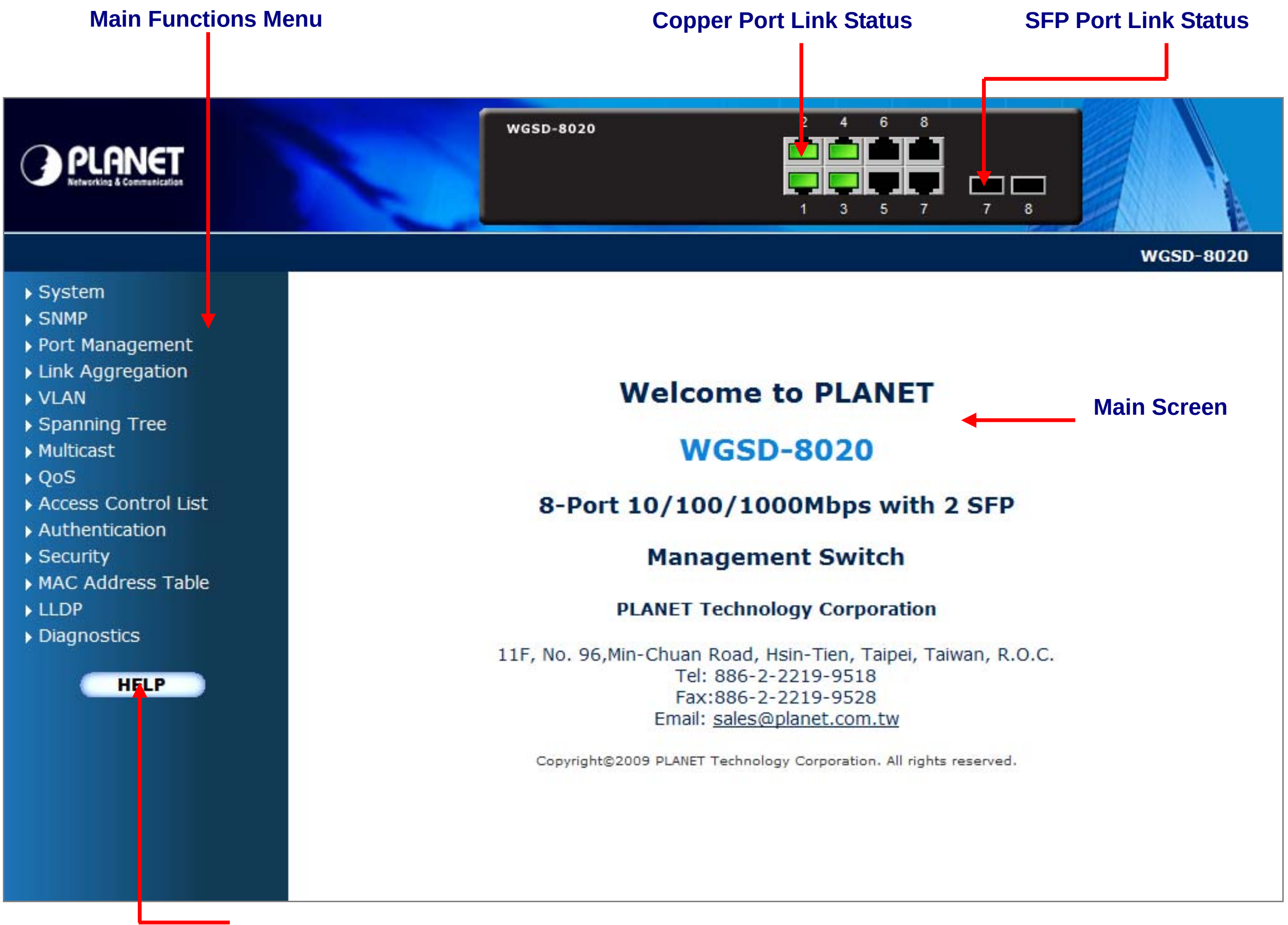
Now, you can use the Web management interface to continue the switch management or manage the Managed Switch by Web interface. The Switch Menu on the left of the web page let you access all the commands and statistics the Managed Switch provides.

Note

1. It is recommended to use Internet Explore 6.0 or above to access Managed Switch.
2. The changed IP address take effect immediately after click on the **Save** button, you need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.
4. Only accept command in lowercase letter under web interface.

4.1 Main WEB PAGE

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



Welcome to PLANET

WGSD-8020

8-Port 10/100/1000Mbps with 2 SFP

Management Switch

PLANET Technology Corporation

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

Copyright©2009 PLANET Technology Corporation. All rights reserved.

Figure 4-1-4 Main page screenshot

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.

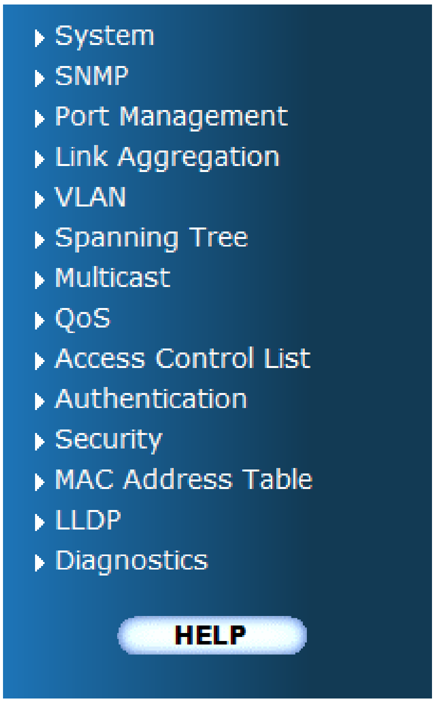


Figure 4-1-5 WGSD-8020 Managed Switch Main Funcrions Menu

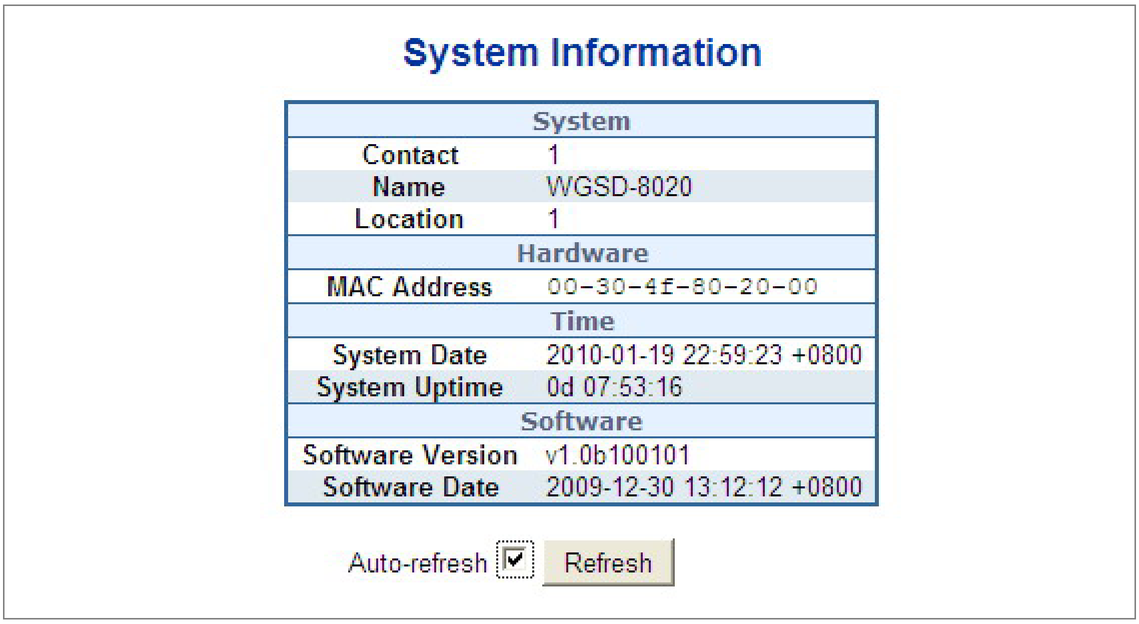
4.2 System

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

- **System Information** Provides basic system description, including contact information.
- **IP Configuration** Sets the IPv4 address for management access.
- **IPv6 Configuration** Sets the IPv6 address for management access.
- **Users Configuration** Configure the system user name and password required to access the web pages or log in from CLI.
- **Users Provolege Levels** Provides an overview of the users privilege levels.
- **NTP Configuration** Network Time Protocol. Configures NTP client settings, including broadcast mode or aspecified list of servers.
- **UPnP** Configure UPnP.
- **DHCP Relay** Configure DHCP Relay.
- **DHCP Relay Statistics** Provides statistics for DHCP relay.
- **System Log** Provides switch system log information here.
- **Detail Log** Provides switch detail log information here.
- **Web Firmware Upgrade** Upgrade the firmware via Web browser
- **TFTP Firmware Upgrade** Upgrade the firmware via TFTP server
- **Configuration Save** Save/view the switch configuration to remote host
- **Configuration Upload** Upload the switch configuration from remote host
- **Factory Default** Reset the configuration of the Managed Switch
- **System Reboot** Restarts the Managed Switch.

4.2.1 System Information

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



System Information

System	
Contact	1
Name	WGSD-8020
Location	1
Hardware	
MAC Address	00-30-4f-80-20-00
Time	
System Date	2010-01-19 22:59:23 +0800
System Uptime	0d 07:53:16
Software	
Software Version	v1.0b100101
Software Date	2009-12-30 13:12:12 +0800

Figure 4-2-1 System Information page screenshot

The page includes the following fields:

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

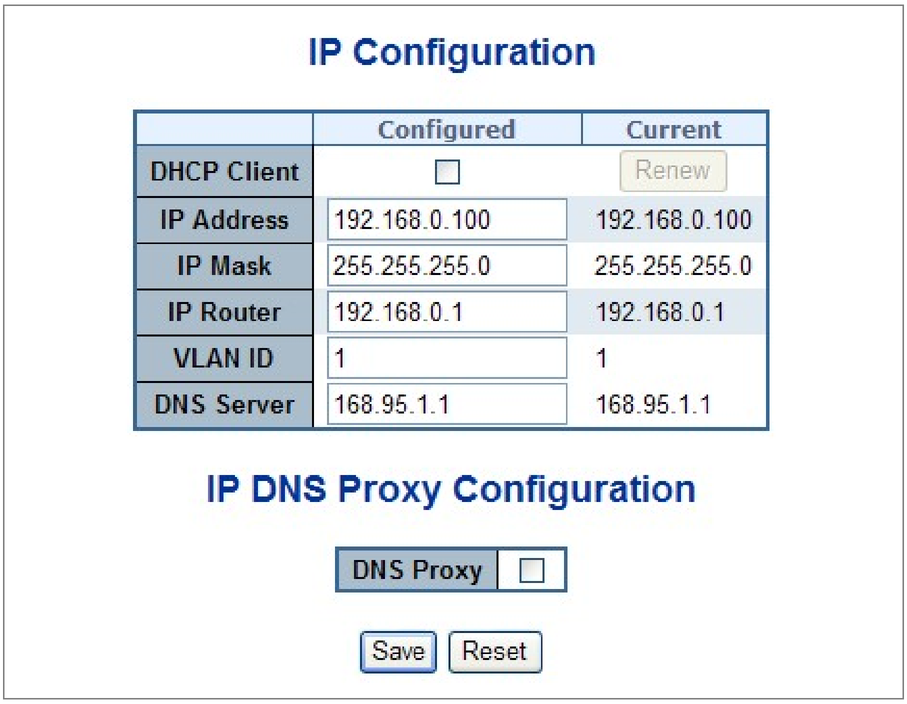
Buttons

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 IPv4 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.



IP Configuration

	Configured	Current
DHCP Client	□	Renew
IP Address	192.168.0.100	192.168.0.100
IP Mask	255.255.255.0	255.255.255.0
IP Router	192.168.0.1	192.168.0.1
VLAN ID	1	1
DNS Server	168.95.1.1	168.95.1.1

IP DNS Proxy Configuration

DNS Proxy □

Figure 4-2-2 IP Configuration page screenshot

The page includes the following fields:

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.
• **VLAN ID**	Provide the managed VLAN ID. The allowed range is **`1`** through **`4095`**.
• **DNS Server**	Provide the IP address of the DNS Server in dotted decimal notation.
• **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.

4.2.3 IPv6 Configuration

Internet Protocol version 6 (IPv6) is the next-generation Internet Protocol version designated as the successor to IPv4, the first implementation used in the Internet that is still in dominant use currently[update]. It is an Internet Layer protocol for packet-switched internetworks. The main driving force for the redesign of Internet Protocol is the foreseeable IPv4 address exhaustion.

IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

IPv6 also implements new features that simplify aspects of address assignment (stateless address autoconfiguration) and network renumbering (prefix and router announcements) when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from Link Layer media addressing information (MAC address).

Network security is integrated into the design of the IPv6 architecture. Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread optional deployment first in IPv4 (into which it was back-engineered). The IPv6 specifications mandate IPsec implementation as a fundamental interoperability requirement.

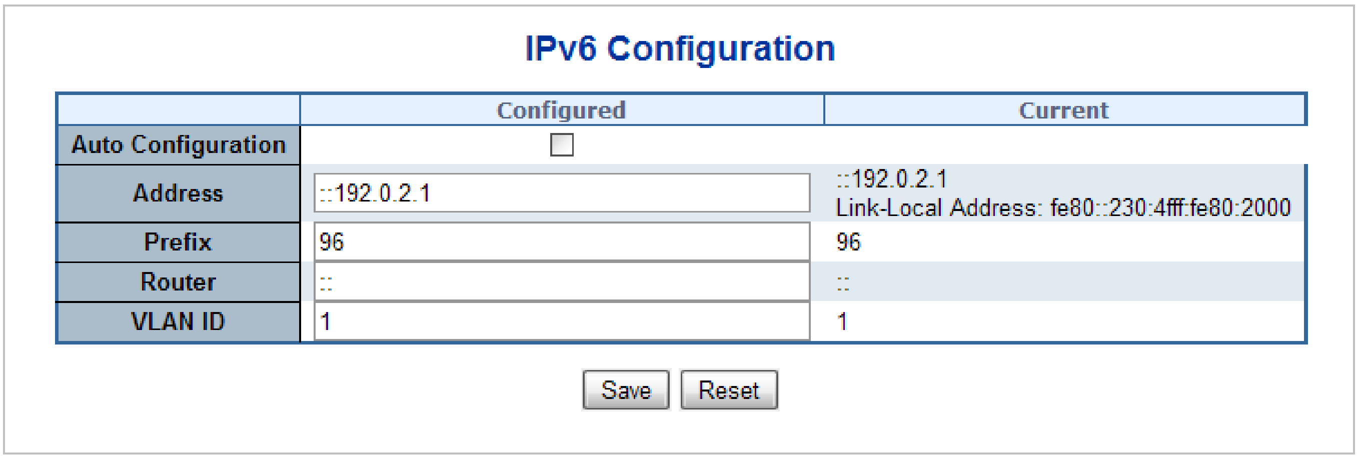
The address is an eight-part hex address separated by colons (" :"). Each part n can equal a 16-bit number and is eight parts long, providing a 128-bit address length (16 * 8 = 128),

Note

Format of IPv6 Addresses are **n:n:n:n:n:n:n:n** n = 4 digit hexadecimal integer, 16 * 8 = 128 address.

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.



IPv6 Configuration

	Configured	Current
Auto Configuration	☐	
Address	::192.0.2.1	::192.0.2.1 Link-Local Address: fe80::230:4fff:fe80:2000
Prefix	96	96
Router	::	::
VLAN ID	1	1

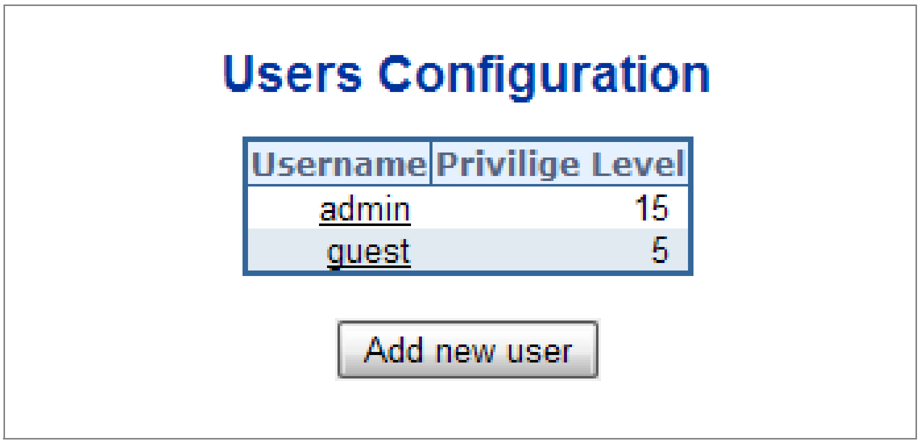
Figure 4-2-3 IPv6 Configuration page screenshot

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.
• **VLAN ID**	Provide the managed VLAN ID. The allowed range is 1 through 4095

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 and Figure 4-2-5 appears.



Users Configuration

Username	Privilige Level
admin	15
guest	5

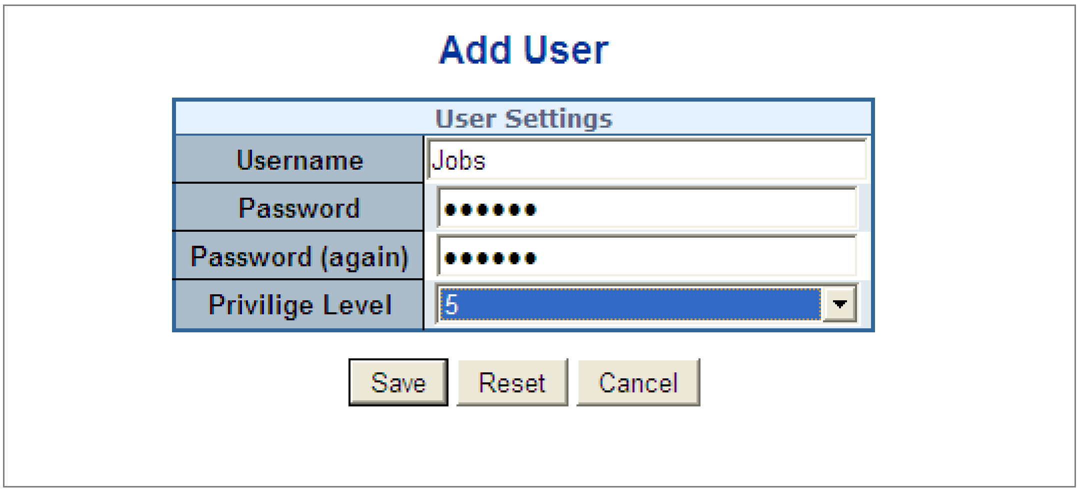
Figure 4-2-4 Users Configuration page screenshot

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.
• **Add new User**	Click to add a new user.

Add / Edit User

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



Add User

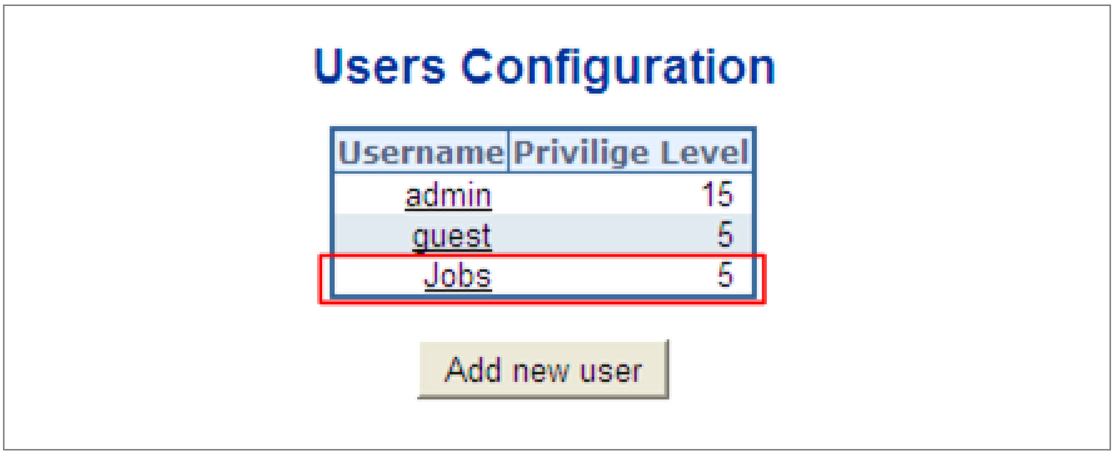
User Settings	
Username	Jobs
Password	••••••
Password (again)	••••••
Privilige Level	5

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.
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.



Users Configuration

Username	Privilige Level
admin	15
guest	5
Jobs	5

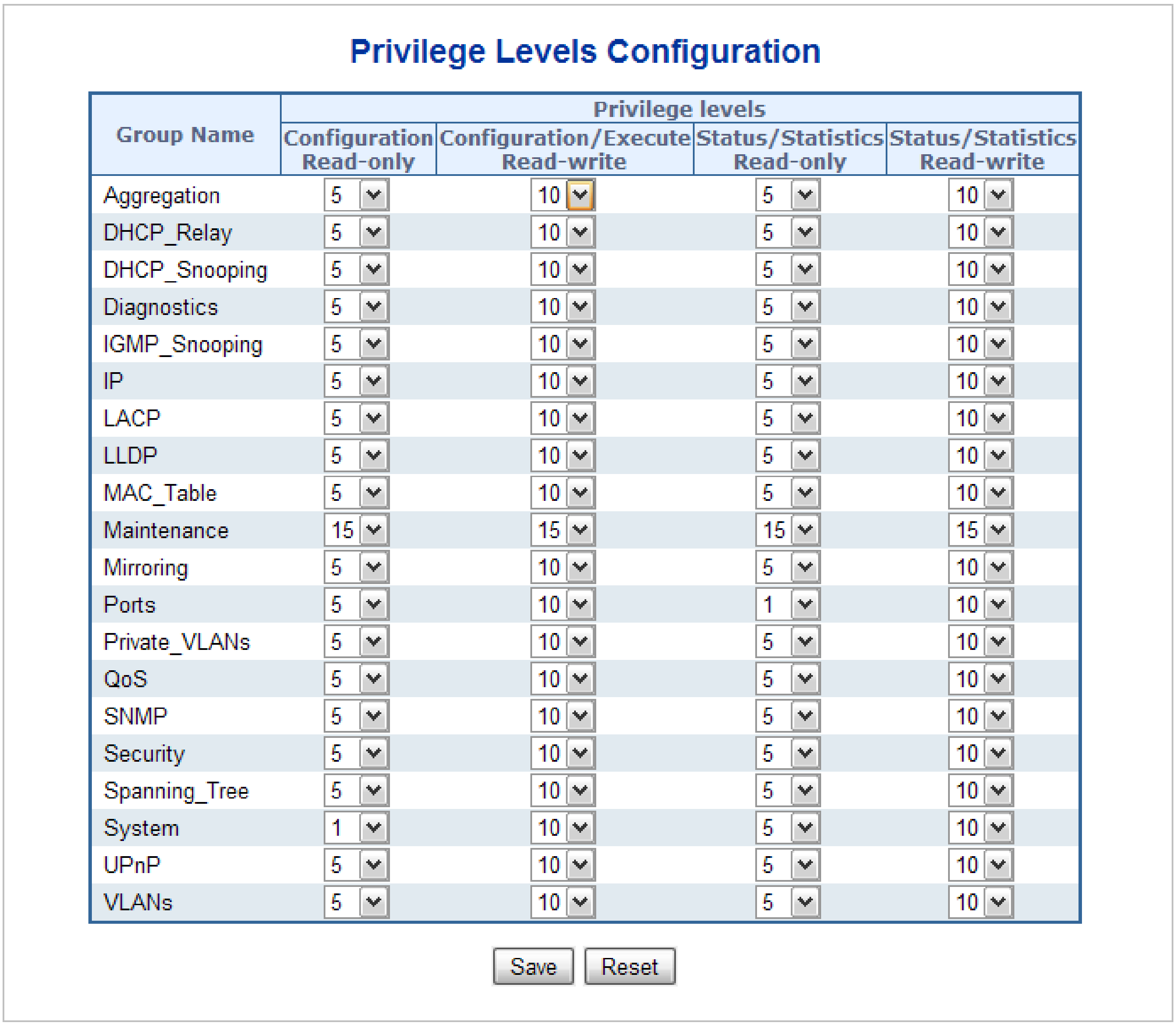
Figure 4-2-6 User Configuration page screenshot

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 Privildge Levels

This page provides an overview of the privilege levels.



Privilege Levels Configuration

Group Name	Privilege levels			
	Configuration Read-only	Configuration/Execute Read-write	Status/Statistics Read-only	Status/Statistics Read-write
Aggregation	5	10	5	10
DHCP_Relay	5	10	5	10
DHCP_Snooping	5	10	5	10
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
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
Mirroring	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	1	10	5	10
UPnP	5	10	5	10
VLANs	5	10	5	10

Figure 4-2-7 User privilege levels Configuration page screenshot

The page includes the following fields:

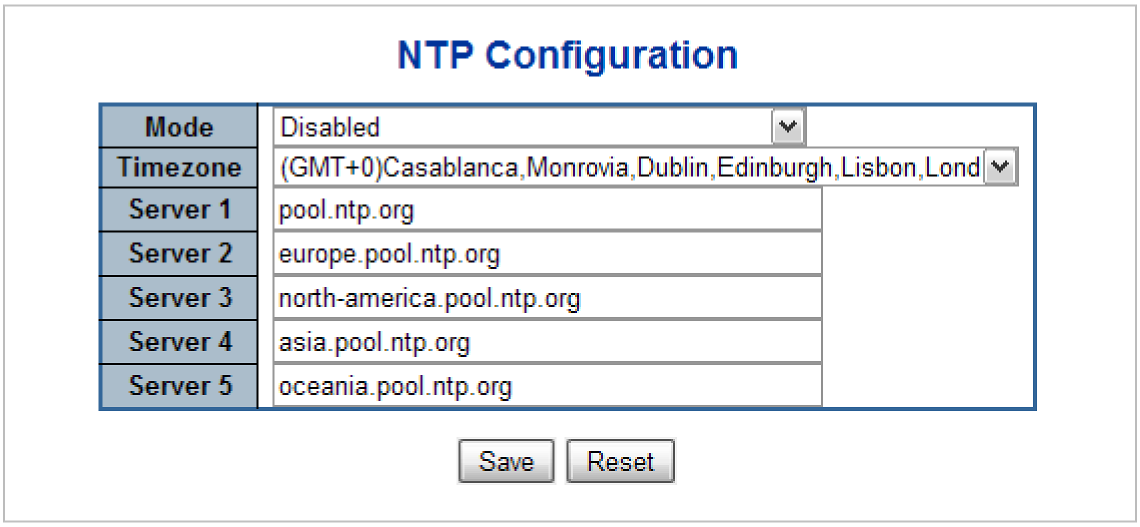
Object	Description
• **Group Name**	The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details: ■ **System**: 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 Levels**	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 (datagrams) as transport layer. You can specify NTP Servers and set GMT Timezone. The NTP Configuration screen in Figure 4-2-8 appears.



NTP Configuration

Mode	Disabled
Timezone	(GMT+0)Casablanca,Monrovia,Dublin,Edinburgh,Lisbon,Lond
Server 1	pool.ntp.org
Server 2	europe.pool.ntp.org
Server 3	north-america.pool.ntp.org
Server 4	asia.pool.ntp.org
Server 5	oceania.pool.ntp.org

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.
• **Time Zone**	The difference between **Greenwich Mean Time (GMT)** and local time. For example, the Time Zone Offset for Paris is GMT +1, while the local time in Taipei is GTM +8.
• **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'.

Note

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

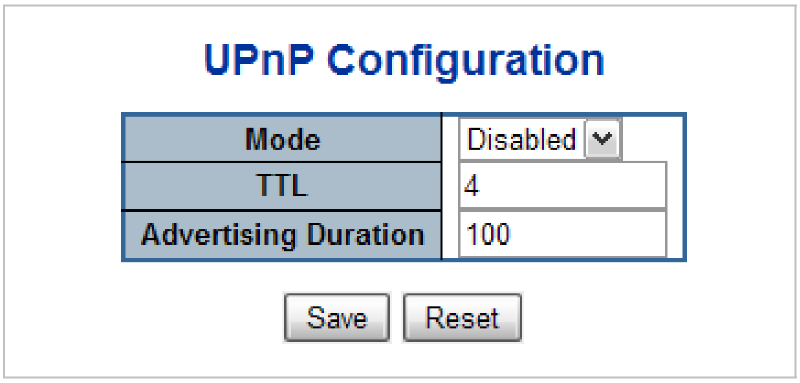
For more detail about the Time Server and Time Server List, please refer to the following URL:

http://ntp.isc.org/bin/view/Servers/WebHome
http://ntp.isc.org/bin/view/Servers/NTPPoolServers
http://support.microsoft.com/kb/262680/en-us

4.2.7 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.



UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100

Figure 4-2-9 UPnP Configuration page screenshot

The page includes the following fields:

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

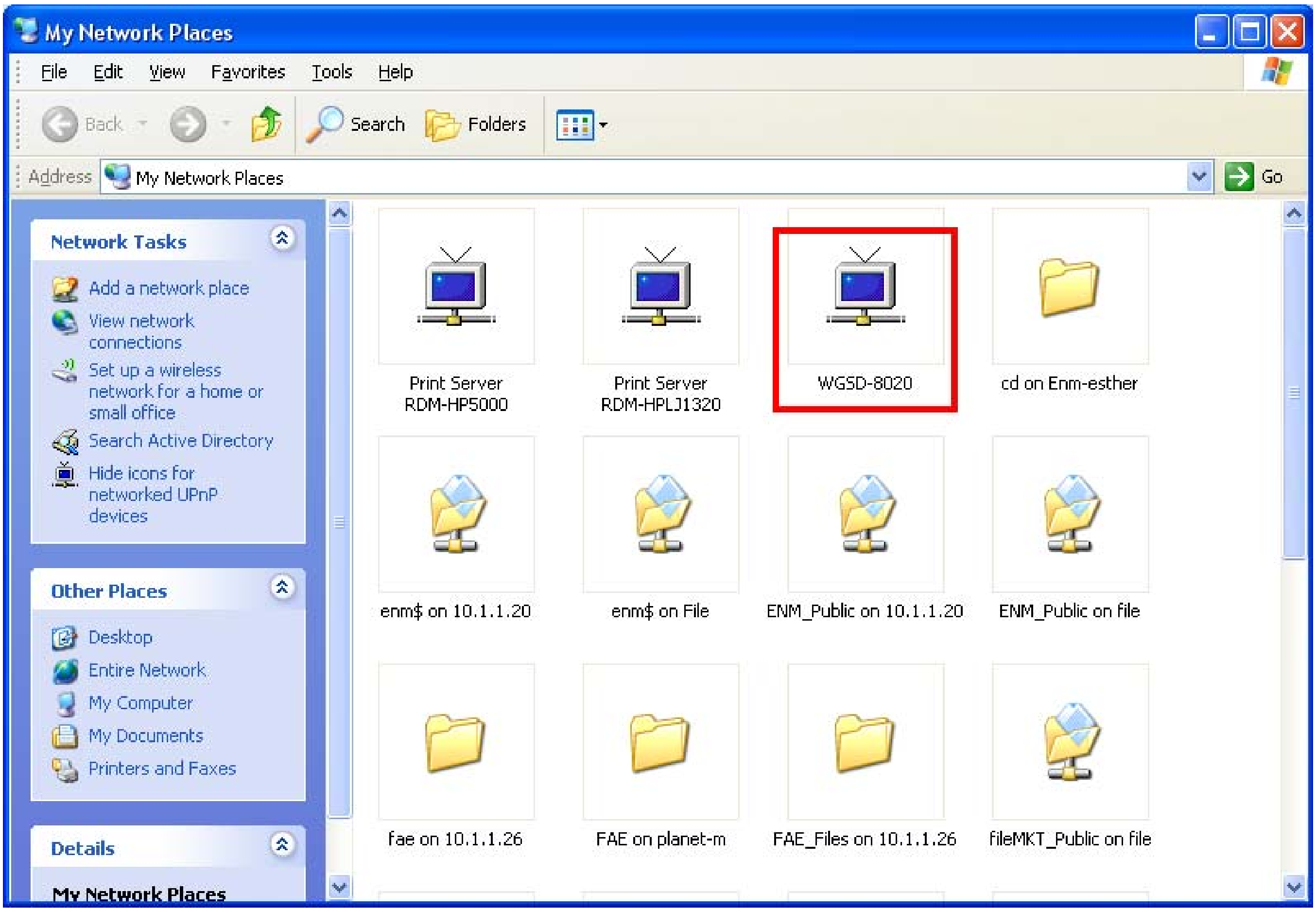


Figure 4-2-10 UPnP devices shows on Windows My Network Places

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.

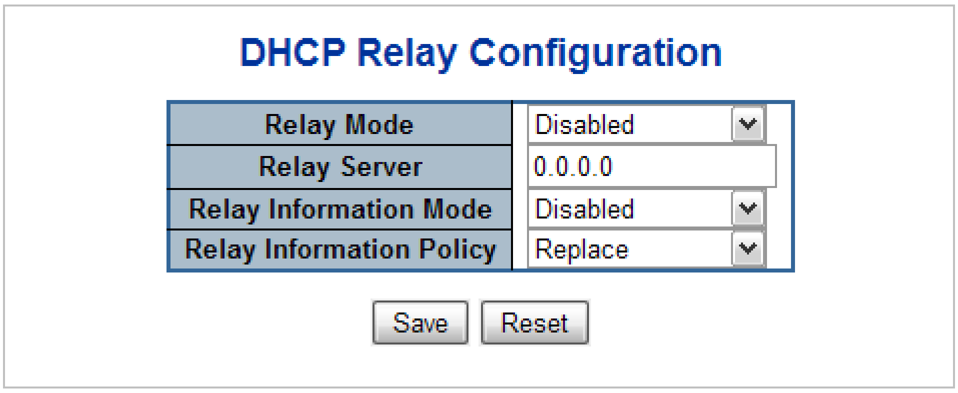
The **DHCP option 82** enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use 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.



DHCP Relay Configuration

Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Replace

Figure 4-2-11 DHCP Relay Configuration page screenshot

The page includes the following fields:

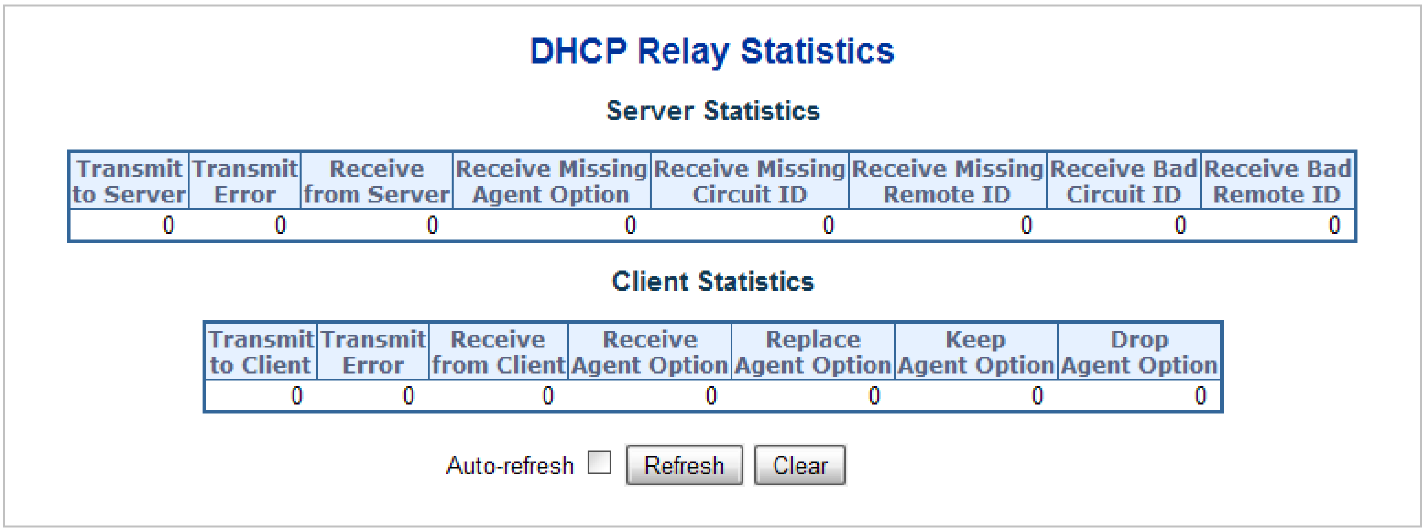
Object	Description
• **Relay Mode**	Indicates the DHCP relay mode operation. Possible modes are: ■ **Enabled**: Enable DHCP relay mode operation. When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet 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 remote 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.

Server Statistics



DHCP Relay Statistics

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Auto-refresh □ Refresh Clear

Figure 4-2-12 DHCP Relay Statistics page screenshot

The page includes the following fields:

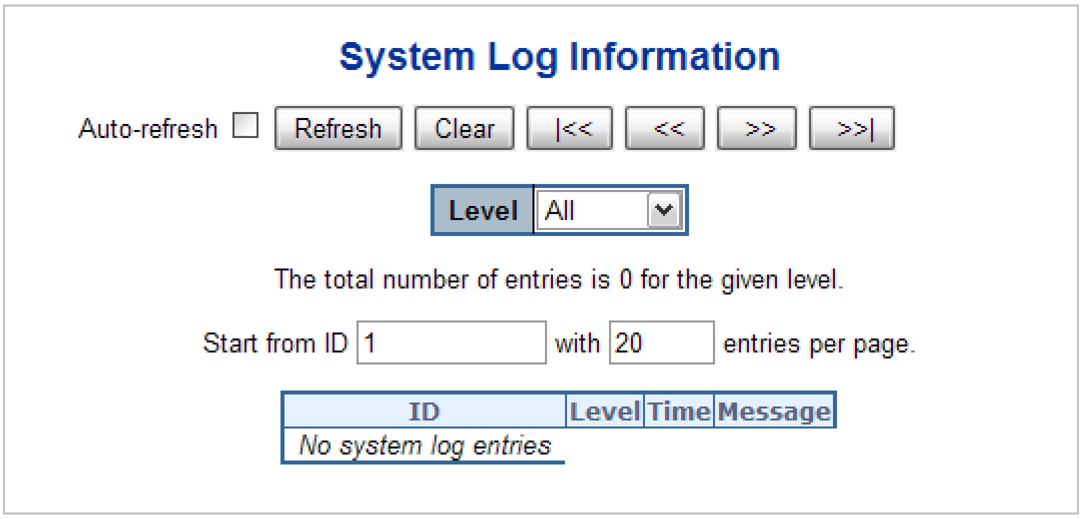
Object	Description
• **Transmit to Server**	The packets number that relayed from client to server.
• **Transmit Error**	The packets number that errors sending packets to clients.
• **Receive from Server**	The packets number that received packets from server.
• **Receive Missing Agent Option**	The packets 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**	The packets number that error sending packets to servers.
• **Receive from 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 Option**	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.

4.2.10 System Log

The switch system log information is provided here.



System Log Information

Auto-refresh □ Refresh Clear |<< << >> >>|

Level: All

The total number of entries is 0 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
No system log entries			

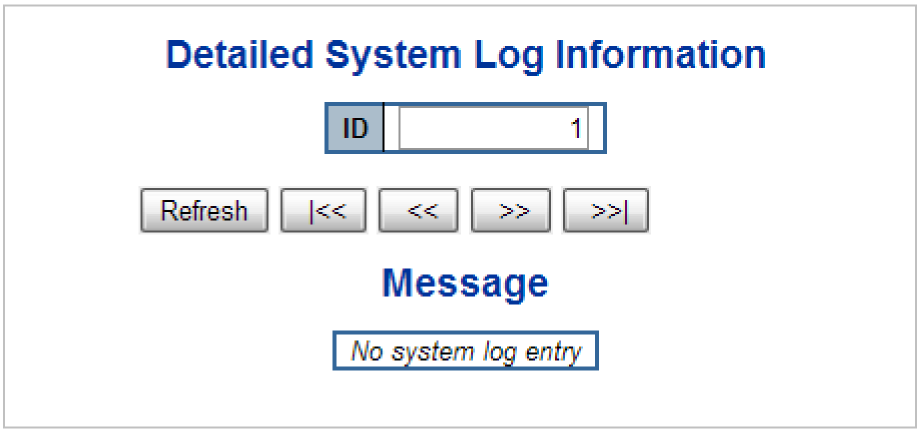
Figure 4-2-13 System Log Information page screenshot

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.
Refresh	Updates the system log entries, starting from the current entry ID.
Clear	Flushes all system log entries.
|<<	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.

4.2.11 Detailed Log

The switch system detailed log information is provided here.



No system log entry

Figure 4-2-14 Detailed System Log Information page screenshot

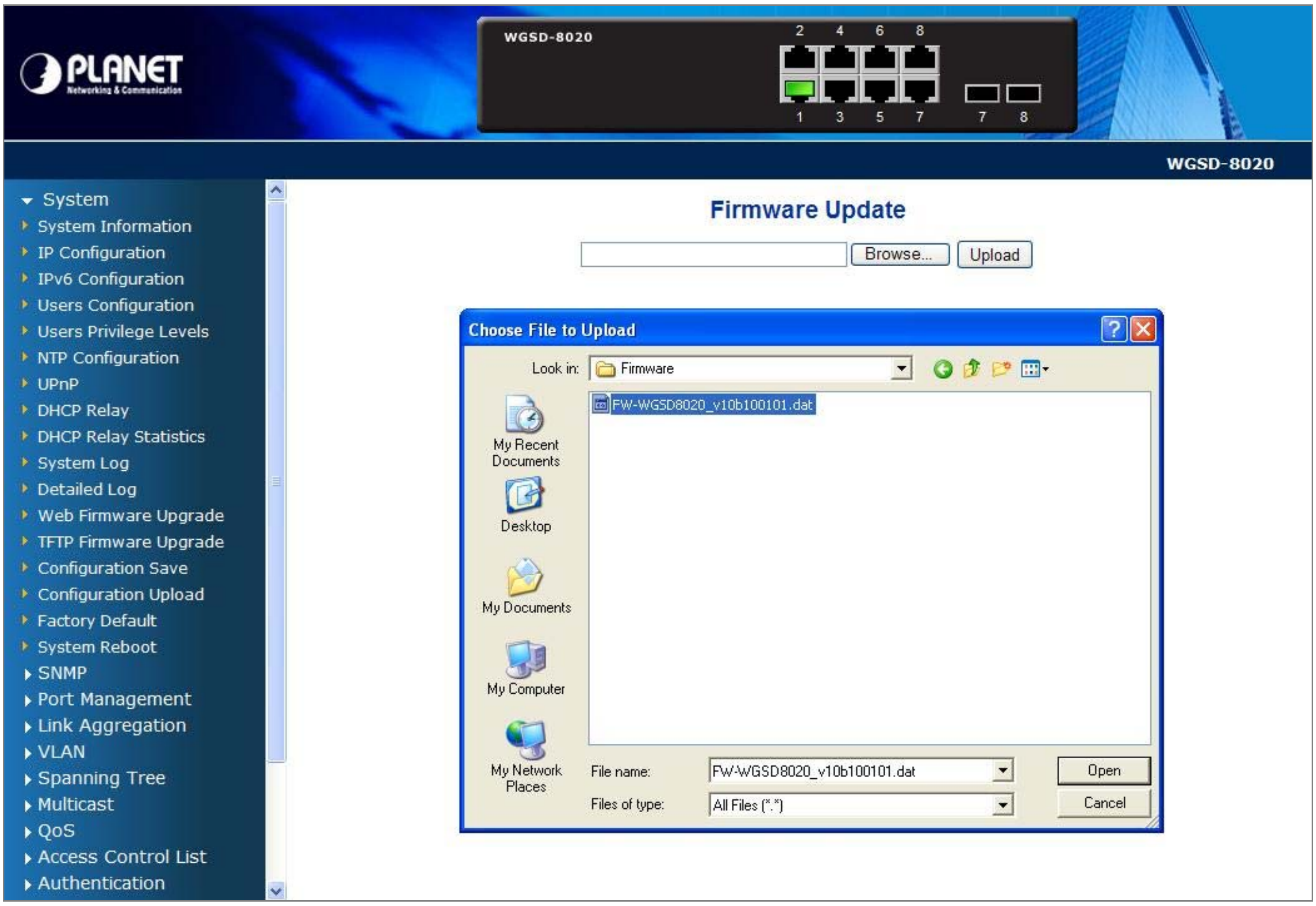
The page includes the following fields:

Object	Description
• **ID**	The ID (>= 1) of the system log entry.
• **Messages**	The detailed messages of the system log entry.
Refresh	Updates the system log entry to the current entry ID.
|<<	Updates the system log entry to the first available entry ID.
<<	Updates the system log entry to the previous available entry ID.
>>	Updates the system log entry to the next available entry ID.
>>|	Updates the system log entry to the last available entry ID.

4.2.12 WEB Firmware Upgrade

This page facilitates an update of the firmware controlling the switch.

The **Web Firmware Upgrade** page contains fields for downloading system image files from the Local File browser to the device. The Web Firmware Upgrade screen in Figure 4-2-15 appears.



Look in: Firmware

FW-WGSD8020_v10b100101.dat

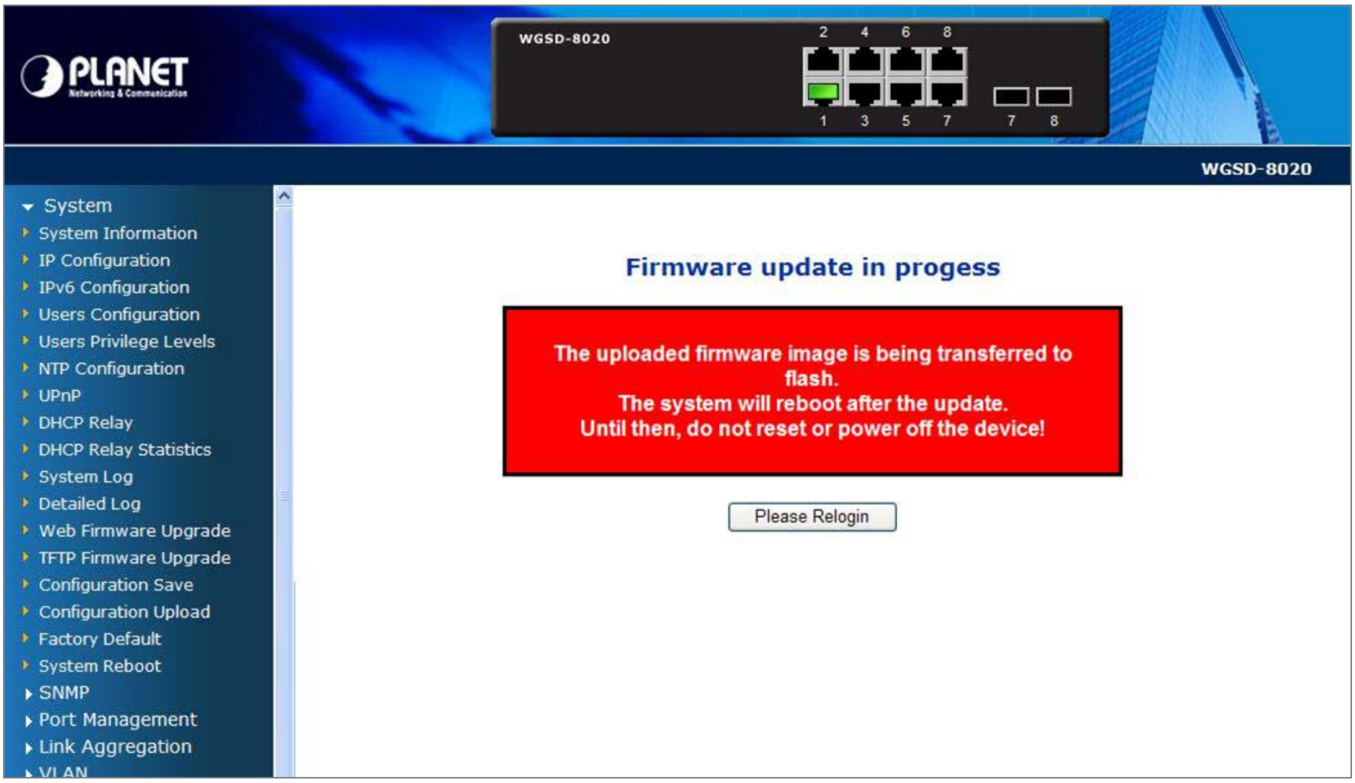
File name: FW-WGSD8020_v10b100101.dat

Files of type: All Files (*.*)

Figure 4-2-15 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 4-2-15.
3. Click the "**Browse**" button of the main page, the system would pop up the file selection menu to choose firmware.
4. Select on the firmware then click "**Upload**", the **Software Upload Progress** would show the file upload status.
5. Once the software be loaded to the system successfully. The following screen appears. Click the "**Please Relogin**" button to activate the new software immediately. The system will load the new software after reboot.



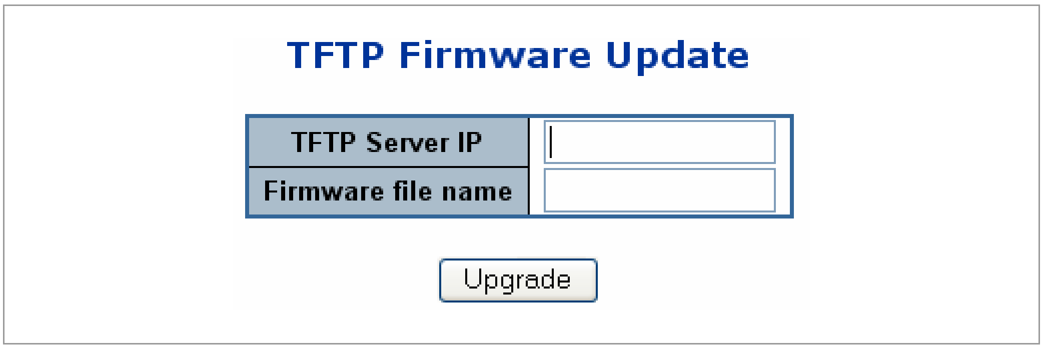
Firmware update in progess

The uploaded firmware image is being transferred to flash.
The system will reboot after the update.
Until then, do not reset or power off the device!

Figure 4-2-16 Software successfully loaded notice screen

4.2.13 TFTP Firmware Upgrade

The **Firmware Upgrade** page provides the functions to allow a user to update the Managed Switch firmware from the TFTP server in the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. The screen in Figure 4-2-17 appears.



TFTP Firmware Update

TFTP Server IP	
Firmware file name	

Figure 4-2-17 TFTP Firmware Update page screenshot

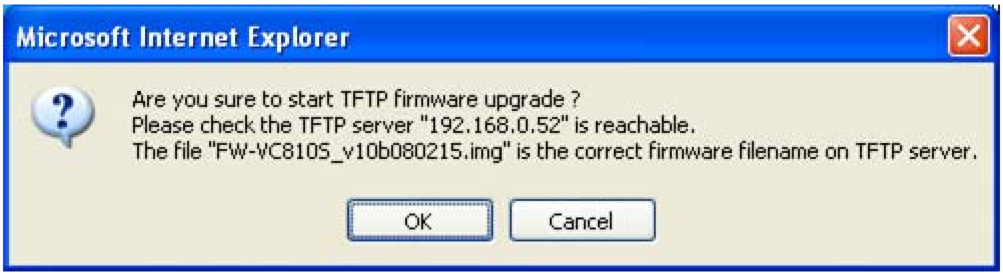
The page includes the following fields:

Object	Description
• **TFTP Server IP**	Fill in your TFTP server IP address.
• **Filename**	The name of firmware image.

	(Maximum length : 24 characters)
• **Upgrade button**	Press the button for upgrade the switch firmware.

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

1. Click **System** -> **TFTP Firmware Upgrade**.
2. The Firmware Upgrade screen is displayed as in Figure 4-2-18.
3. Fill in the **TFTP server IP Address** and the **firmware file name**, click the "**Upgrade**" button of the main page, the system would pop up the confirm message

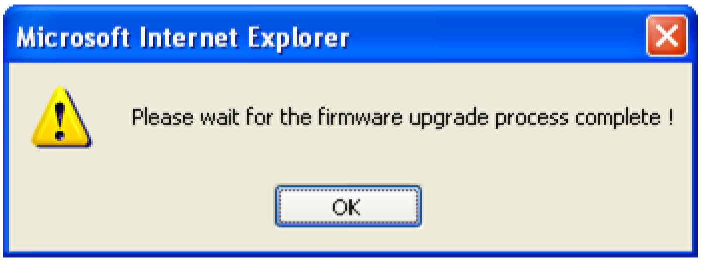


Microsoft Internet Explorer

Are you sure to start TFTP firmware upgrade ?
Please check the TFTP server "192.168.0.52" is reachable.
The file "FW-VC810S_v10b080215.img" is the correct firmware filename on TFTP server.

Figure 4-2-18 TFTP Firmware upgrade pop-up message

4. Click "**OK**", the Managed Switch will start the TFTP upgrade procedure.
5. Please check your TFTP server application to confirm the TFTP file is well transmit to the Managed Switch.



Microsoft Internet Explorer

Please wait for the firmware upgrade process complete !

Figure 4-2-19 Firmware Upgrade pop-up message

6. The Managed Switch will reboot then, and It will cost 2 to 3 minutes for the TFTP firmware upgrade and reboot procedure. Please wait for the process complete.
7. Once the new software is loaded to the system successfully, the Login screen appears. Enter the user name and password to login the Managed Switch.

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

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 Configuration Save

This function allows backup and reload the current configuration of the Managed Switch to the local management station. The screen in Figure 4-2-20 appears.

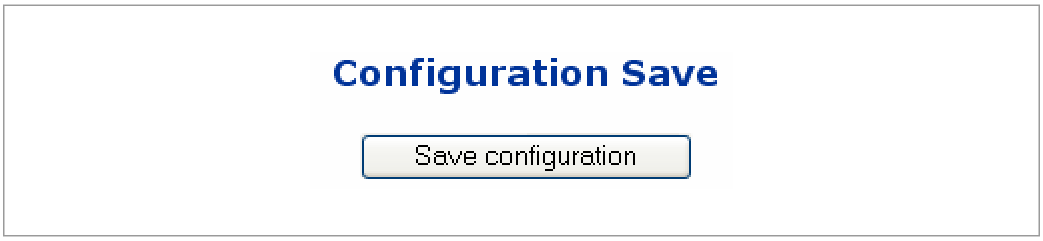


Figure 4-2-20 Configuration Save page screenshot

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

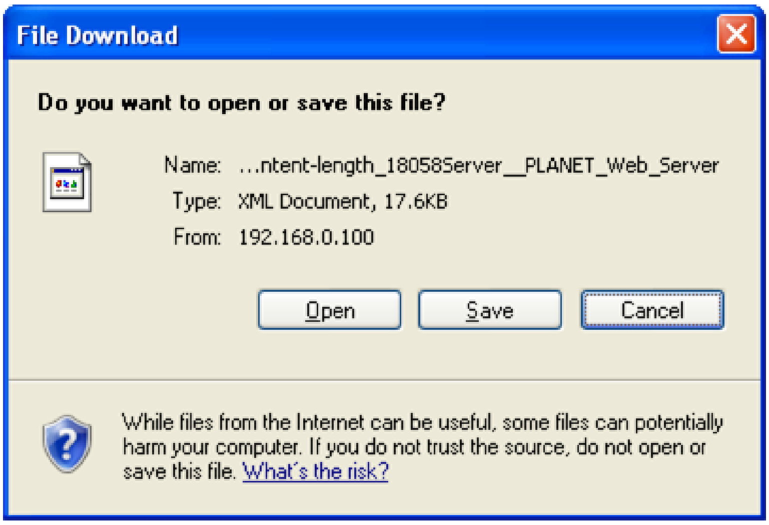
Header tags:	<?xml version="1.0"?> and <configuration>. These tags are mandatory and must be present at the beginning of the file.
Section tags:	<platform>, <global> and <switch>. The platform section must be the first section tag and this section must include the correct platform ID and version. The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

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

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

- **Save Configuration**

1. Press the **"Save Configuration"** button to save the current configuration in manager workstation. The following screens in Figure 4-2-21 and 4-2-22 appear



Do you want to open or save this file?

Name: ...ntent-length_18058Server__PLANET_Web_Server

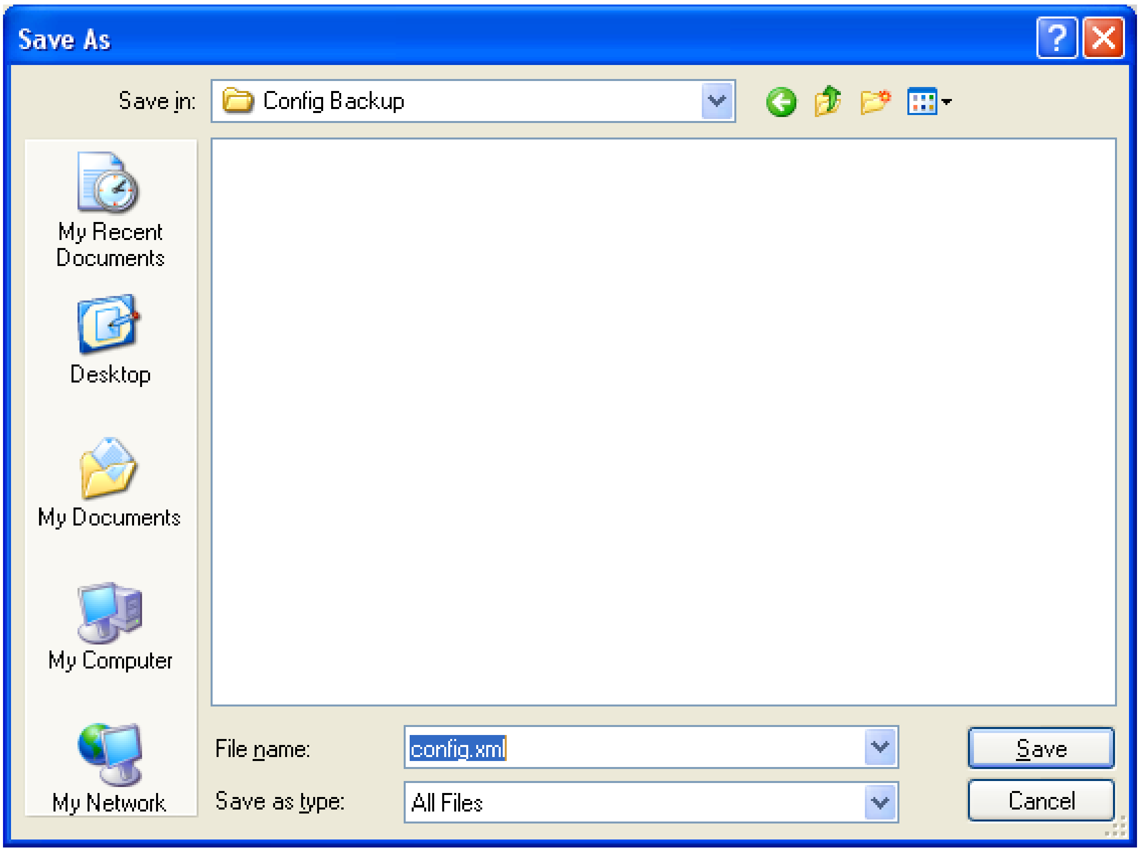
Type: XML Document, 17.6KB

From: 192.168.0.100

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

Figure 4-2-21 File Download screen

2. Chose the file save path in management workstation.



Save in: Config Backup

File name: config.xml

Save as type: All Files

Figure 4-2-22 File save screen

4.2.15 Configuration Upload

This function allows backup and reload the current configuration of the Managed Switch to the local management station. The screen in Figure 4-2-23 appears.

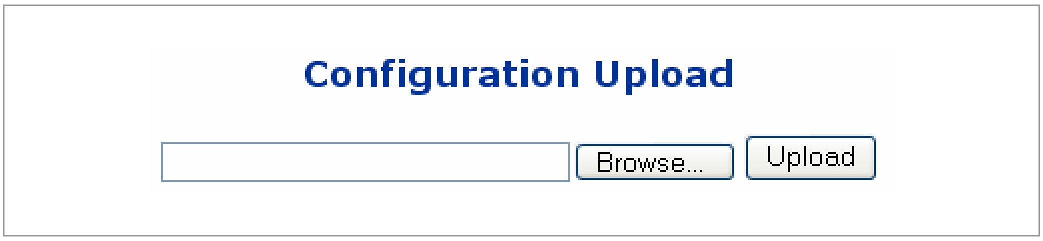


Figure 4-2-23 Configuration Upload page screenshot

- **Configuration Upload**

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

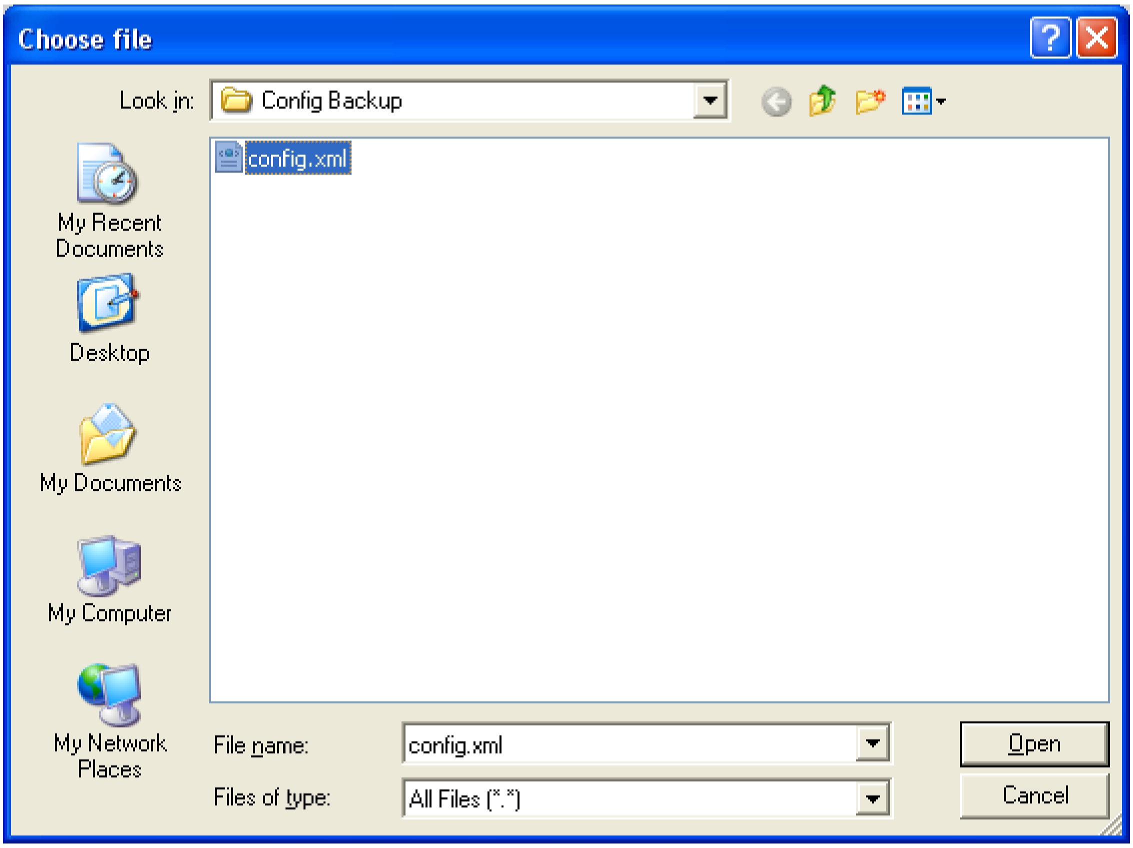


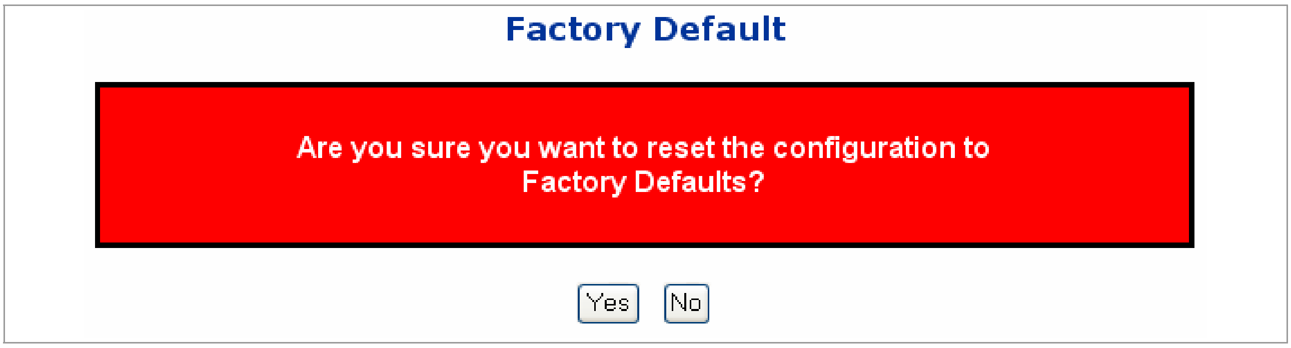
Figure 4-2-24 Windows file selection menu popup

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**".

4.2.16 Factory Default

The Factory Reset button can reset the Managed Switch back to the factory default mode. Be aware that the entire configuration will be reset; only the IP address of the Managed Switch is retained. Once the Factory Reset item is pressed, the screen in Figure 4-2-25 appears.



Factory Default

Are you sure you want to reset the configuration to Factory Defaults?

Figure 4-2-25 Factory Default page screenshot

The new configuration is available immediately, which means that no reboot is necessary.

Yes: Click to reset the configuration to Factory Defaults.

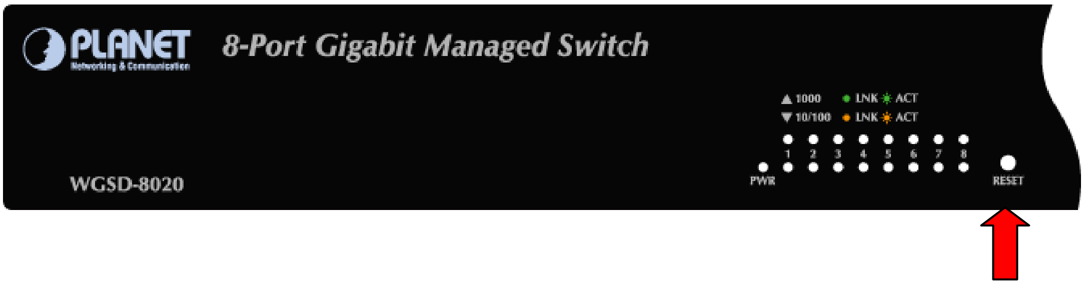
No: Click to return to the Port State page without resetting the configuration.

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.

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.

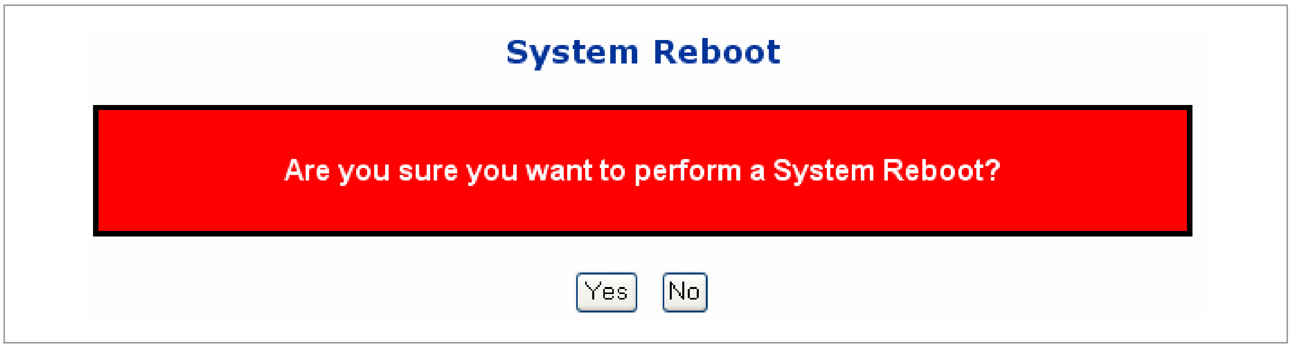
Note



Hardware Reset button

4.2.17 System Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user have to re-login the WEB interface about 60 seconds later, the screen in Figure 4-2-26 appears.



System Reboot

Are you sure you want to perform a System Reboot?

Figure 4-2-26 System Reboot page screenshot

Yes : Click to reboot device.

No : Click to return to the Welcome page without rebooting.

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

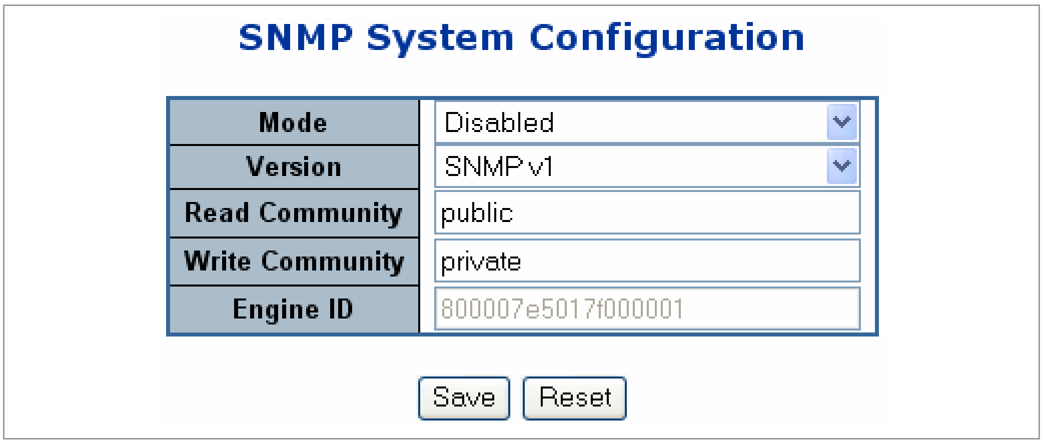
An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations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



SNMP System Configuration

Mode	Disabled
Version	SNMP v1
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Figure 4-3-1 SNMP System Configuration page screenshot

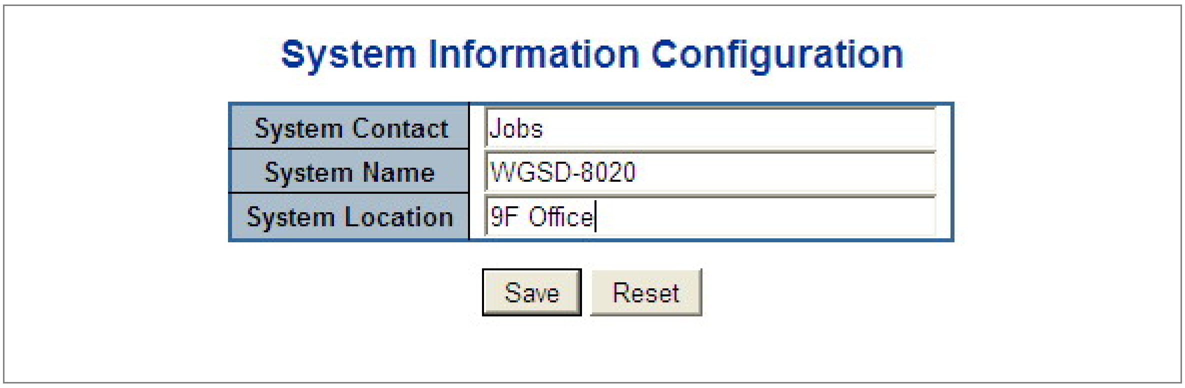
The page includes the following fields:

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.

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.



System Information Configuration

System Contact	Jobs
System Name	WGSD-8020
System Location	9F Office

Figure 4-3-2 System Information Configuration page screenshot

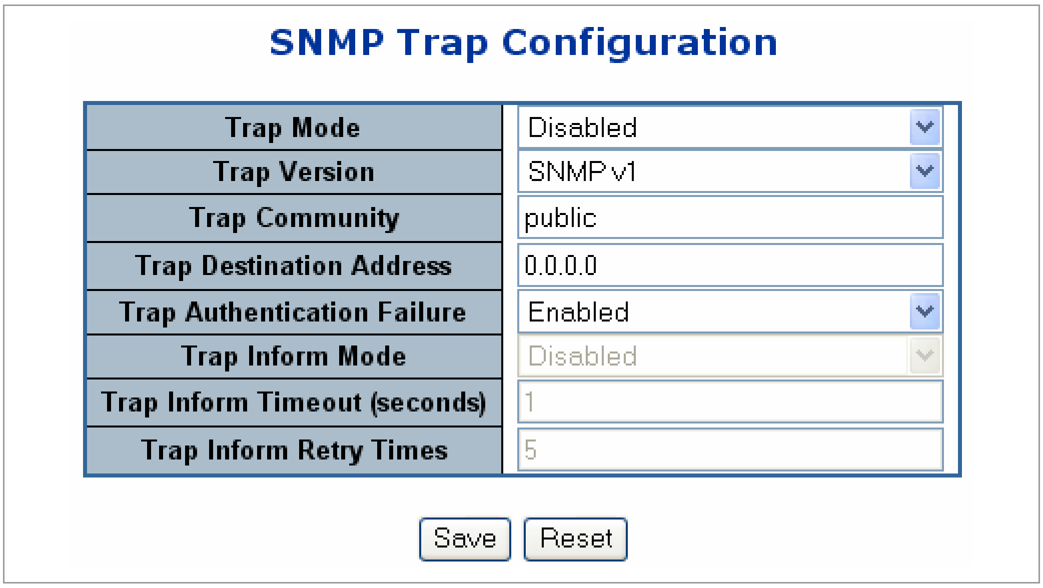
The page includes the following fields:

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

4.3.4 SNMP Trap Configuration

Configure SNMP trap on this page.

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



SNMP Trap Configuration

Trap Mode	Disabled
Trap Version	SNMP v1
Trap Community	public
Trap Destination Address	0.0.0.0
Trap Authentication Failure	Enabled
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

Figure 4-3-3 SNMP Trap Configuration page screenshot

The page includes the following fields:

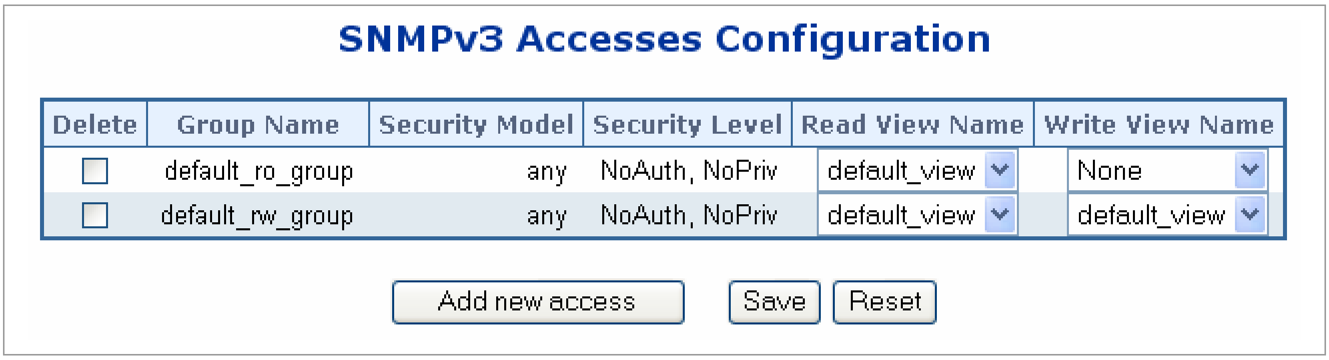
Object	Description
• **Trap Mode**	Indicates the SNMP trap mode operation. Possible modes are: ■ **Enabled**: Enable SNMP trap mode operation. ■ **Disabled**: Disable SNMP trap mode operation.
• **Trap Version**	Indicates the SNMP trap supported version. Possible versions are: ■ **SNMP v1**: Set SNMP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

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

4.3.5 SNMPv3 Configuration

4.3.5.1 SNMPv3 Accesses Configuration

Configure SNMPv3 accesses table on this page. The entry index key are Group Name, Security Model and Security Level. The SNMPv3 Accesses Configuration screen in Figure 4-3-4 appears.



SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

Figure 4-3-4 SNMPv3 Accesses Configuration page screenshot

The page includes the following fields:

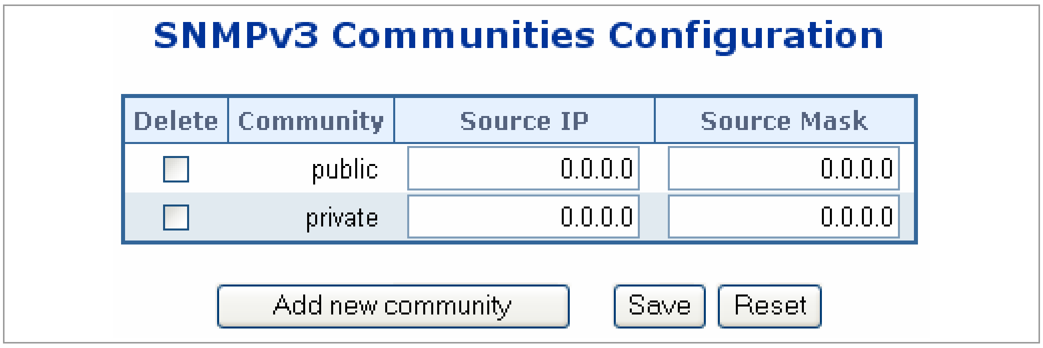
Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Security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

	The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

4.3.5.2 SNMPv3 Communities Configuration

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

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



SNMPv3 Communities Configuration

Delete	Community	Source IP	Source Mask
□	public	0.0.0.0	0.0.0.0
□	private	0.0.0.0	0.0.0.0

Figure 4-3-5 SNMPv3 Communities Configuration page screenshot

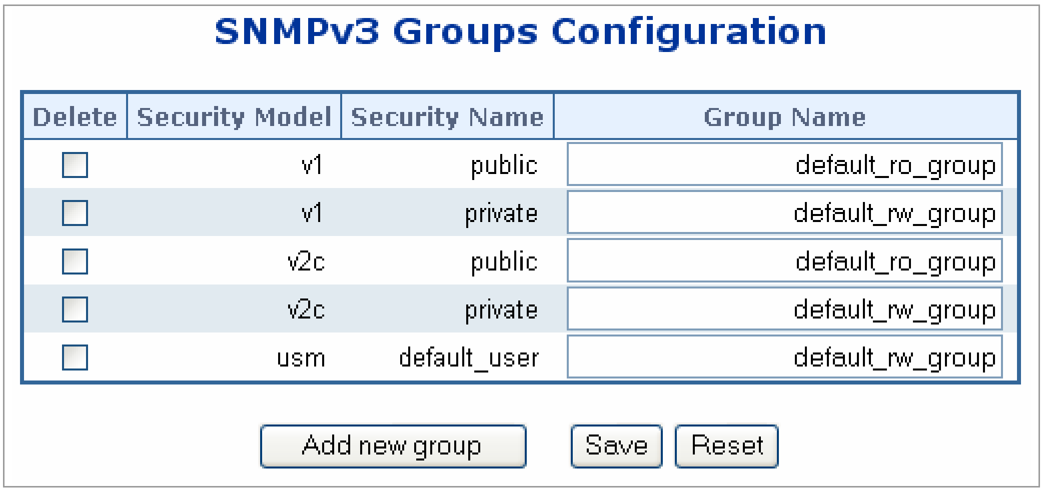
The page includes the following fields:

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

4.3.5.3 SNMPv3 Groups Configuration

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

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



SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group

Figure 4-3-6 SNMPv3 Groups Configuration page screenshot

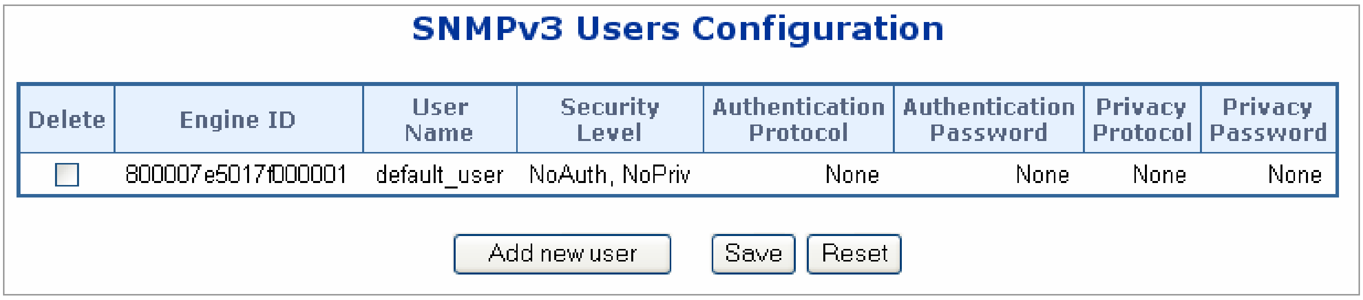
The page includes the following fields:

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

4.3.5.4 SNMPv3 Users Configuration

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

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



SNMPv3 Users Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Figure 4-3-7 SNMPv3 Users Configuration page screenshot

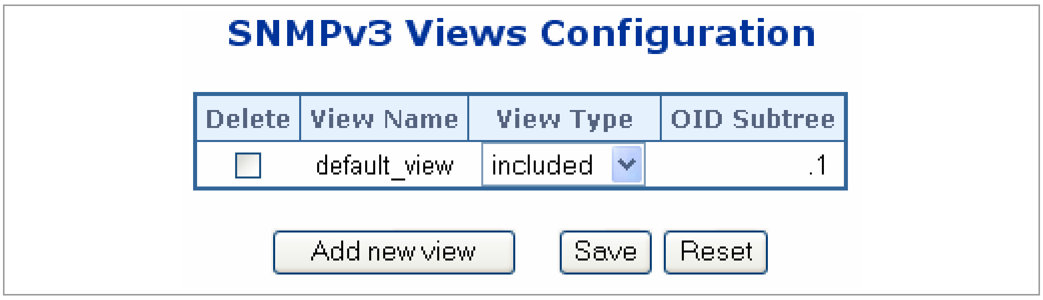
The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Engine ID**	A octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
• **User Name**	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are: ■ **NoAuth, NoPriv**: None authentication and none privacy. ■ **Auth, NoPriv**: Authentication and none privacy. ■ **Auth, Priv**: Authentication and privacy. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.
• **Authentication Protocol**	Indicates the authentication protocol that this entry should belong to. Possible authentication protocol are: ■ **None**: None authentication protocol. ■ **MD5**: An optional flag to indicate that this user using MD5 authentication protocol. ■ **SHA**: An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.
• **Authentication Password**	A string identifying the authentication pass phrase. • For MD5 authentication protocol, the allowed string length is 8 to 32. • For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.
• **Privacy Protocol**	Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are: ■ **None**: None privacy protocol. ■ **DES**: An optional flag to indicate that this user using DES authentication protocol.
• **Privacy Password**	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

4.3.5.5 SNMPv3 Views Configuration

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

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



SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included	.1

Figure 4-3-8 SNMPv3 Views Configuration page screenshot

The page includes the following fields:

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

4.4 Port Management

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

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

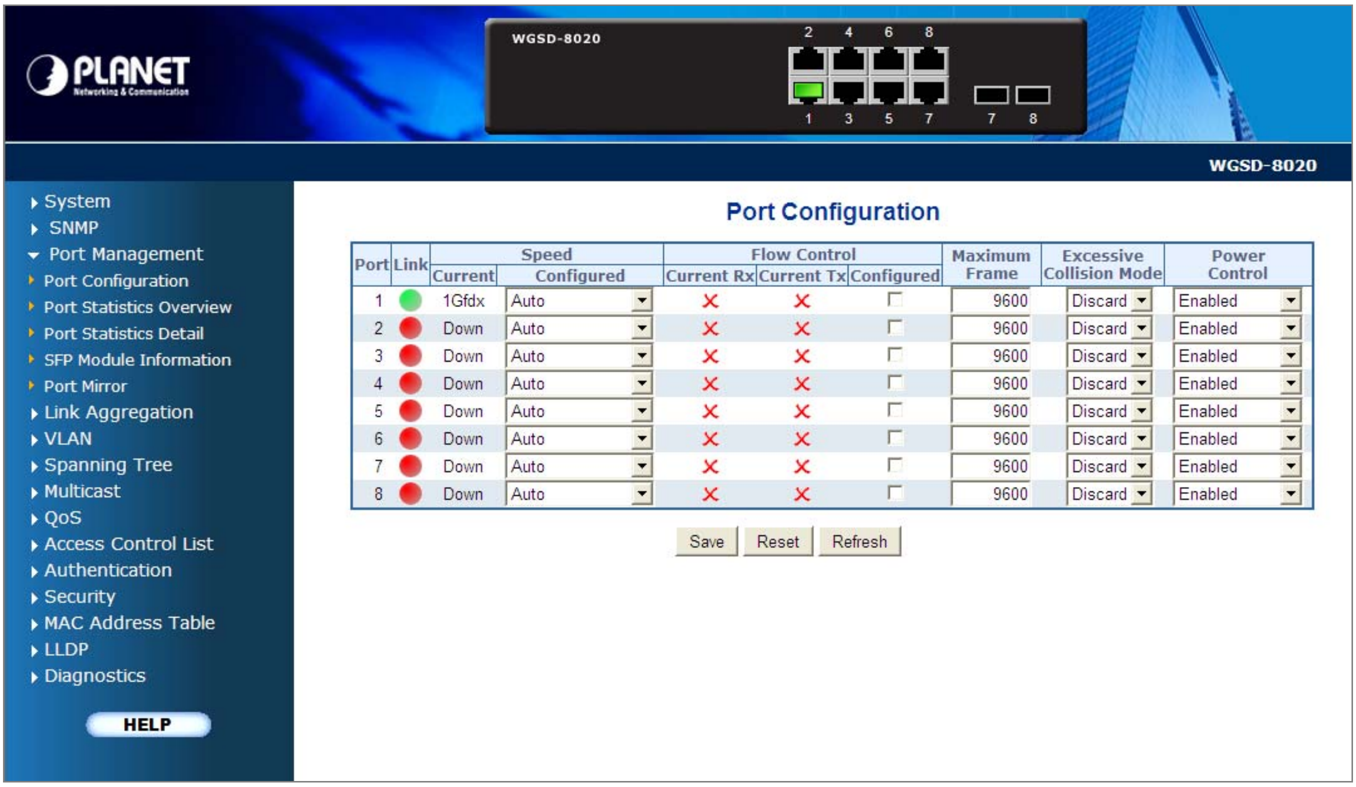
4.4.1 Port Configuration

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

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

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

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



Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
1	🟢	1Gfdx	Auto	✗	✗	□	9600	Discard	Enabled
2	🔴	Down	Auto	✗	✗	□	9600	Discard	Enabled
3	🔴	Down	Auto	✗	✗	□	9600	Discard	Enabled
4	🔴	Down	Auto	✗	✗	□	9600	Discard	Enabled
5	🔴	Down	Auto	✗	✗	□	9600	Discard	Enabled
6	🔴	Down	Auto	✗	✗	□	9600	Discard	Enabled
7	🔴	Down	Auto	✗	✗	□	9600	Discard	Enabled
8	🔴	Down	Auto	✗	✗	□	9600	Discard	Enabled

Figure 4-4-1 Port Configuration page screenshot

The page includes the following fields:

Object	Description
• **Port**	This is the logical port number for this row.
• **Link**	The current link state is displayed graphically. Green indicates the link is up and red that it is down.

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

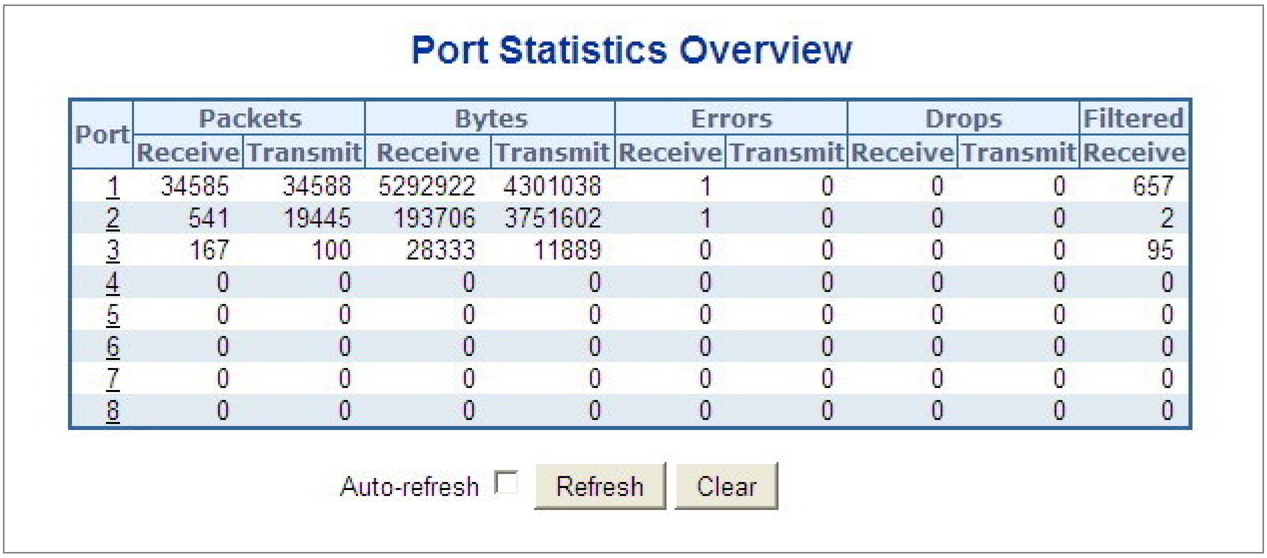
Note

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

4.4.2 Port Statistics Overview

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

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



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	34585	34588	5292922	4301038	1	0	0	0	657
2	541	19445	193706	3751602	1	0	0	0	2
3	167	100	28333	11889	0	0	0	0	95
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

Figure 4-4-2 Port Statistics Overview page screenshot

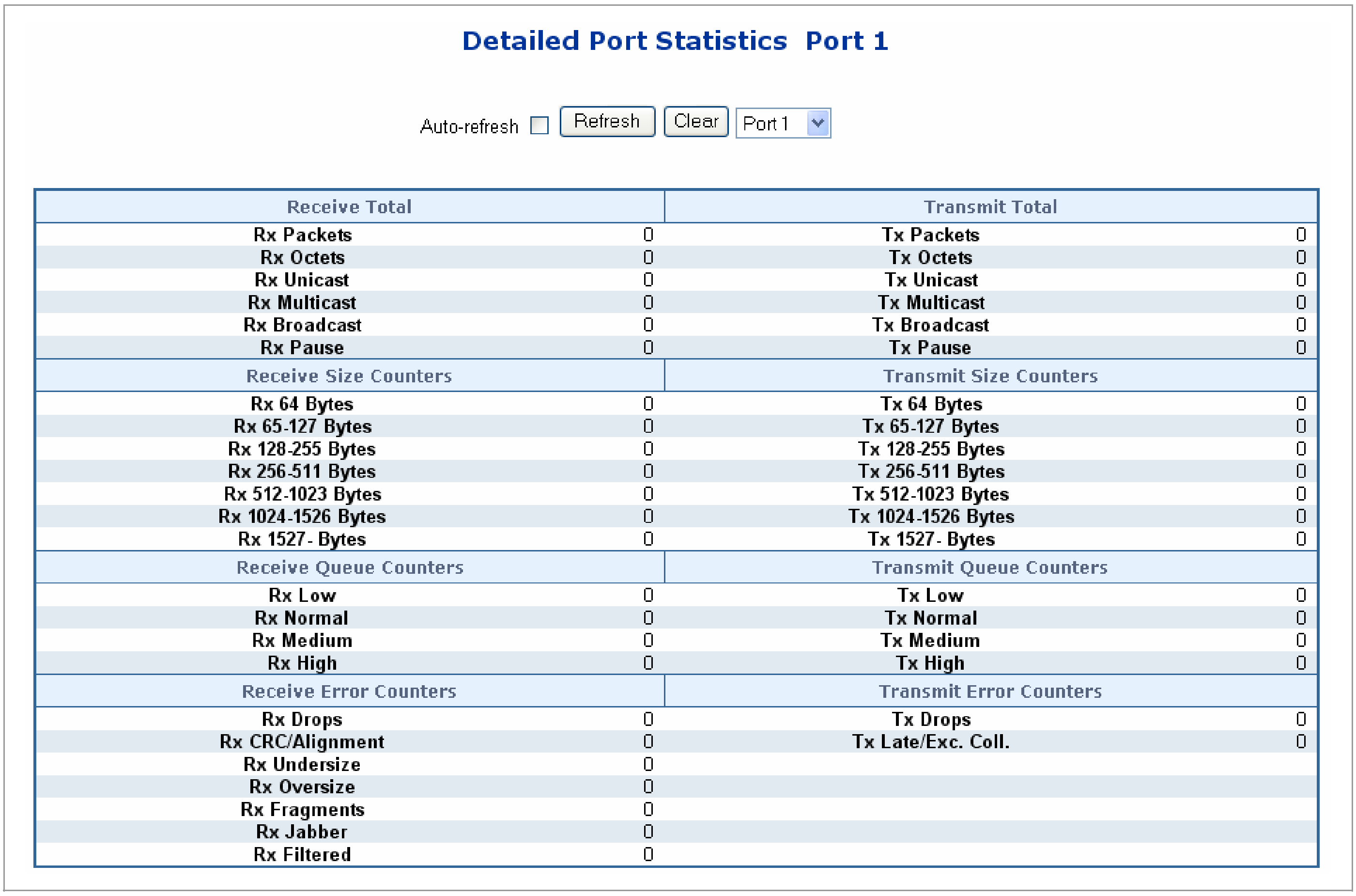
The displayed counters are:

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

4.4.3 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.



Detailed Port Statistics Port 1

Auto-refresh □ Refresh Clear Port 1

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Low	0	Tx Low	0
Rx Normal	0	Tx Normal	0
Rx Medium	0	Tx Medium	0
Rx High	0	Tx High	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

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

Receive Total and Transmit Total

The page includes the following fields:

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

The page includes the following fields:

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

The page includes the following fields:

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

4.4.4 Port Mirroring Configuration

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

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

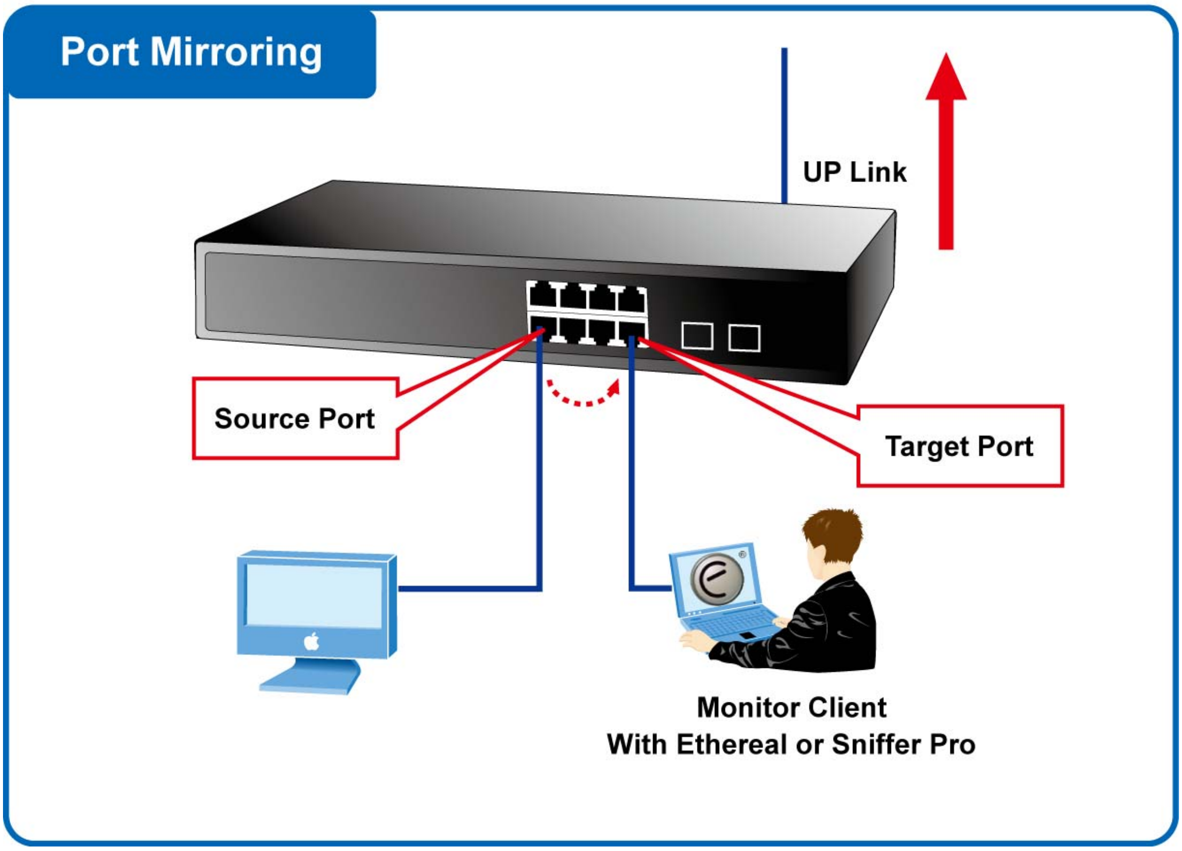


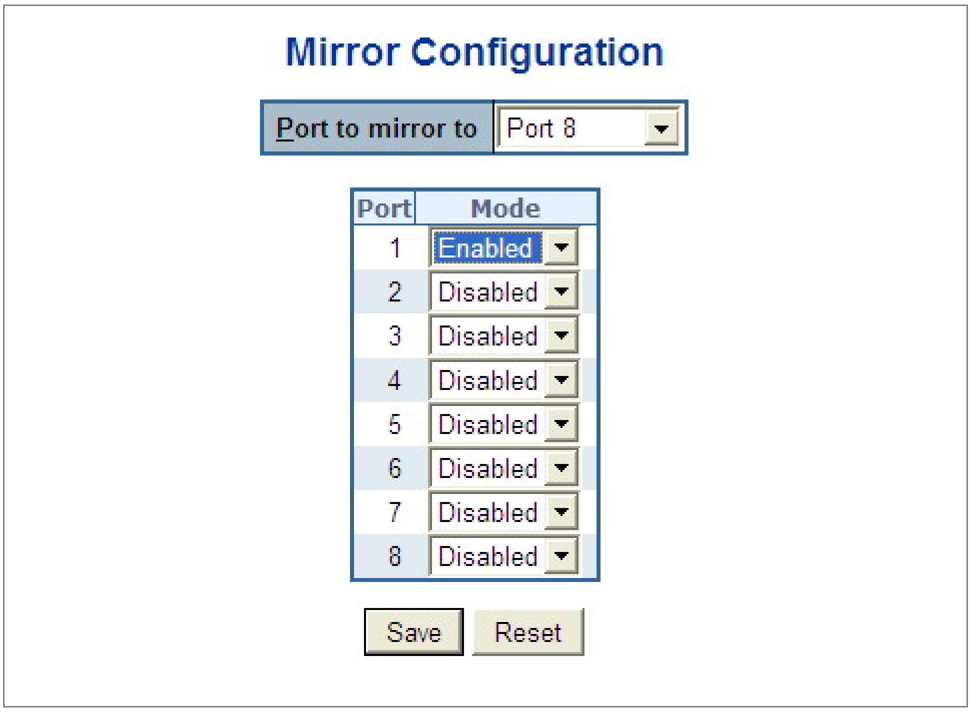
Figure 4-4-4 Port Mirror application

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

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

Mirror Port Configuration

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



Mirror Configuration

Port to mirror to: Port 8

Port	Mode
1	Enabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

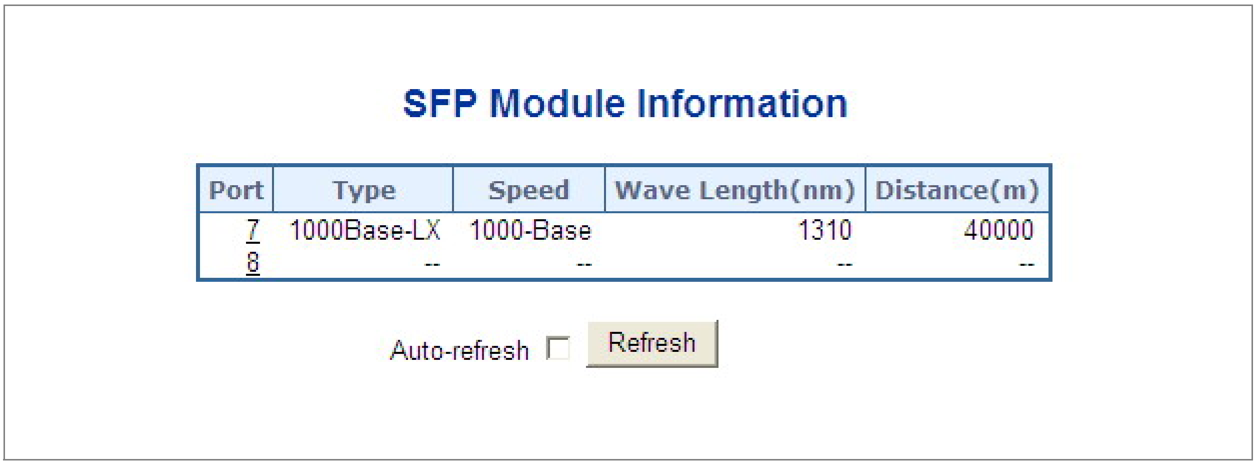
Figure 4-4-5 Port Mirror Configuration page screenshot

The page includes the following fields:

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

4.4.5 SFP Module Information

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



SFP Module Information

Port	Type	Speed	Wave Length(nm)	Distance(m)
7	1000Base-LX	1000-Base	1310	40000
8	--	--	--	--

Figure 4-4-6 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.

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.

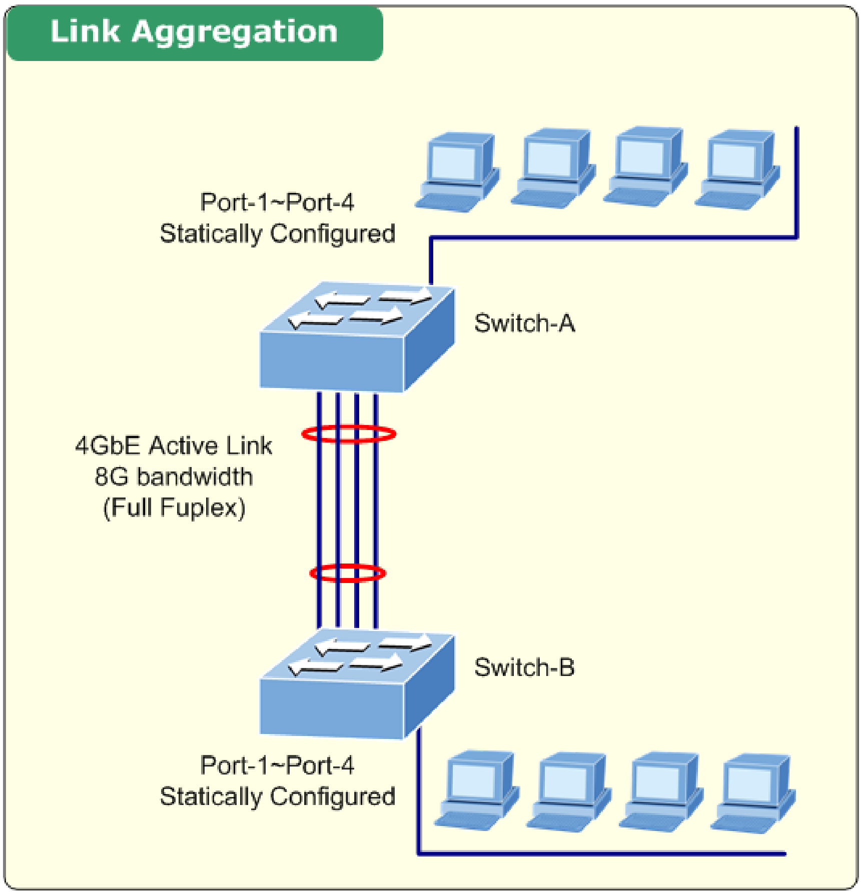


Figure 4-5-1 Link Aggregation

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 Managed Switch supports the following Aggregation links :

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

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 4 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:

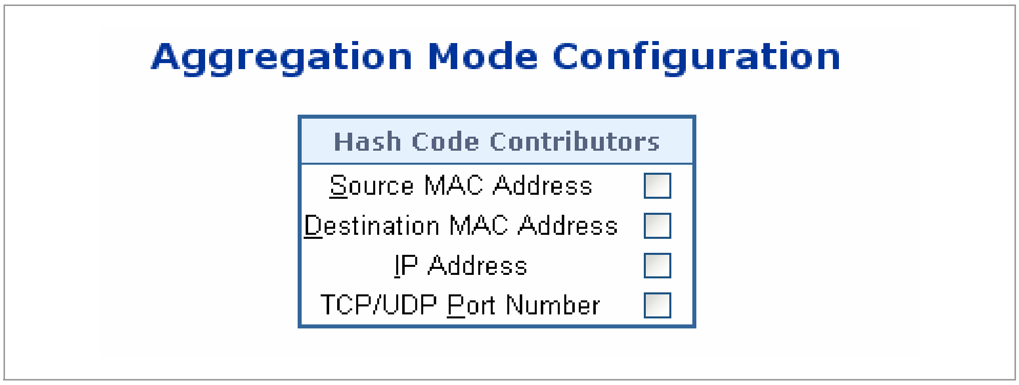
- **Source MAC**
- **Destination MAC**
- **Source and destination IPv4 address.**
- **Source and destination TCP/UDP ports for IPv4 packets**

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



Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	□
Destination MAC Address	□
IP Address	□
TCP/UDP Port Number	□

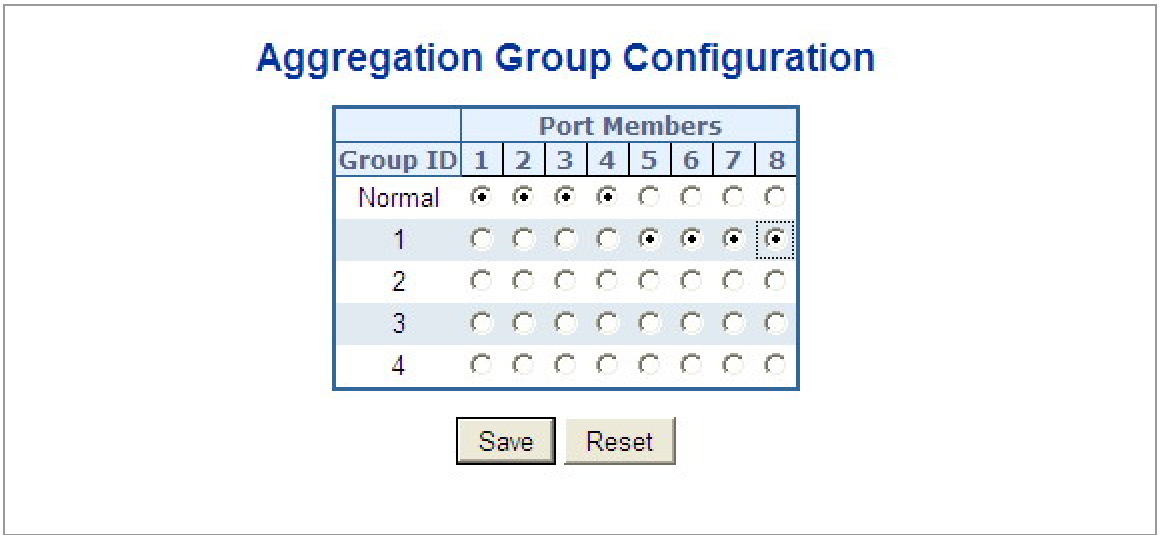
Figure 4-5-2 Aggregation Mode Configuration page screenshot

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.



Aggregation Group Configuration

	Port Members							
Group ID	1	2	3	4	5	6	7	8
Normal	●	●	●	●	○	○	○	○
1	○	○	○	○	●	●	●	●
2	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○

Figure 4-5-3 Aggregation Group Configuration page screenshot

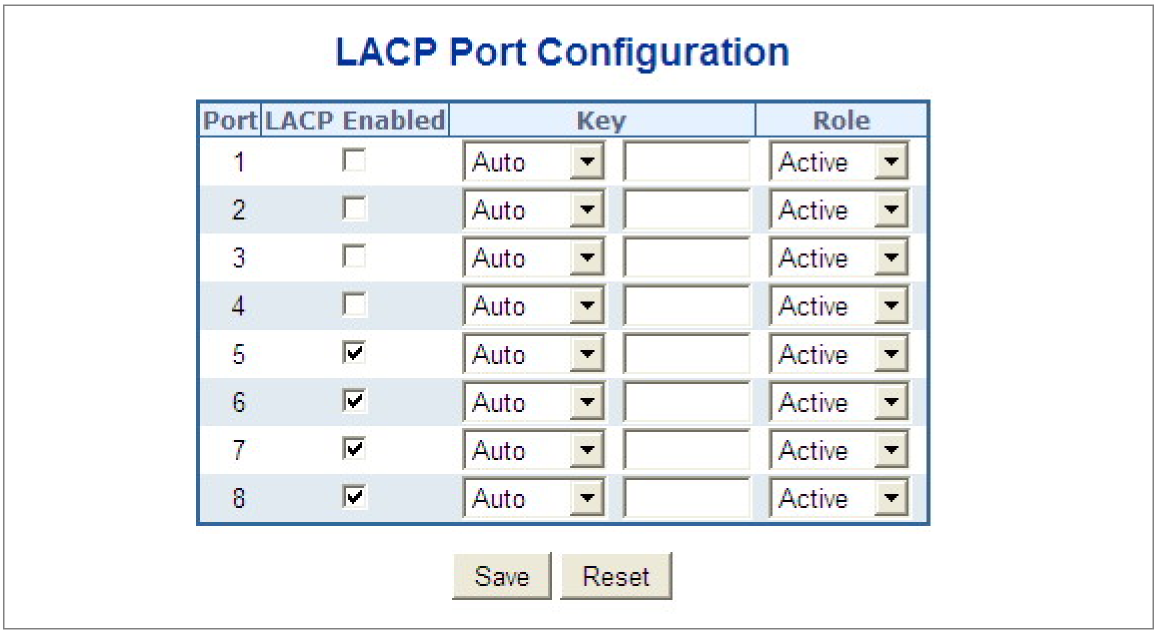
The page includes the following fields:

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

4.5.2 LACP Configuration

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

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



LACP Port Configuration

Port	LACP Enabled	Key		Role
1	□	Auto		Active
2	□	Auto		Active
3	□	Auto		Active
4	□	Auto		Active
5	☑	Auto		Active
6	☑	Auto		Active
7	☑	Auto		Active
8	☑	Auto		Active

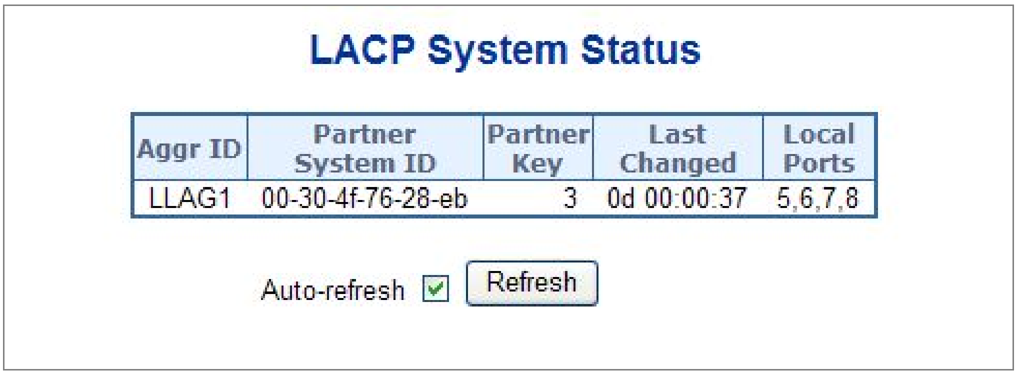
Figure 4-5-4 LACP Port Configuration page screenshot

The page includes the following fields:

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

4.5.3 LACP System Status

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



LACP System Status

Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
LLAG1	00-30-4f-76-28-eb	3	0d 00:00:37	5,6,7,8

Auto-refresh ☑ Refresh

Figure 4-5-5 LACP System Status page screenshot

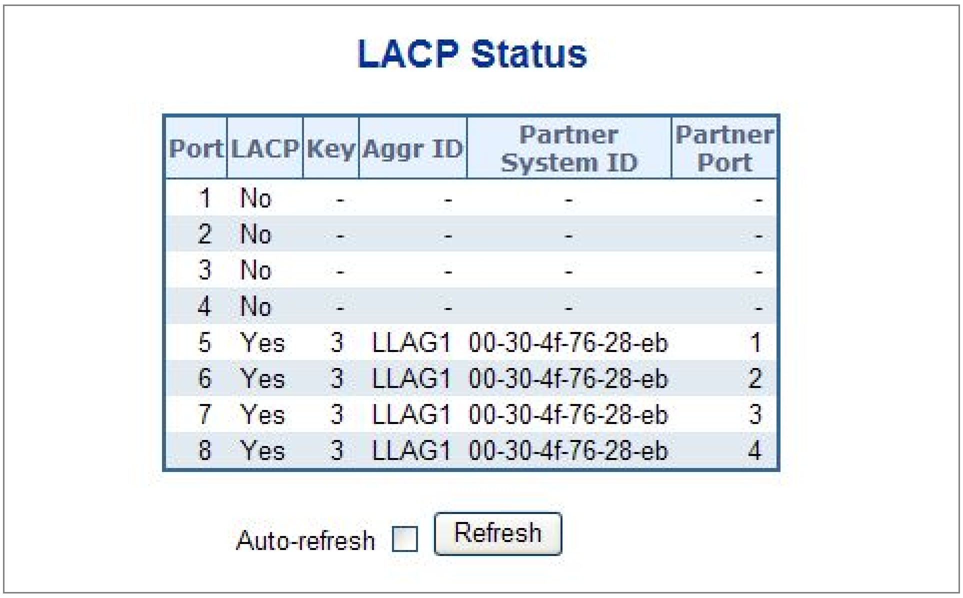
The page includes the following fields:

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. The format is: "Port".

4.5.4 LACP Port Status

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

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



LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	Yes	3	LLAG1	00-30-4f-76-28-eb	1
6	Yes	3	LLAG1	00-30-4f-76-28-eb	2
7	Yes	3	LLAG1	00-30-4f-76-28-eb	3
8	Yes	3	LLAG1	00-30-4f-76-28-eb	4

Figure 4-5-6 LACP Port Status page screenshot

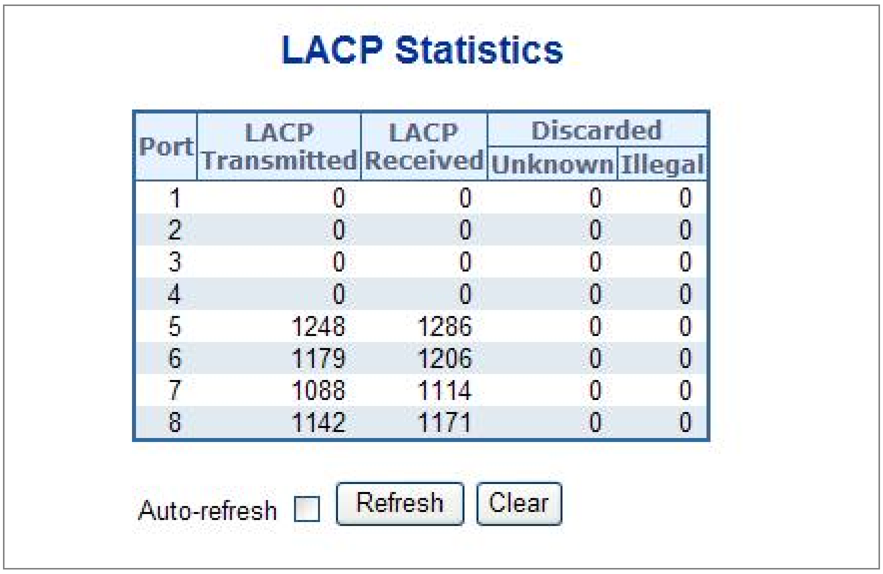
The page includes the following fields:

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

4.5.5 LACP statistics

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

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



LACP Statistics

Port	LACP Transmitted	LACP Received	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	1248	1286	0	0
6	1179	1206	0	0
7	1088	1114	0	0
8	1142	1171	0	0

Figure 4-5-7 LACP Port statistics page screenshot

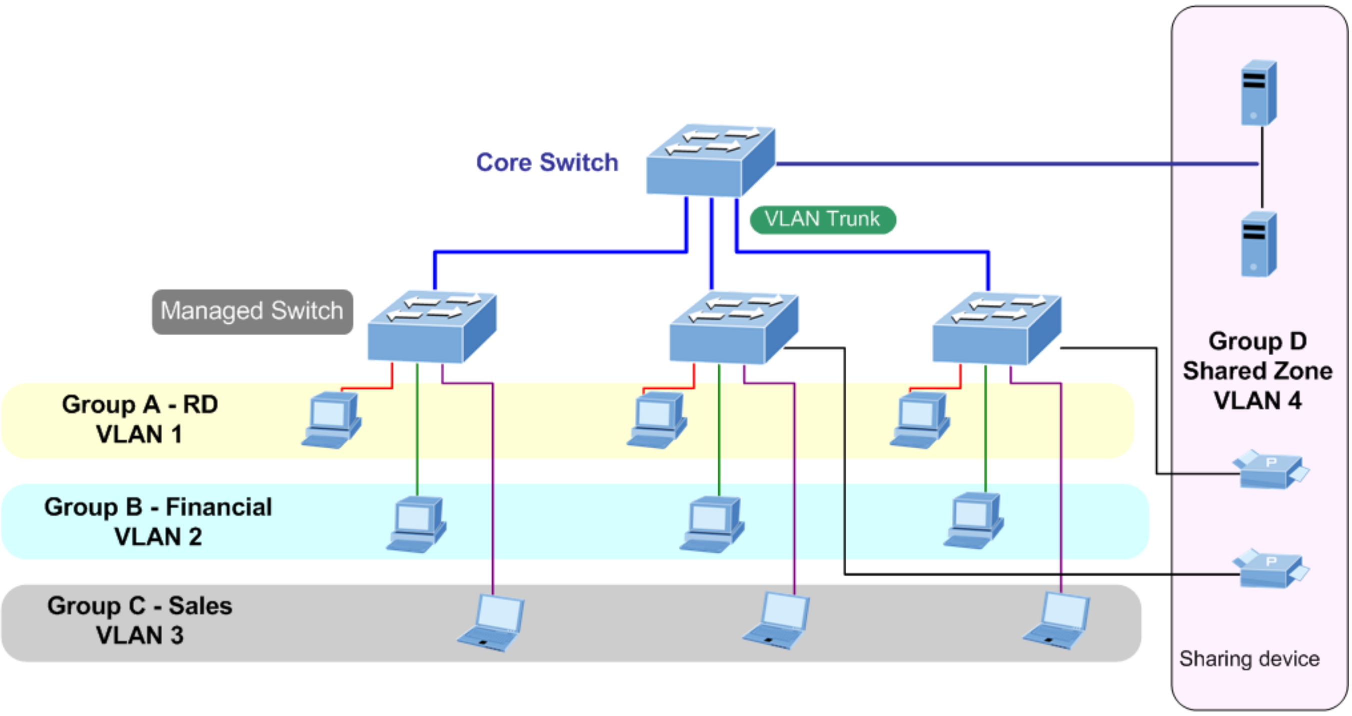
The page includes the following fields:

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

4.6 VLAN

4.6.1 VLAN Overview

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



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

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

Note

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

This section has the following items:

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

4.6.2 IEEE 802.1Q VLAN

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

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

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

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

This Managed Switch supports the following VLAN features:

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

IEEE 802.1Q Standard

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

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

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

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

Some relevant terms:

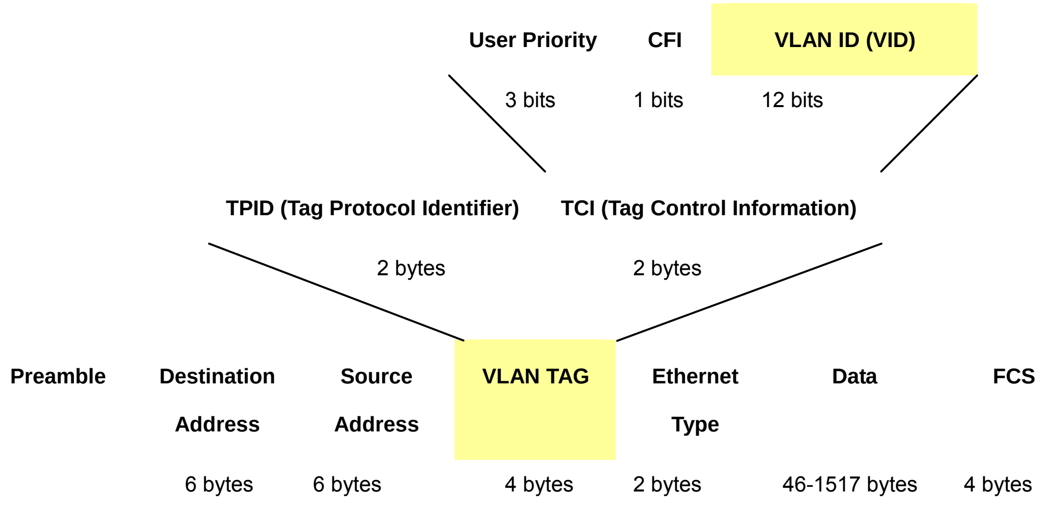
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN Tags

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

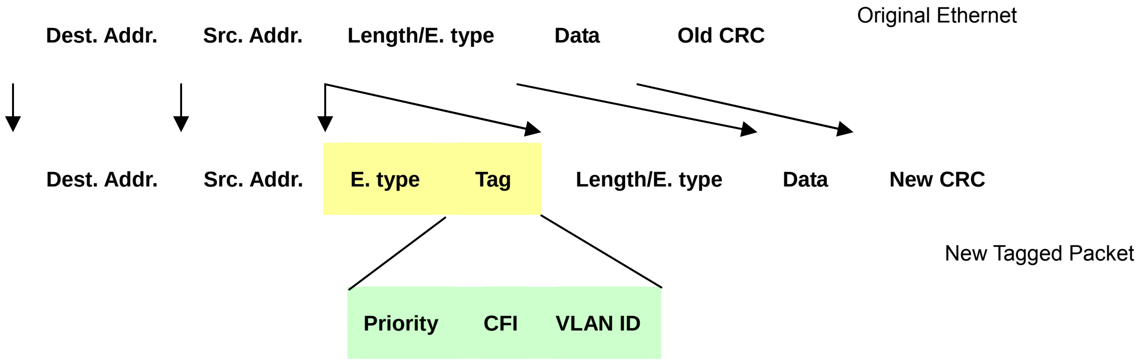
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



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

Adding an IEEE802.1Q Tag



Port VLAN ID

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

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

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

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

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

Default VLANs

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

Assigning Ports to VLANs

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

Note

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

■ VLAN Classification

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

■ Port Overlapping

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

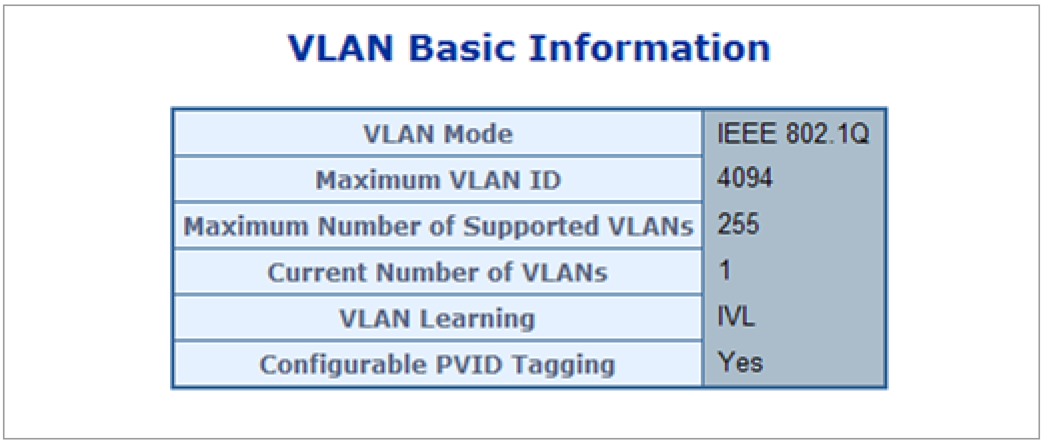
■ Untagged VLANs

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

4.6.3 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.



VLAN Basic Information

VLAN Mode	IEEE 802.1Q
Maximum VLAN ID	4094
Maximum Number of Supported VLANs	255
Current Number of VLANs	1
VLAN Learning	IVL
Configurable PVID Tagging	Yes

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.

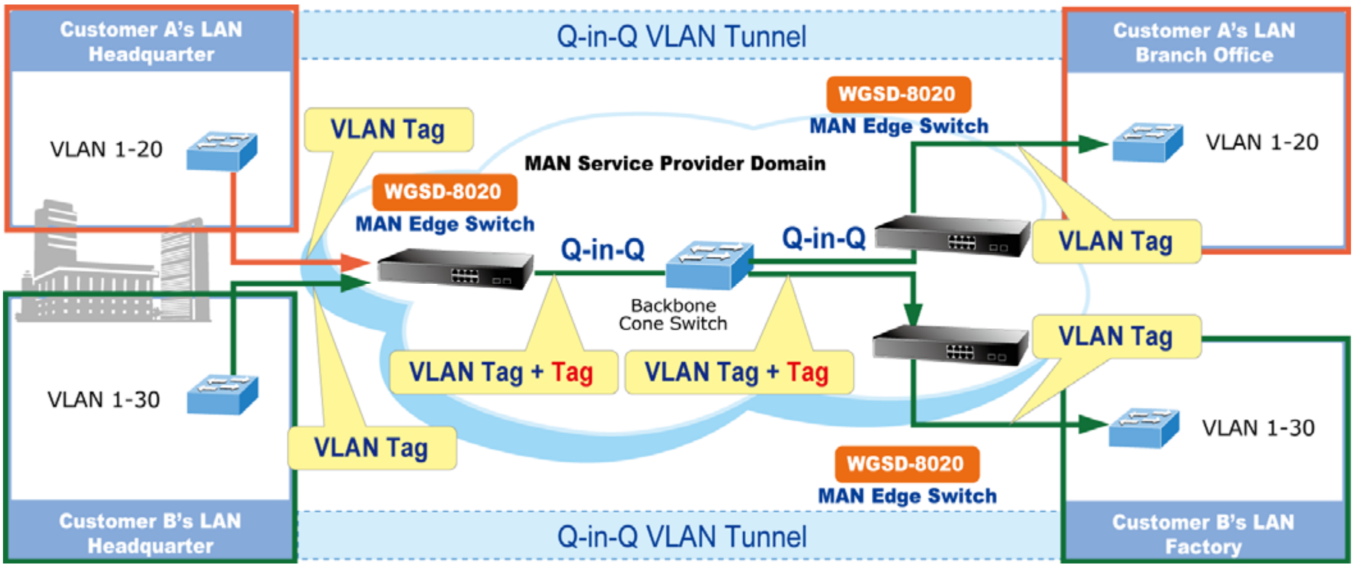


Figure 4-6-2 Q-in-Q VLAN Tunnel

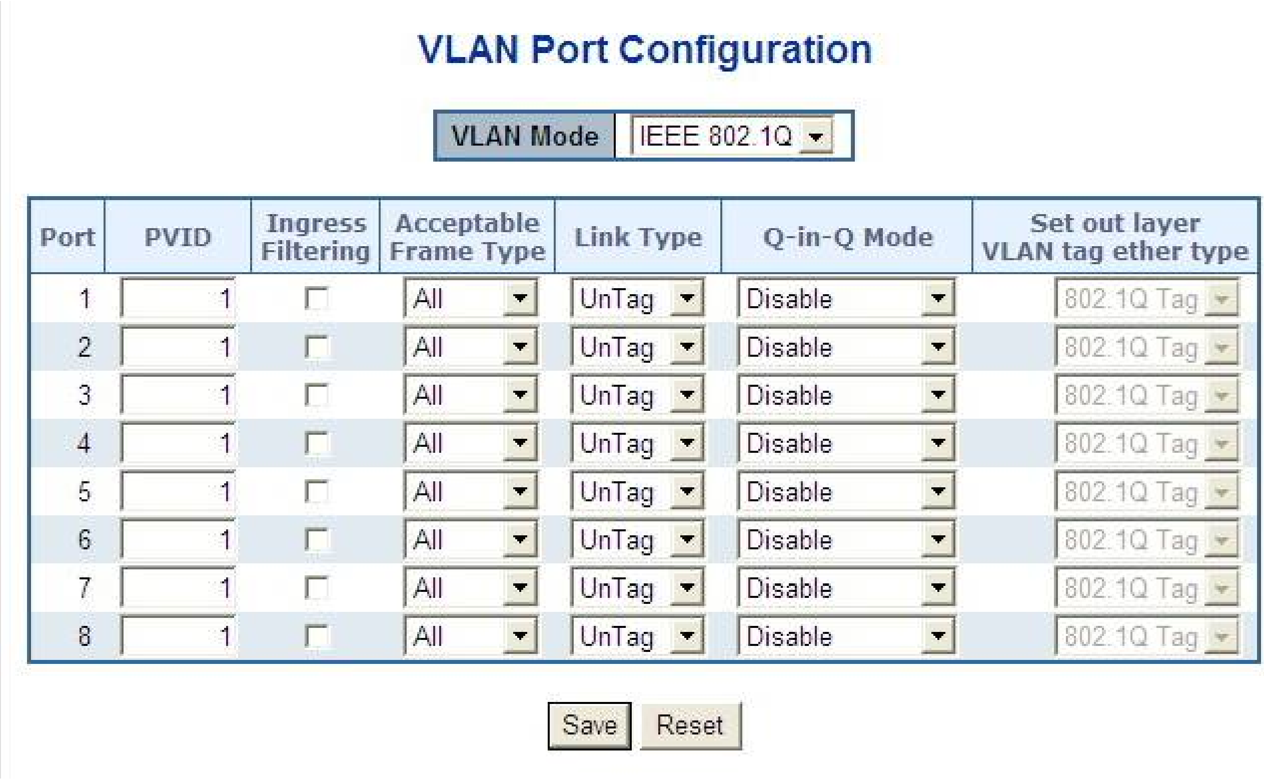
The Managed Switch supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so 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 4-6-3 appears.



VLAN Port Configuration

VLAN Mode: IEEE 802.1Q

Port	PVID	Ingress Filtering	Acceptable Frame Type	Link Type	Q-in-Q Mode	Set out layer VLAN tag ether type
1	1	□	All	UnTag	Disable	802.1Q Tag
2	1	□	All	UnTag	Disable	802.1Q Tag
3	1	□	All	UnTag	Disable	802.1Q Tag
4	1	□	All	UnTag	Disable	802.1Q Tag
5	1	□	All	UnTag	Disable	802.1Q Tag
6	1	□	All	UnTag	Disable	802.1Q Tag
7	1	□	All	UnTag	Disable	802.1Q Tag
8	1	□	All	UnTag	Disable	802.1Q Tag

Figure 4-6-3 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

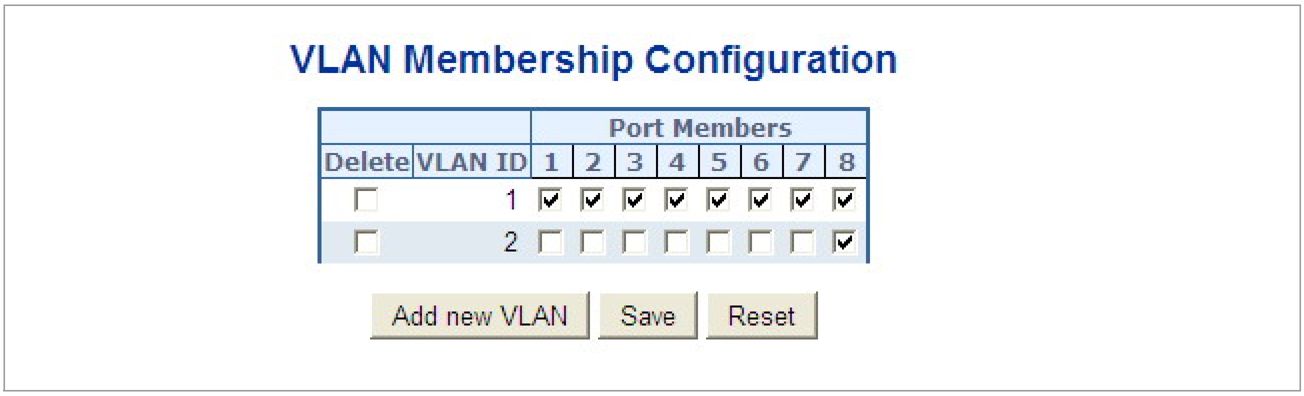
Note

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

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 4-6-4 appears.



VLAN Membership Configuration

		Port Members							
Delete	VLAN ID	1	2	3	4	5	6	7	8
□	1	☑	☑	☑	☑	☑	☑	☑	☑
□	2	□	□	□	□	□	□	□	☑

Figure 4-6-4 VLAN Membership Configuration page screenshot

The page includes the following fields:

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

4.6.6 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.

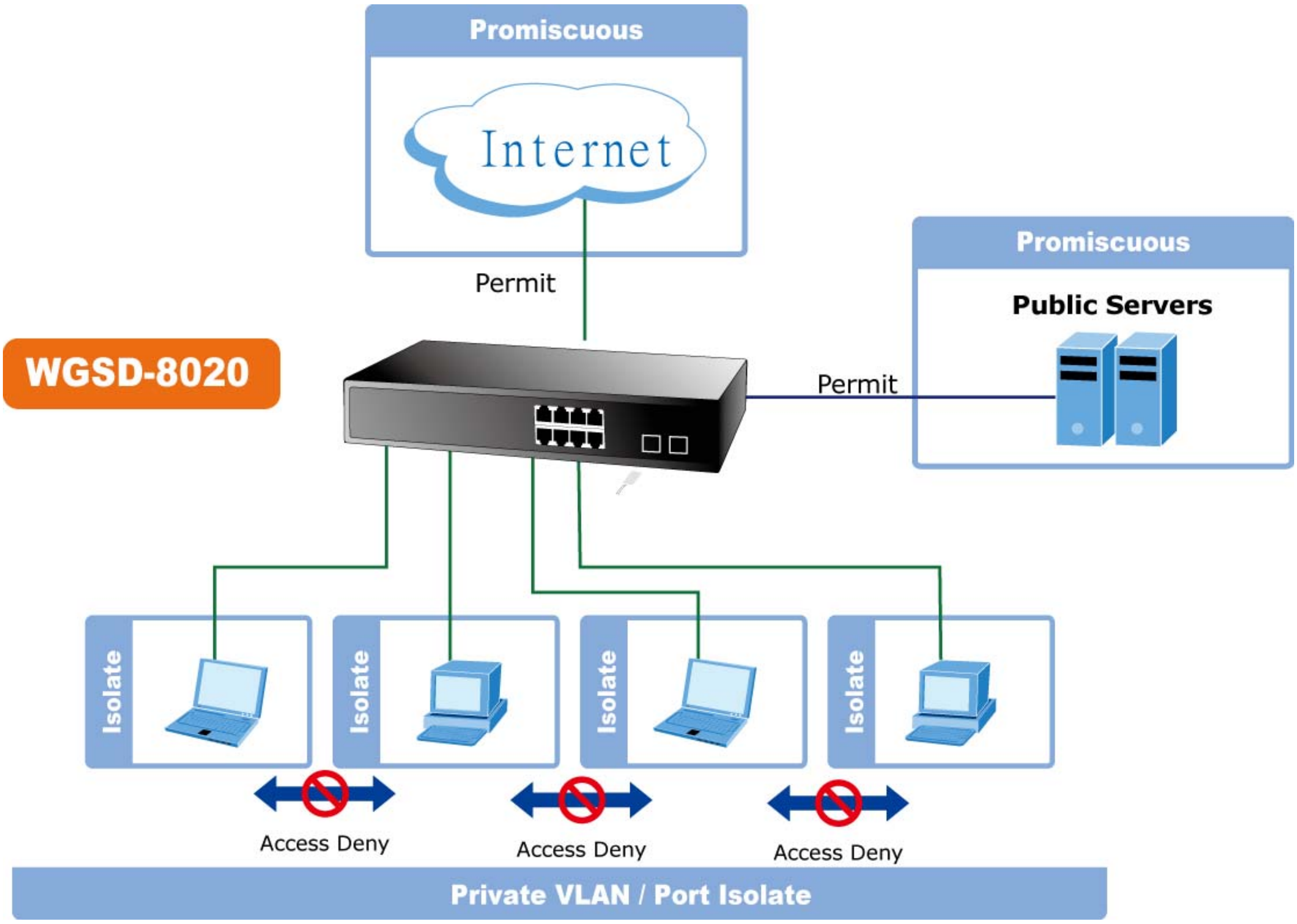


Figure 4-6-5 Private VLAN / Port Isolate application

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

- **Promiscuous ports**

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

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

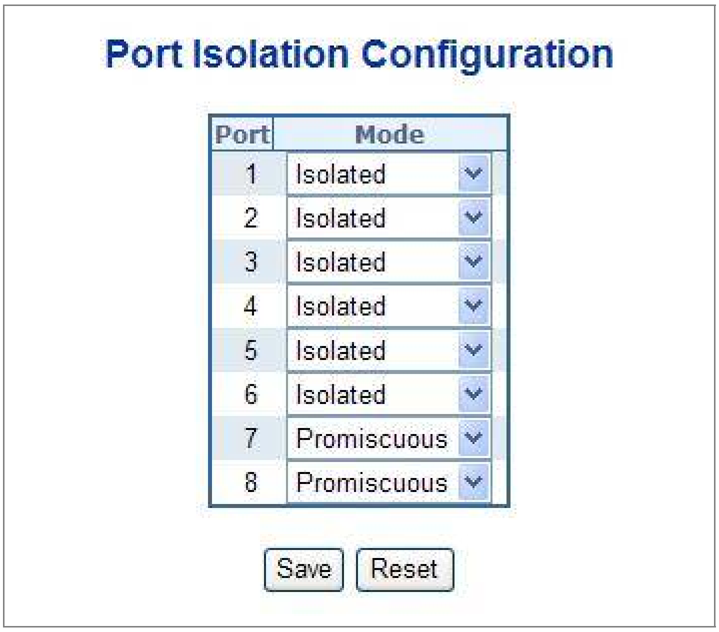
- **Isolated ports**

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

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

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

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



Port Isolation Configuration

Port	Mode
1	Isolated
2	Isolated
3	Isolated
4	Isolated
5	Isolated
6	Isolated
7	Promiscuous
8	Promiscuous

Figure 4-6-6 Port Isolation Configuration page screenshot

The page includes the following fields:

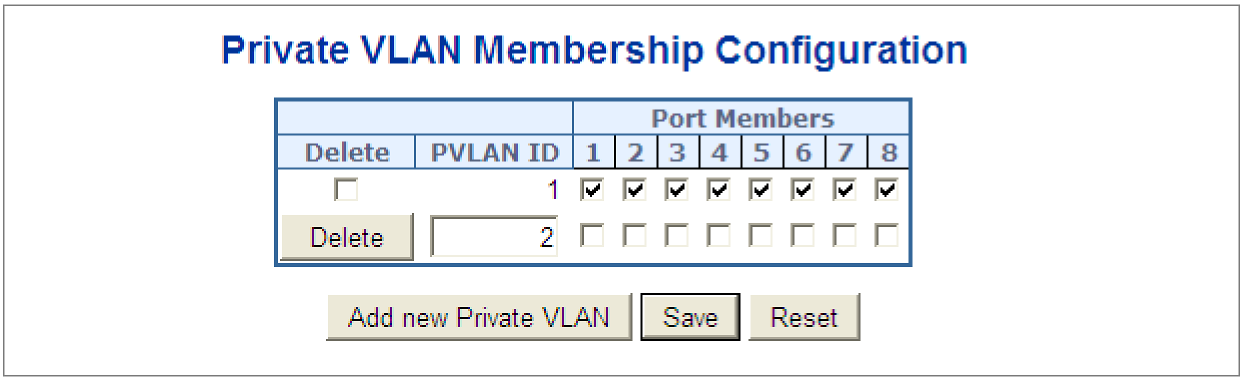
Object	Description	
• **Port**	The switch interface.	
• **Mode**	Configure and Displays private VLAN port types.	
	Isolated	A single stand-alone VLAN that contains one promiscuous port and one or more isolated (or host) ports. This VLAN conveys traffic between the isolated ports and a lone promiscuous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

4.6.7 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.



Private VLAN Membership Configuration

		Port Members							
Delete	PVLAN ID	1	2	3	4	5	6	7	8
□	1	☑	☑	☑	☑	☑	☑	☑	☑
Delete	2	□	□	□	□	□	□	□	□

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

The page includes the following fields:

Object	Description
• **Delete**	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
• **Private VLAN ID**	Indicates the ID of this particular private VLAN.
• **Port Members**	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
• **Adding a New Private VLAN**	Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click "Save". The button can be used to undo the addition of new Private VLANs.
Save	Click to save changes.
Reset	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 Spanning Tree Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

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

The Switch STP performs the following functions:

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

Bridge Protocol Data Units

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

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

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

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

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

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

Creating a Stable STP Topology

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

STP Port States

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

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

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

A port transitions from one state to another as follows:

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

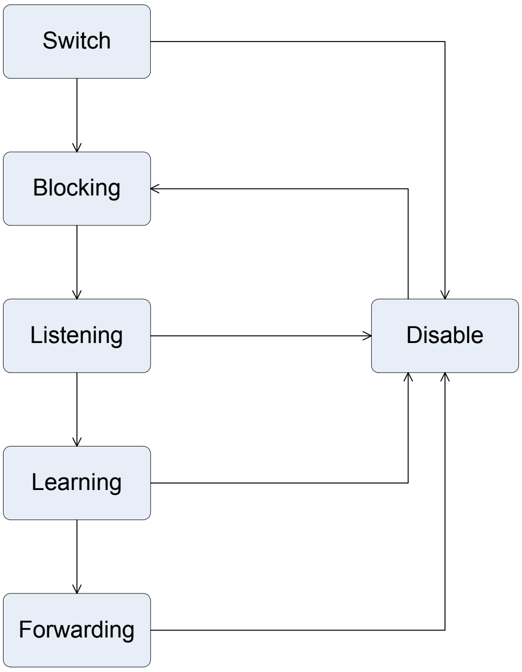


Figure 4-7-1 STP Port State Transitions

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

2. STP Parameters

STP Operation Levels

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

Note

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

On the port level, STP sets the Root Port and the Designated Ports.

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

Parameter	Description	Default Value
Bridge Identifier(Not user configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC	32768 + MAC

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

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

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

Default Spanning-Tree Configuration

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

User-Changeable STA Parameters

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

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

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

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

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

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

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

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

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

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

3. Illustration of STP

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

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

Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there.

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

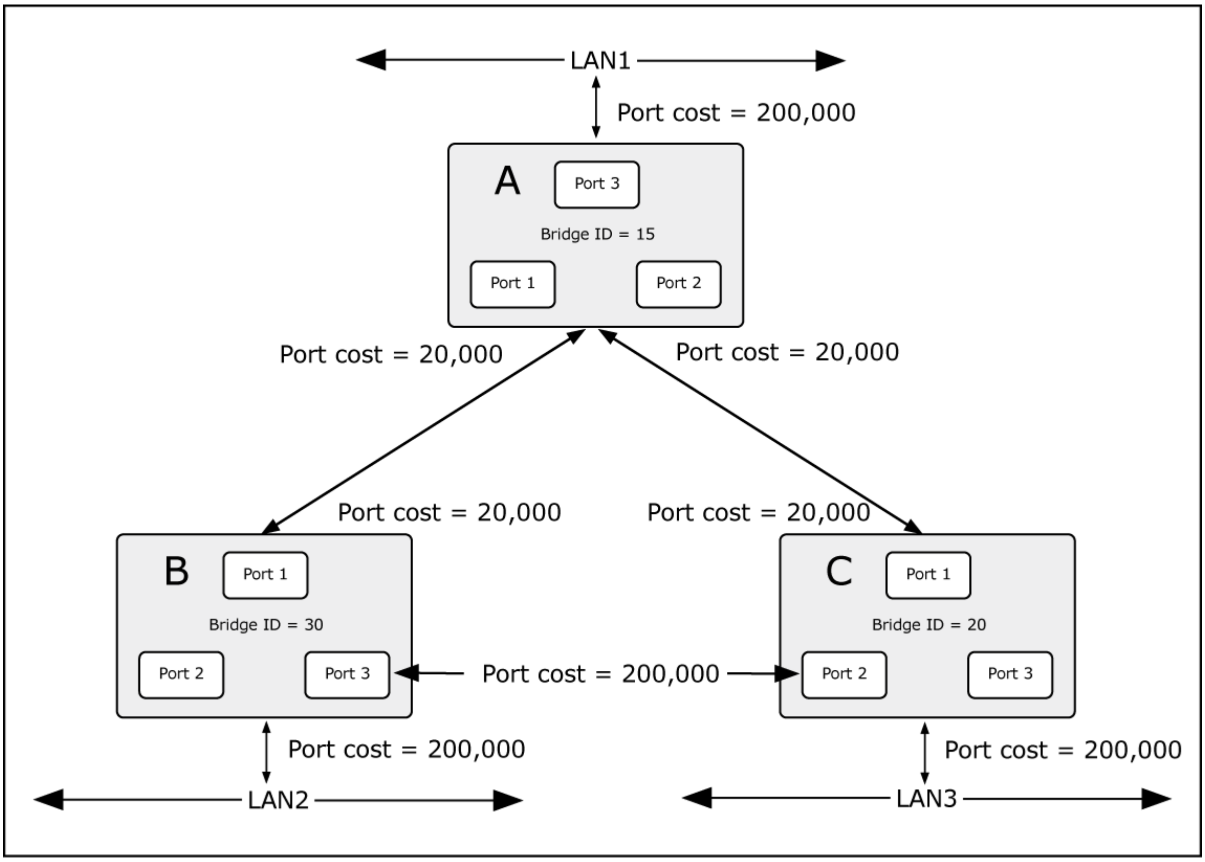


Figure 4-7-2 Before Applying the STA Rules

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

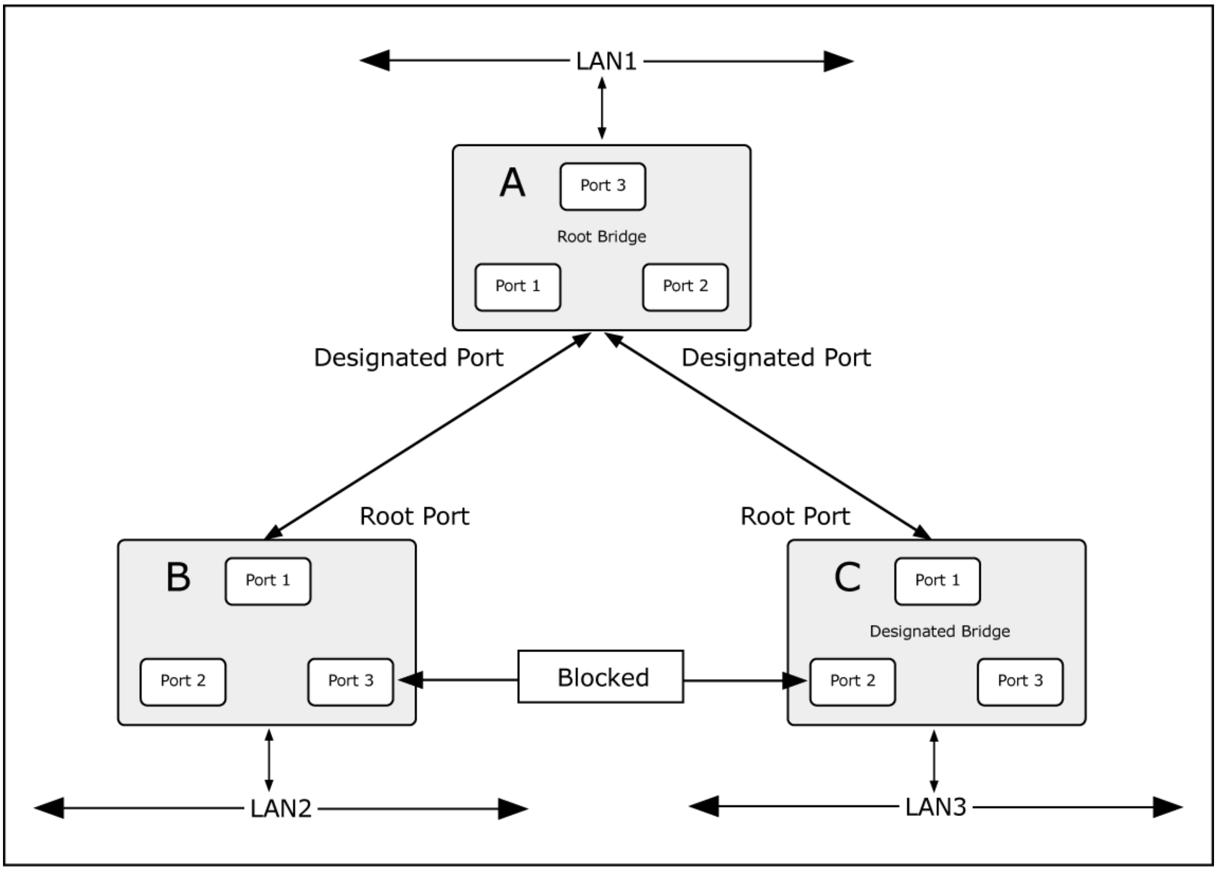


Figure 4-7-3 After Applying the STA Rules

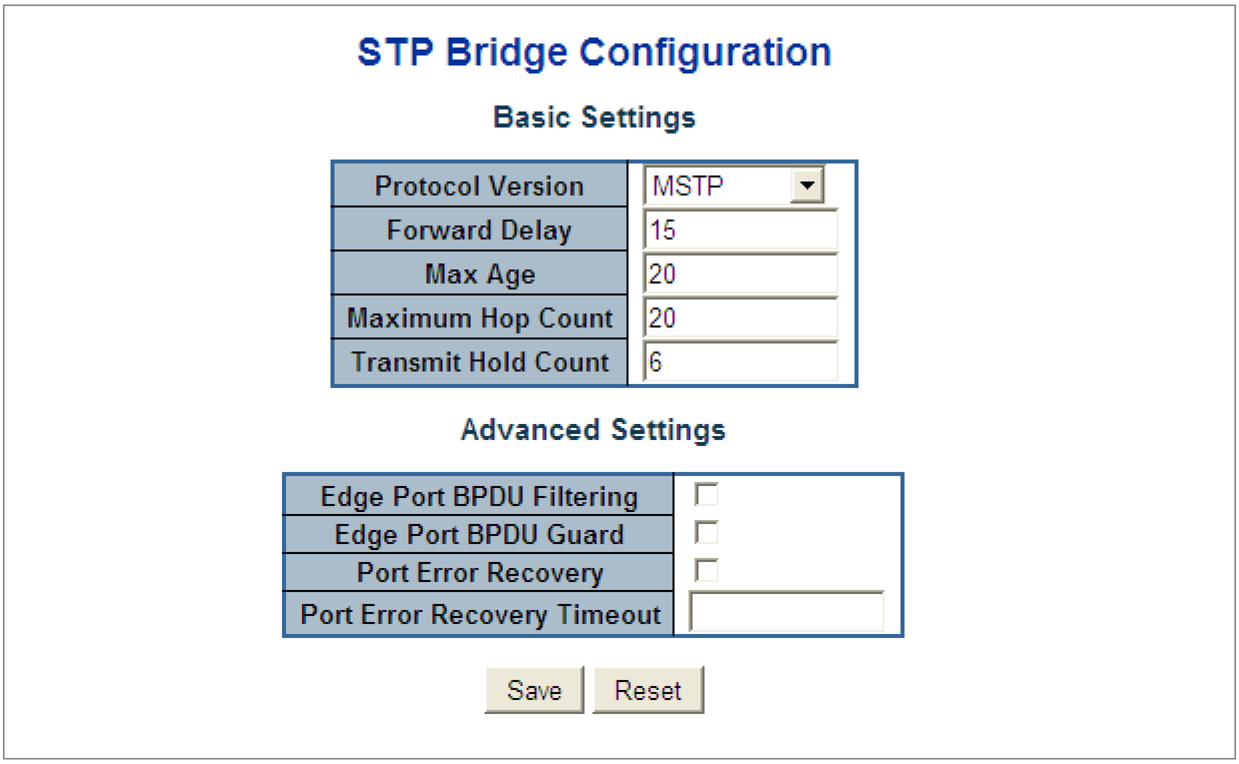
The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 2,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 20,000). 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 System Configuration

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

- **STP (Spanning Tree Protocol):**Provides a single path between end stations, avoiding and eliminating loops.
- **RSTP (Rapid Spanning Tree Protocol) :** Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.
- **MSTP (Multiple Spanning Tree Protocol):** 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 System Configuration screen in Figure 4-7-4 appears.



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Figure 4-7-4 RSTP System Configuration page screenshot

The **Basic Settings** Table includes the following fields:

Object	Description
• **Protocol Version**	The STP compatibility mode setting. Valid values are: ■ **STP** ■ **RSTP** ■ **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 40 seconds. -Default: 20 -Minimum: The higher of 6 or [2 x (Hello Time + 1)]. -Maximum: The lower of 40 or [2 x (Forward Delay -1)]
• **Maximum Hop Count**	This defines the initial value of remainingHops 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 4 to 30 seconds, *and* MaxAge must be <= (FwdDelay-1)*2.
• **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.

The **Advanced Settings** Table includes the following fields:

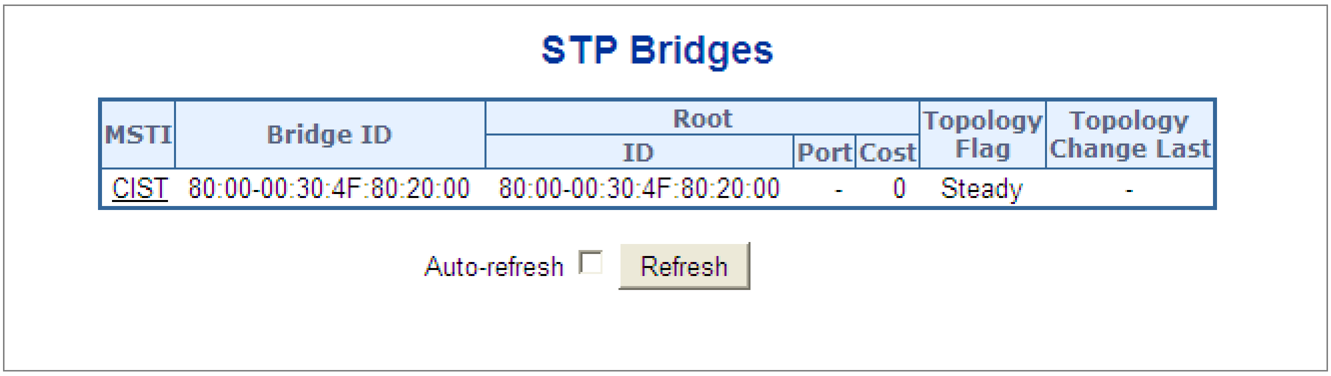
Object	Description
• **Edge Port BPDU Filtering**	Control whether a port explicitly configured as **Edge** will transmit and receive BPDUs.
• **Edge Port BPDU Guard**	Control whether a port explicitly configured as **Edge** will disable itself upon reception of a BPDU. The port will enter the error-disabled 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).

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 4-7-5 appears.



STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:30:4F:80:20:00	80:00-00:30:4F:80:20:00	-	0	Steady	-

Figure 4-7-5 STP Bridge Status page screenshot

The page includes the following fields:

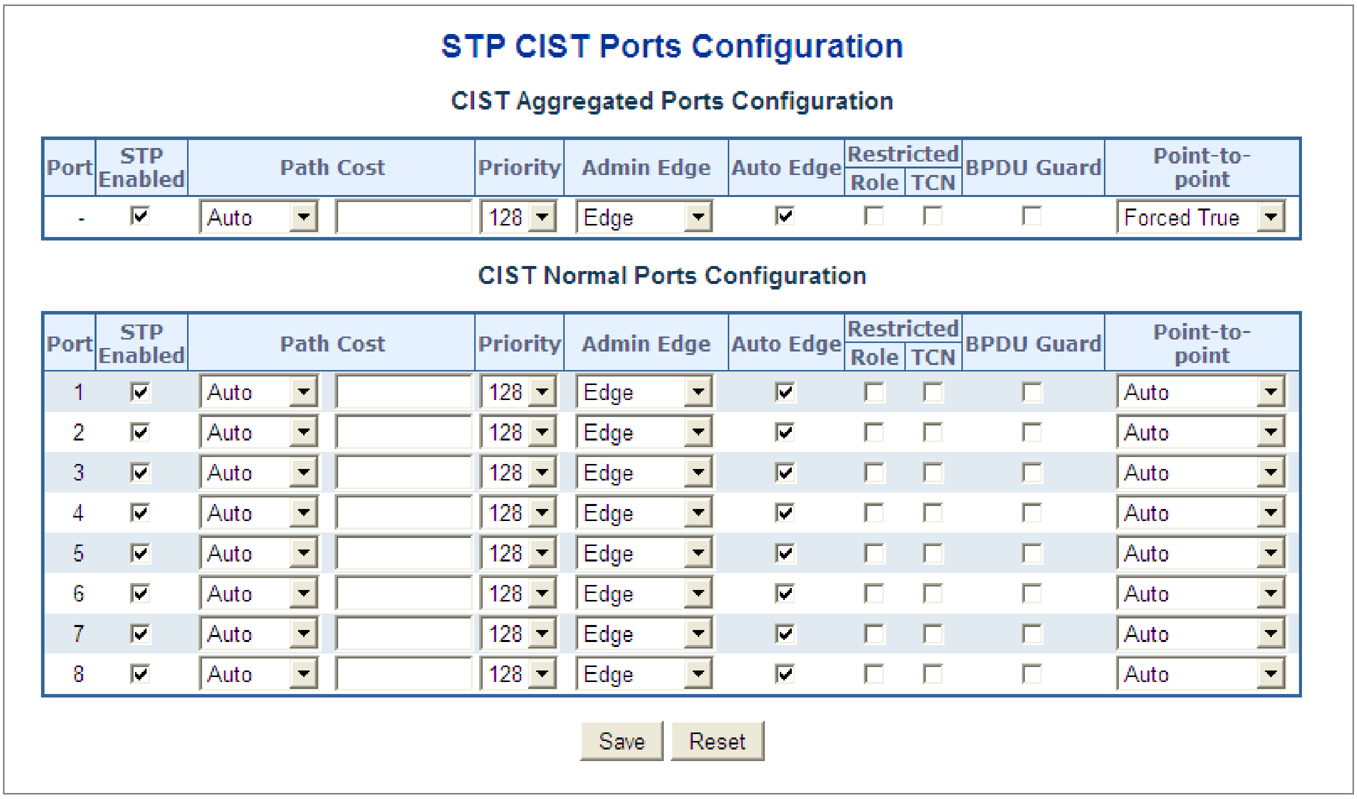
Object	Description
• **MSTI**	The Bridge Instance. This is also a link to the **STP Detailed Bridge Status**.
• **Bridge ID**	The Bridge ID of this Bridge instance.
• **Root ID**	The Bridge ID of the currently elected root bridge.
• **Root Port**	The switch port currently assigned the *root* port role.
• **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 STP Port Configuration screen in Figure 4-7-6 appears.



STP CIST Ports Configuration

CIST Aggregated Ports Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☑	Auto		128	Edge	☑	☐	☐	☐	Forced True

CIST Normal Ports Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
1	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
2	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
3	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
4	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
5	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
6	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
7	☑	Auto		128	Edge	☑	☐	☐	☐	Auto
8	☑	Auto		128	Edge	☑	☐	☐	☐	Auto

Figure 4-7-6 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 STP 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

• **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. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

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

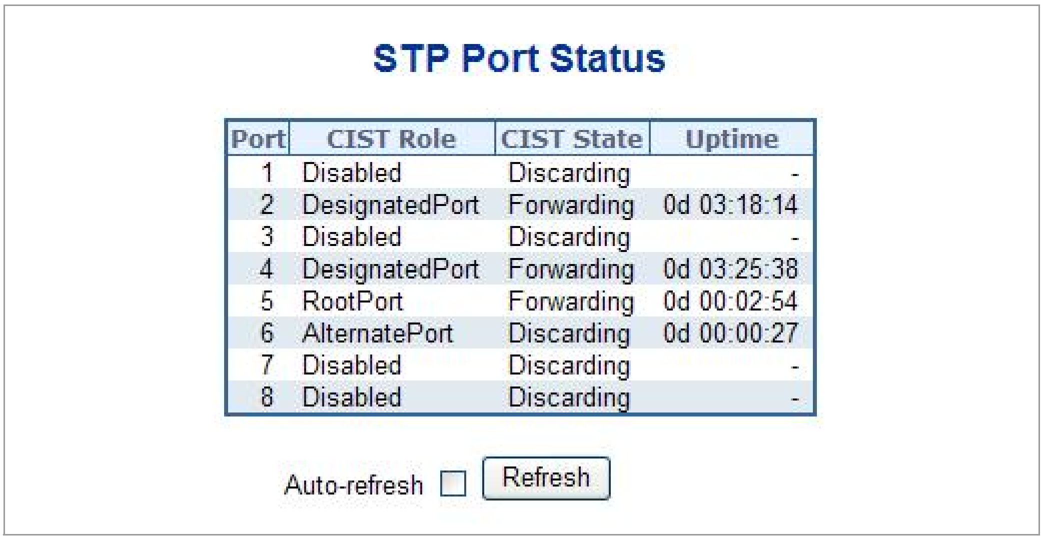
Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

Table 4-7-3 Default STP Path Costs

4.7.5 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 4-7-7 appears.



STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	DesignatedPort	Forwarding	0d 03:18:14
3	Disabled	Discarding	-
4	DesignatedPort	Forwarding	0d 03:25:38
5	RootPort	Forwarding	0d 00:02:54
6	AlternatePort	Discarding	0d 00:00:27
7	Disabled	Discarding	-
8	Disabled	Discarding	-

Figure 4-7-7 STP Port Status page screenshot

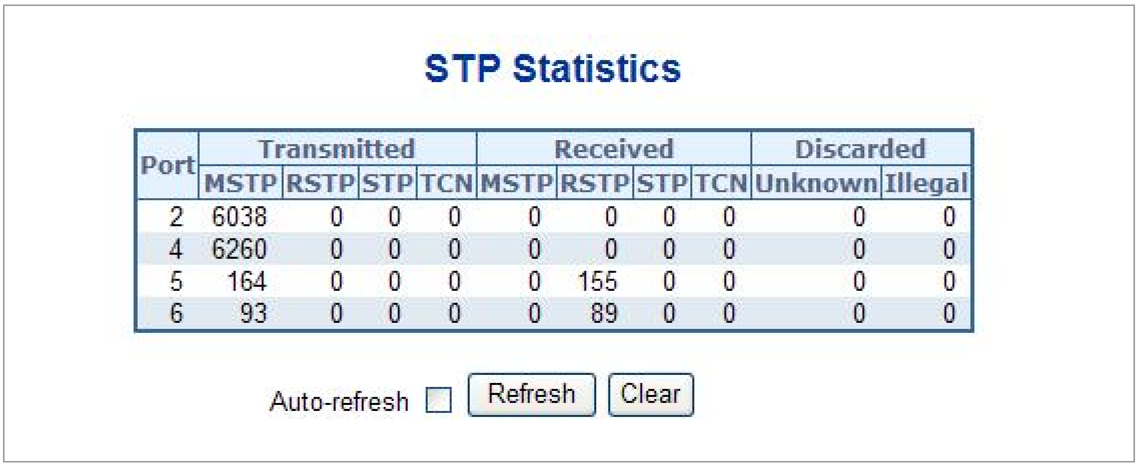
The page includes the following fields:

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: • Disabled • Alternate • Backup • Root • Designated • Non-**STP.**
• **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.

4.7.6 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 4-7-8 appears.



STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
2	6038	0	0	0	0	0	0	0	0	0
4	6260	0	0	0	0	0	0	0	0	0
5	164	0	0	0	0	155	0	0	0	0
6	93	0	0	0	0	89	0	0	0	0

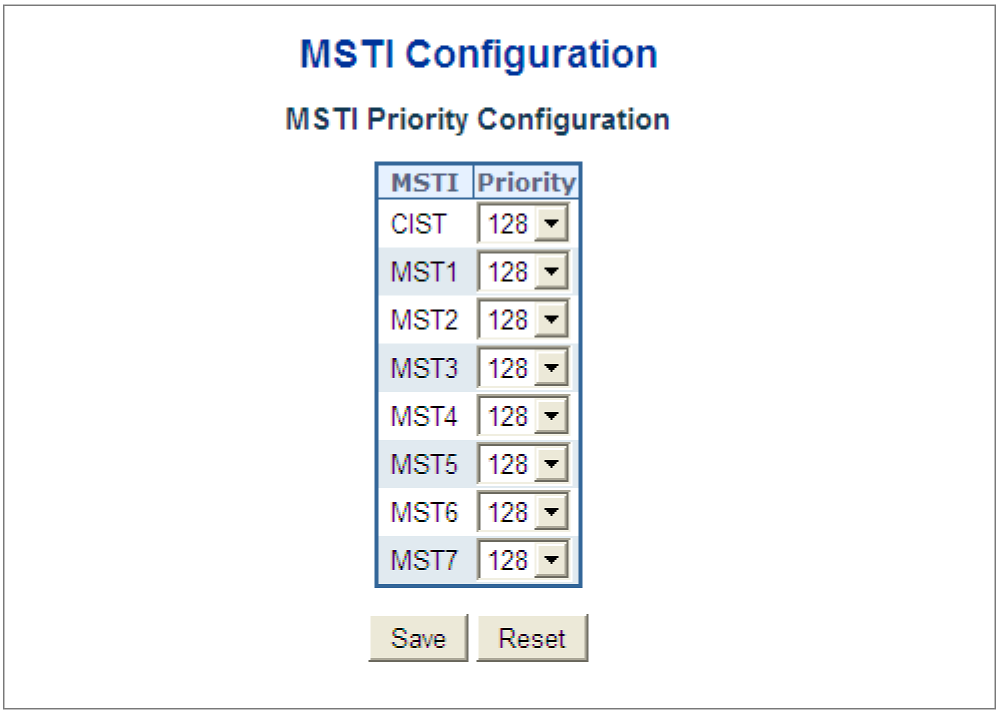
Figure 4-7-8 STP Statistics page screenshot

The page includes the following fields:

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

4.7.7 MSTI Priorities

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



MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
CIST	128
MST1	128
MST2	128
MST3	128
MST4	128
MST5	128
MST6	128
MST7	128

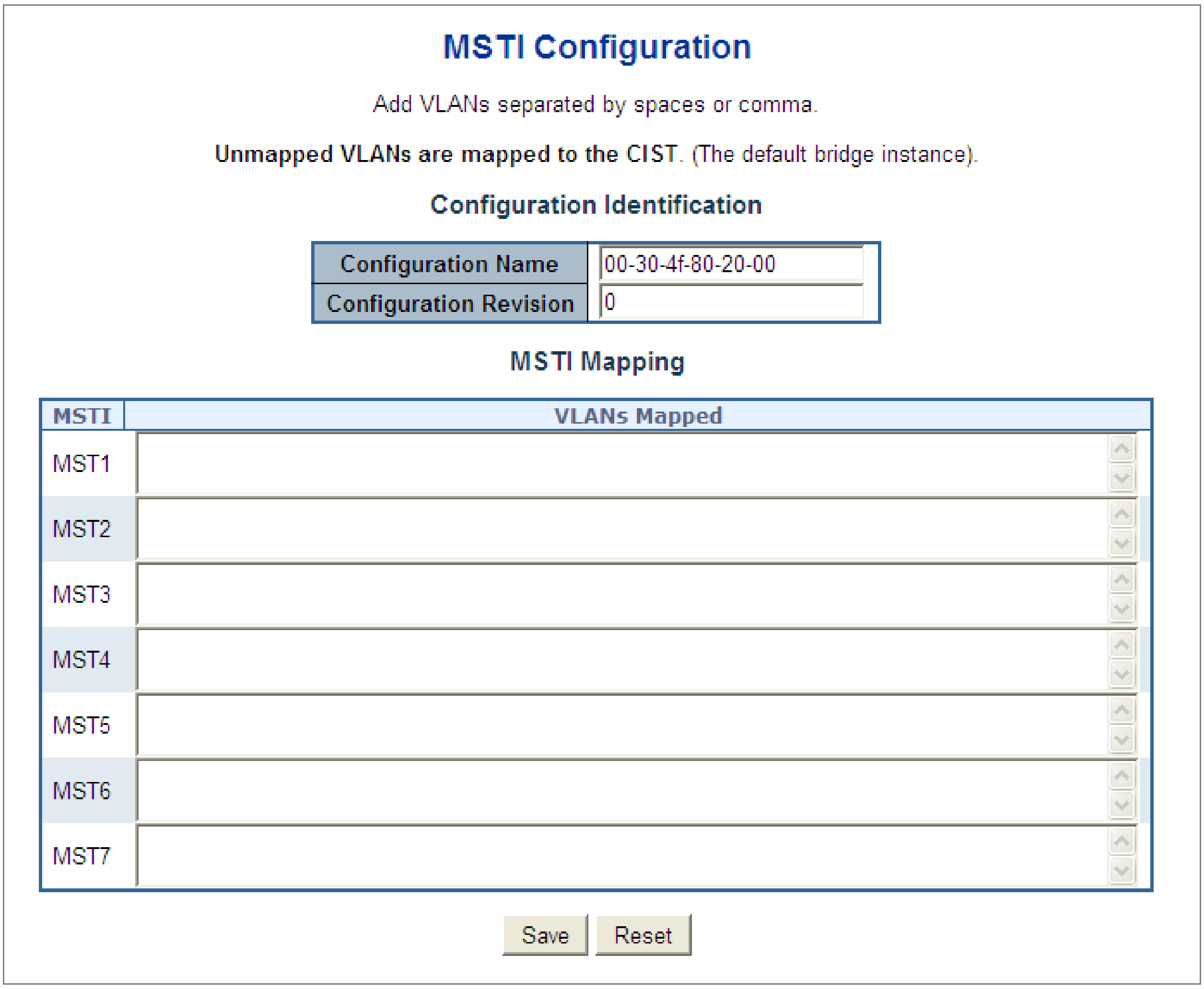
Figure 4-7-9 MSTI Configuration page screenshot

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*.

4.7.8 MSTI Configuration

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



MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-30-4f-80-20-00
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MST1	
MST2	
MST3	
MST4	
MST5	
MST6	
MST7	

Figure 4-7-10 MSTI Configuration Identification page screenshot

The page includes the following fields:

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
- **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.)

4.7.9 MSTI Port 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 seperately 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.

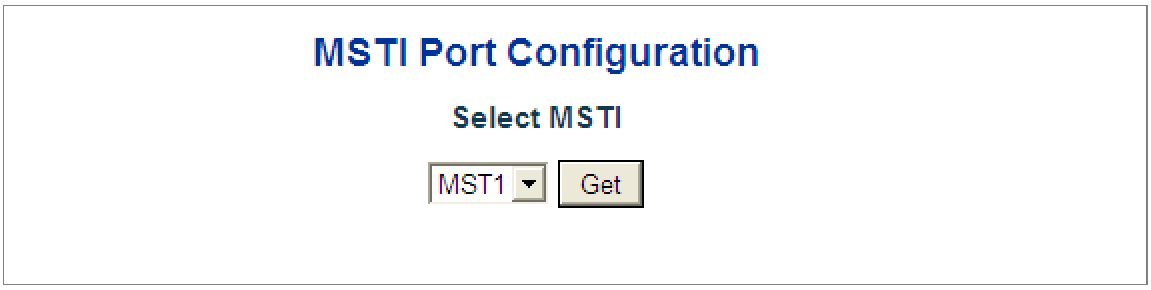
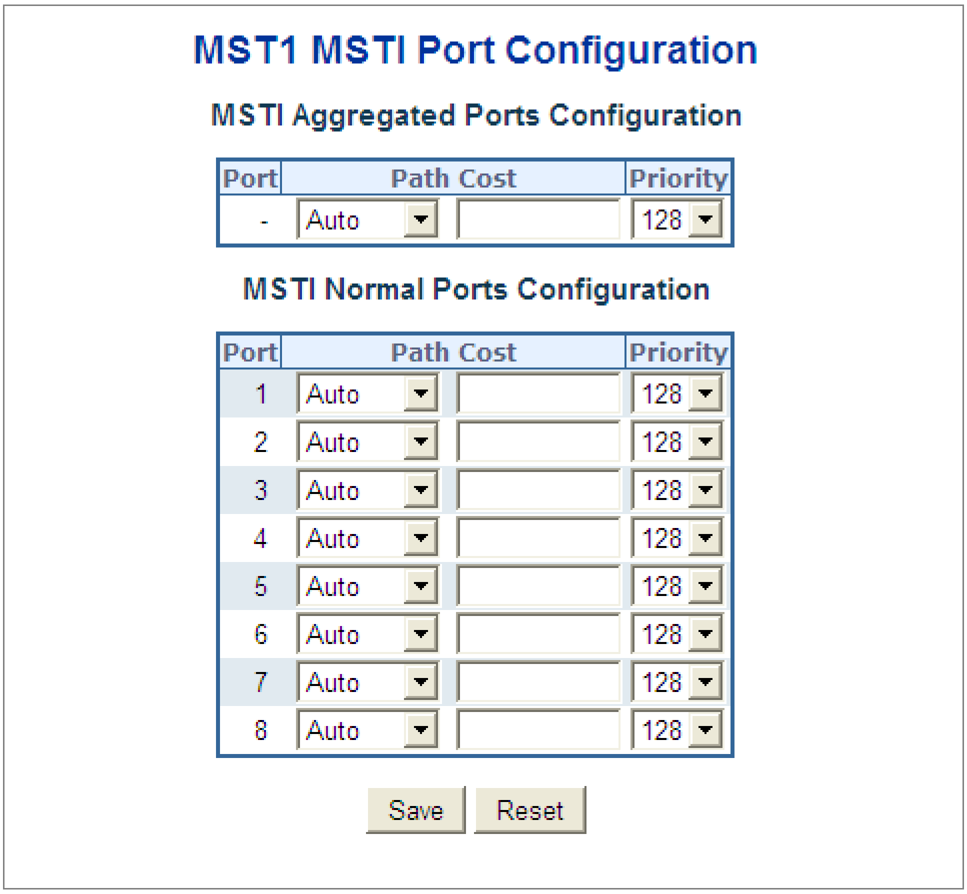


Figure 4-7-11 MSTI Port Configuration page screenshot

The page includes the following fields:

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).



MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost		Priority
-	Auto		128

MSTI Normal Ports Configuration

Port	Path Cost		Priority
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128
7	Auto		128
8	Auto		128

Figure 4-7-12 MSTI MSTI Port Configuration page screenshot

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.

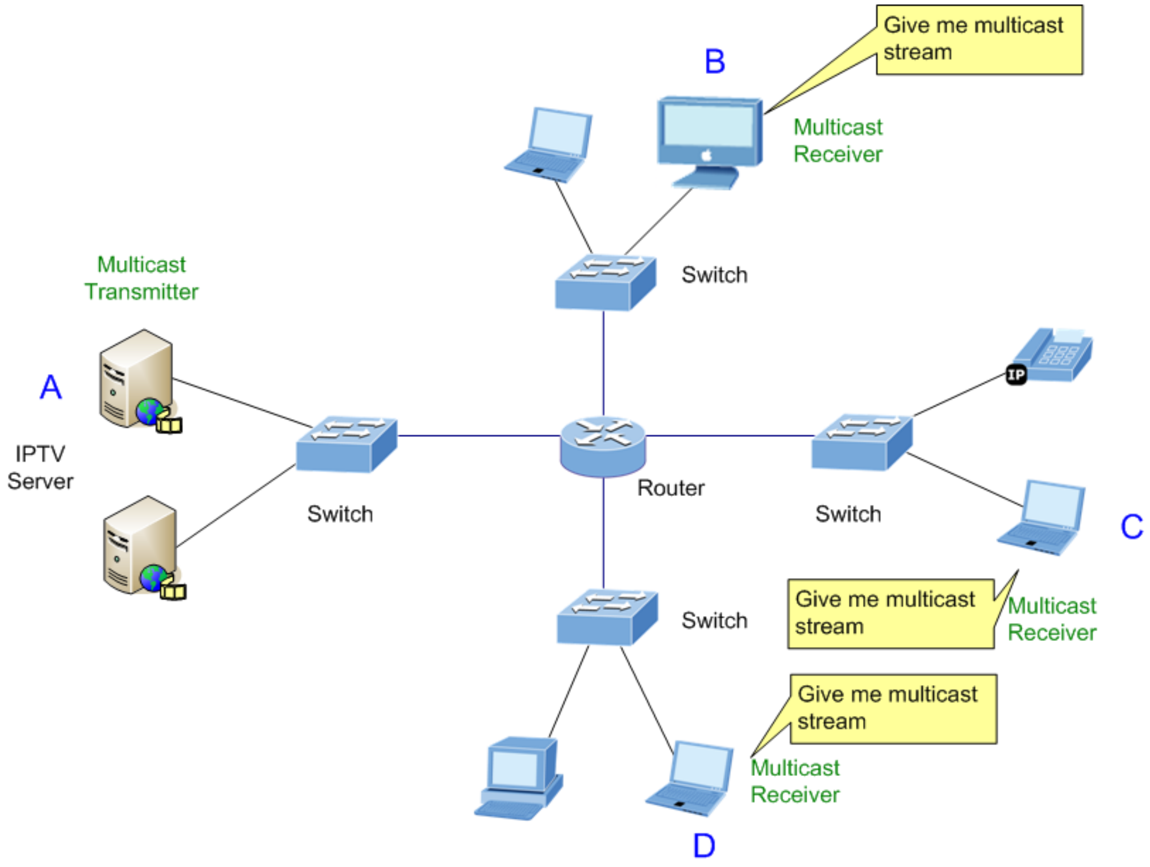


Figure 4-8-1 Multicast Service

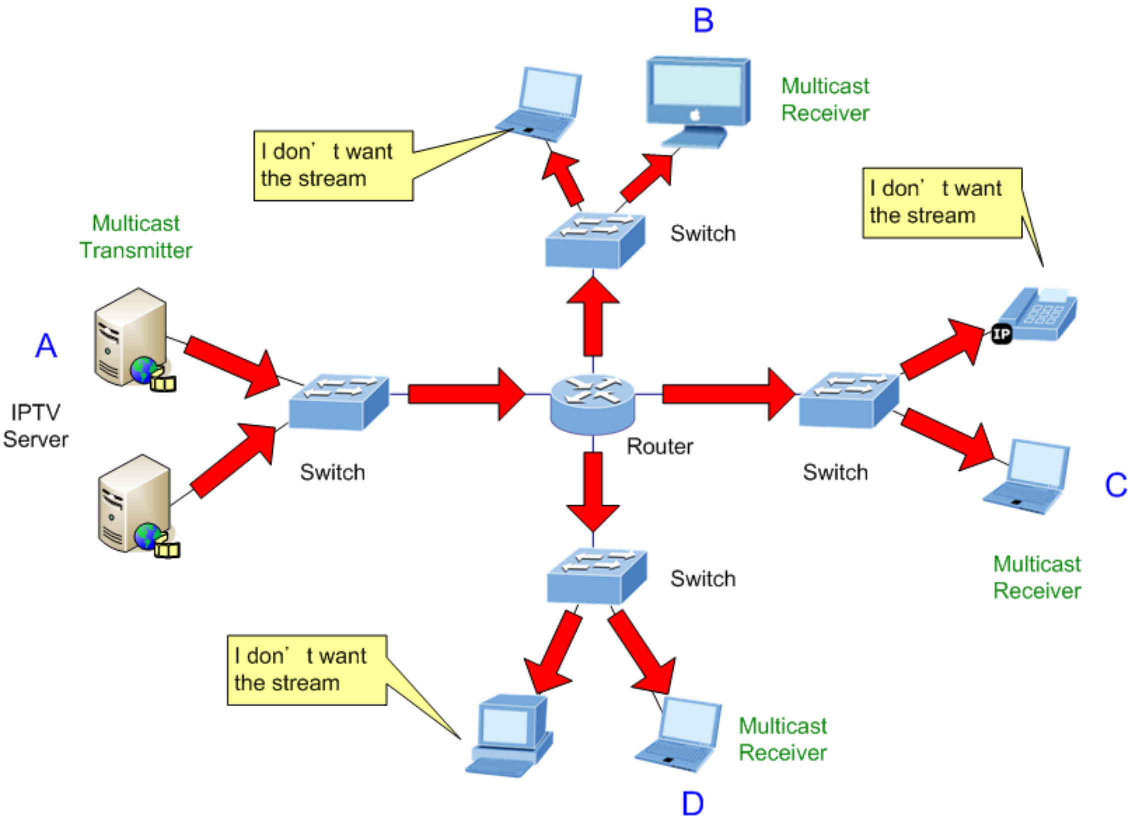


Figure 4-8-2 Multicast flooding

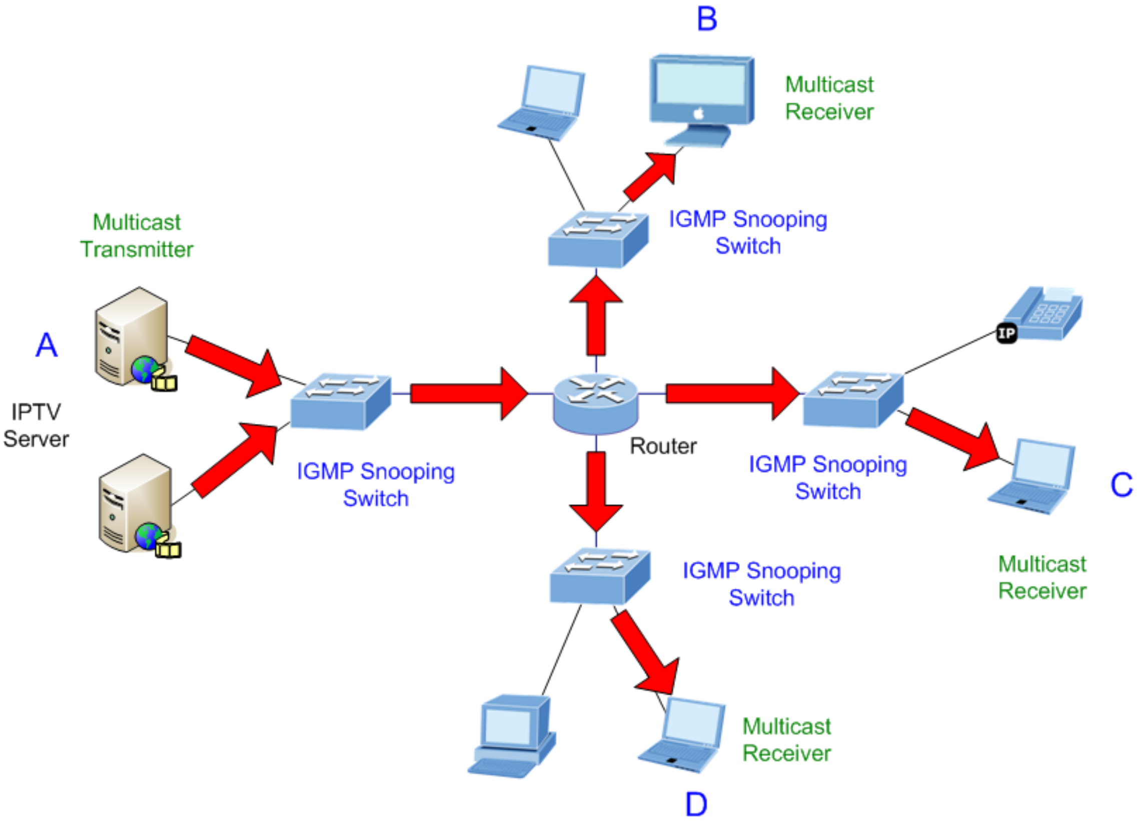


Figure 4-8-3 IGMP Snooping multicast stream control

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

Octets

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

The IGMP Type codes are shown below:

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

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

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

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

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

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

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

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

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

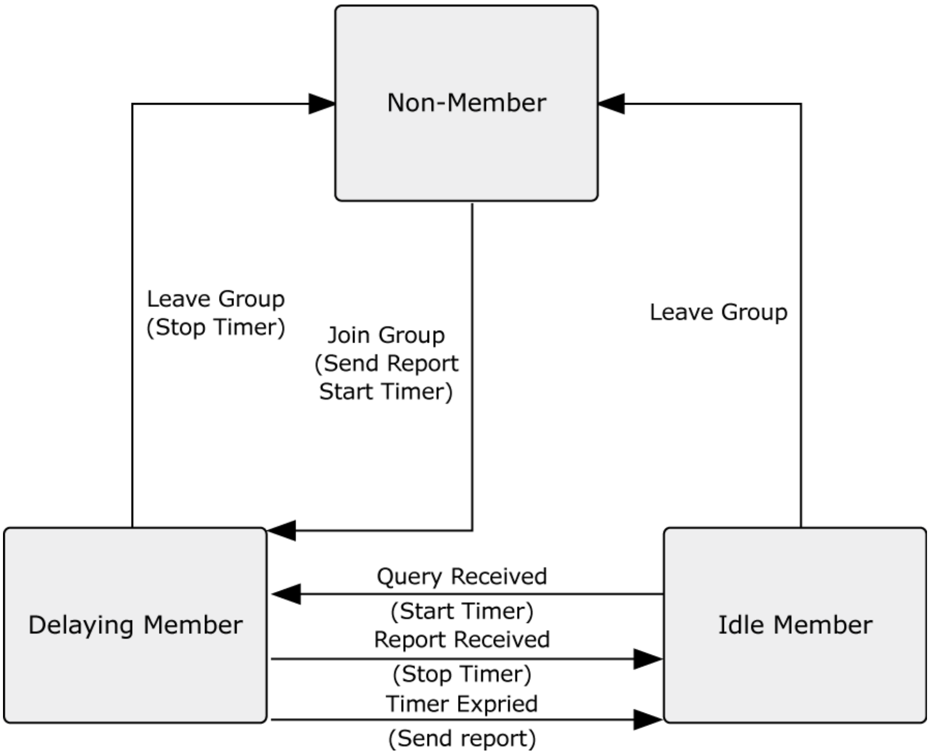


Figure 4-8-4 IGMP State Transitions

- **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.

Note

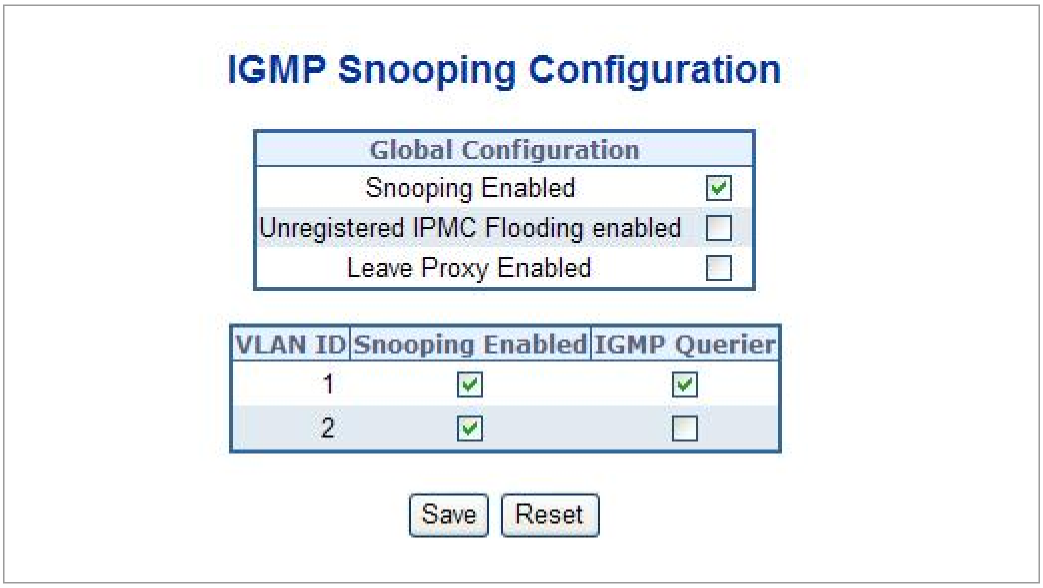
Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

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.



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	☑
Unregistered IPMC Flooding enabled	□
Leave Proxy Enabled	□

VLAN ID	Snooping Enabled	IGMP Querier
1	☑	☑
2	☑	□

Figure 4-8-5 IGMP Snooping Configuration page screenshot

The page includes the following fields:

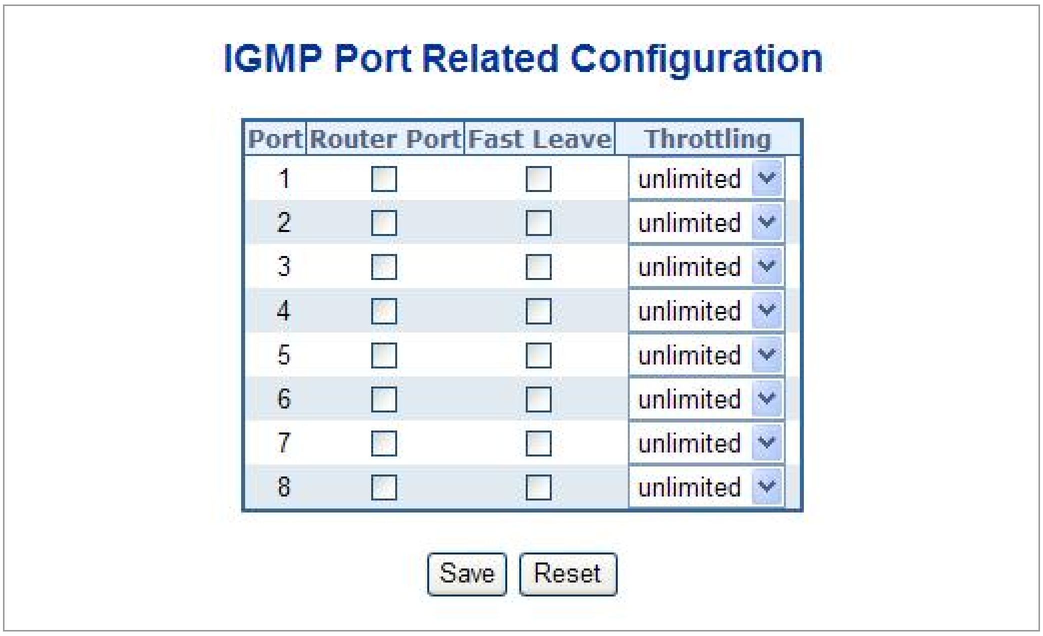
Object	Description
• **Snooping Enabled**	Enable the Global IGMP Snooping.
• **Unregistered IPMC Flooding enabled**	Enable unregistered IPMC traffic flooding.
• **Leave Proxy Enable**	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.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

4.8.3 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.

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 deny the income multicast goups packets - any new IGMP join reports will be dropped.

The IGMP Port Related Configuration screen in Figure 4-8-6 appears.



IGMP Port Related Configuration

Port	Router Port	Fast Leave	Throttling
1	□	□	unlimited
2	□	□	unlimited
3	□	□	unlimited
4	□	□	unlimited
5	□	□	unlimited
6	□	□	unlimited
7	□	□	unlimited
8	□	□	unlimited

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

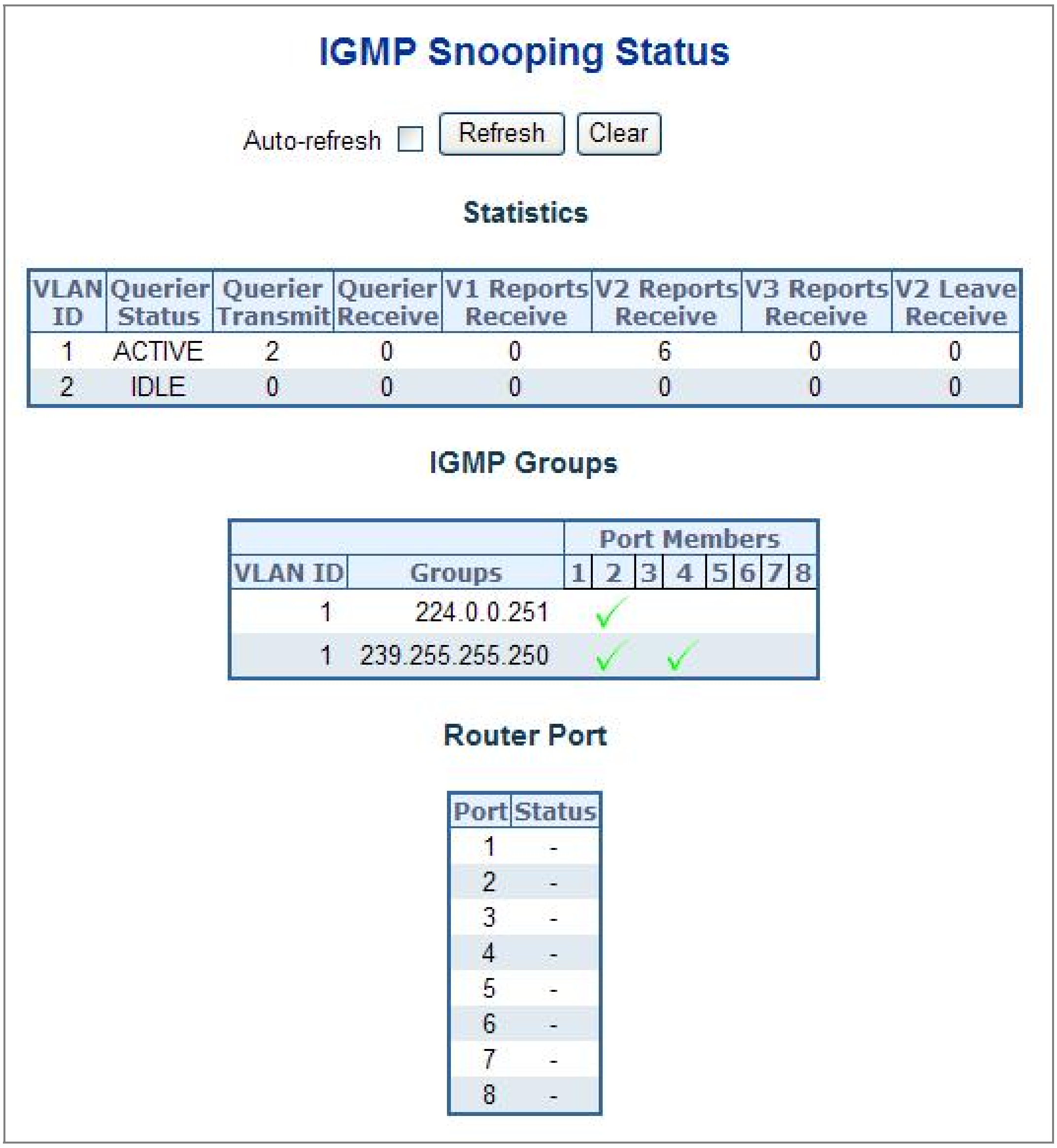
The page includes the following fields:

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.

4.8.4 IGMP Snooping Status

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

The IGMP Snooping status screen in Figure 4-8-7 appears.



IGMP Snooping Status

Statistics

VLAN ID	Querier Status	Querier Transmit	Querier Receive	V1 Reports Receive	V2 Reports Receive	V3 Reports Receive	V2 Leave Receive
1	ACTIVE	2	0	0	6	0	0
2	IDLE	0	0	0	0	0	0

IGMP Groups

		Port Members							
VLAN ID	Groups	1	2	3	4	5	6	7	8
1	224.0.0.251		✓						
1	239.255.255.250		✓		✓				

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

Figure 4-8-7 IGMP Snooping status page screenshot

The page includes the following fields:

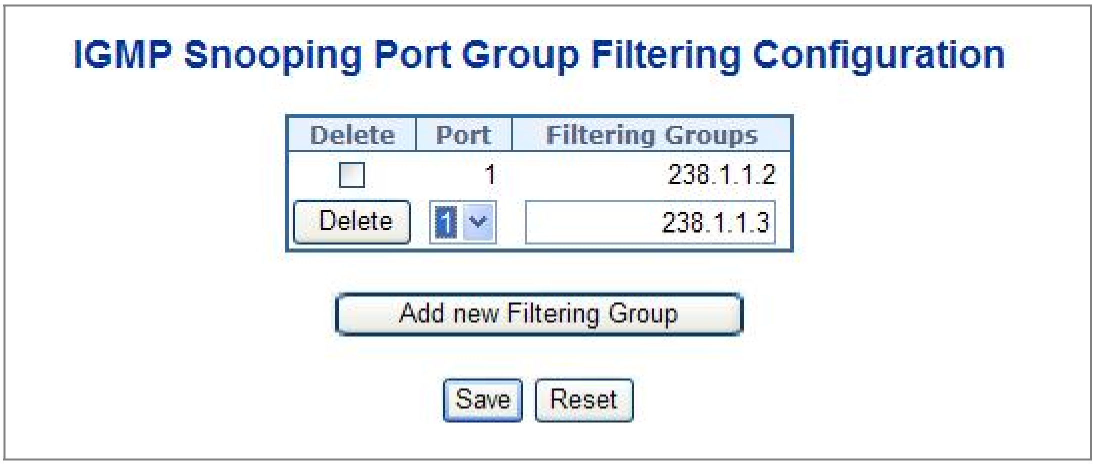
Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **Groups**	The present IGMP groups. Max. are 128 groups for each VLAN.
• **Port Members**	The ports that are members of the entry.
• **Querier Status**	Show the Querier status is "ACTIVE" or "IDLE".
• **Querier Transmit**	The number of Transmitted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

• **Querier Receive**	The number of Received Querier.
• **V1 Reports Receive**	The number of Received V1 Reports.
• **V2 Reports Receive**	The number of Received V2 Reports.
• **V3 Reports Receive**	The number of Received V3 Reports.
• **V2 Leave Receive**	The number of Received V2 Leave.

4.8.5 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 group entry to a switch port that specifies multicast group that are denied on the port. An IGMP filter entry can contain one multicast address. When enabled, IGMP join reports received on the port are checked against the filter entries. If a requested multicast group is denied, the IGMP join report is dropped.



IGMP Snooping Port Group Filtering Configuration

Delete	Port	Filtering Groups
□	1	238.1.1.2
Delete	1	238.1.1.3

Figure 4-8-8 IGMP Snooping Port Group Filtering Configuation 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 Groups**	The IP Multicast Group that will be filtered.
• **Adding New Filtering Group**	Click to add a new entry to the Group Filtering table. Specify the Port, and Filtering Group for the new entry. Click "Save".

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).
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

QoS Terminology

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

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

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

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

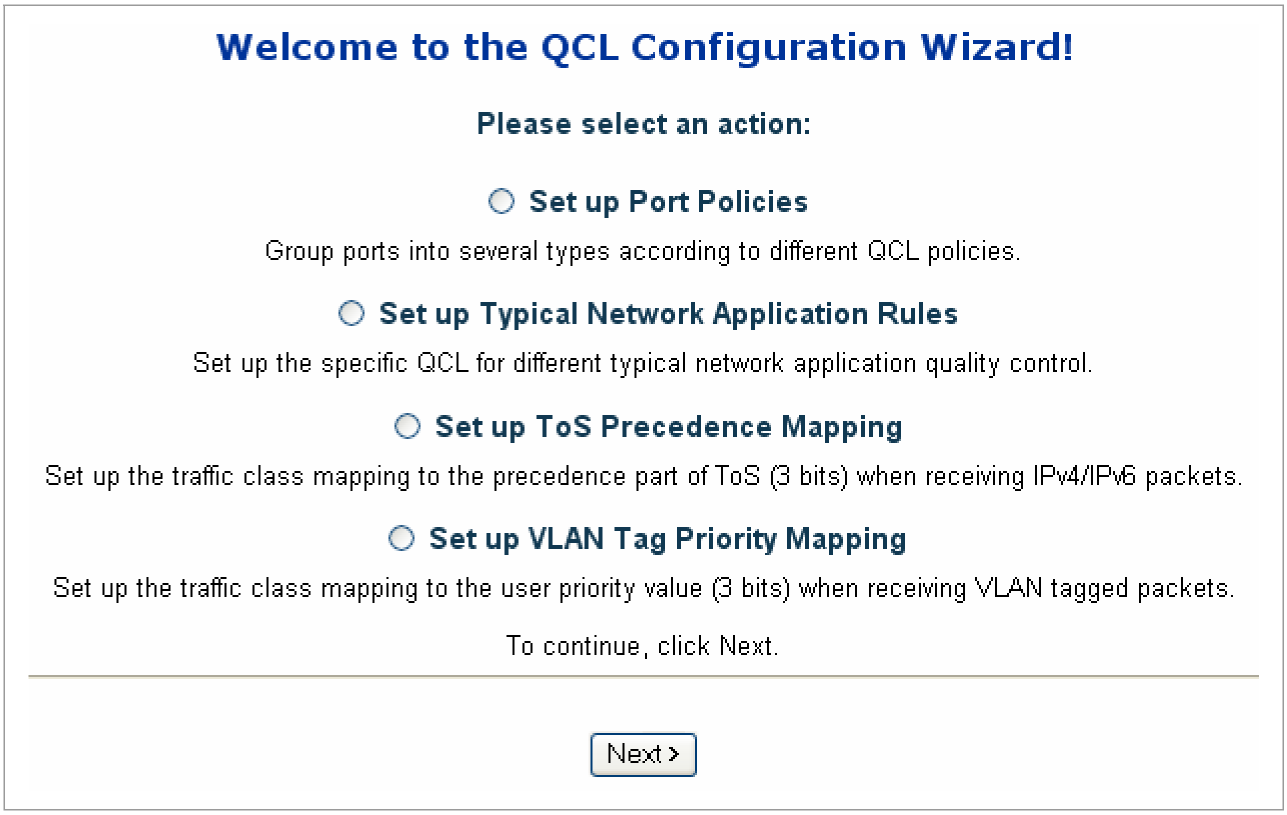
3. Create a QoS profile which associates a service level and a classifier.

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

4.9.2 QCL Configuration Wizard

This handy wizard helps you set up a QCL quickly.

The QCL Configuration Wizard screen in Figure 4-9-1 appears.



Welcome to the QCL Configuration Wizard!

Please select an action:

○ 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.

To continue, click Next.

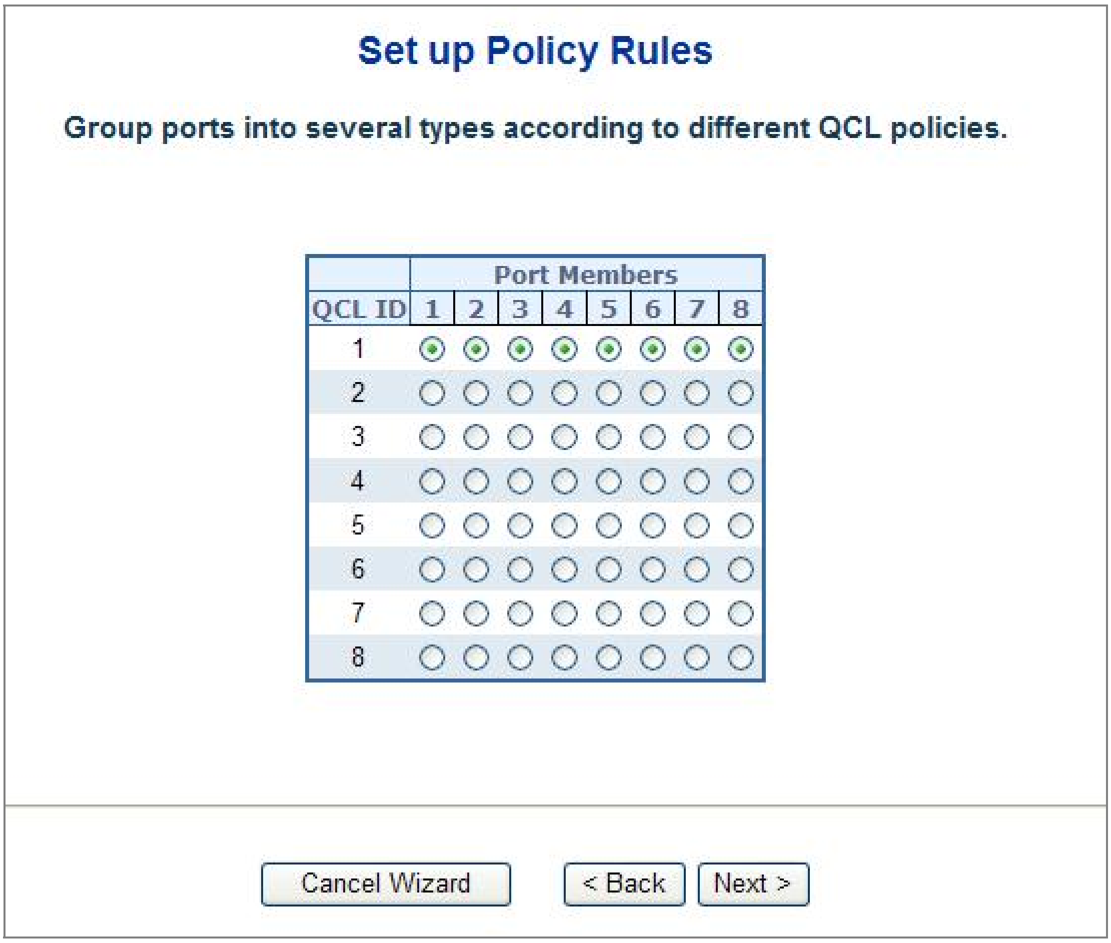
Figure 4-9-1 Welcome to the QCL Configuration Wizard page screenshot

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.

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.



Set up Policy Rules

Group ports into several types according to different QCL policies.

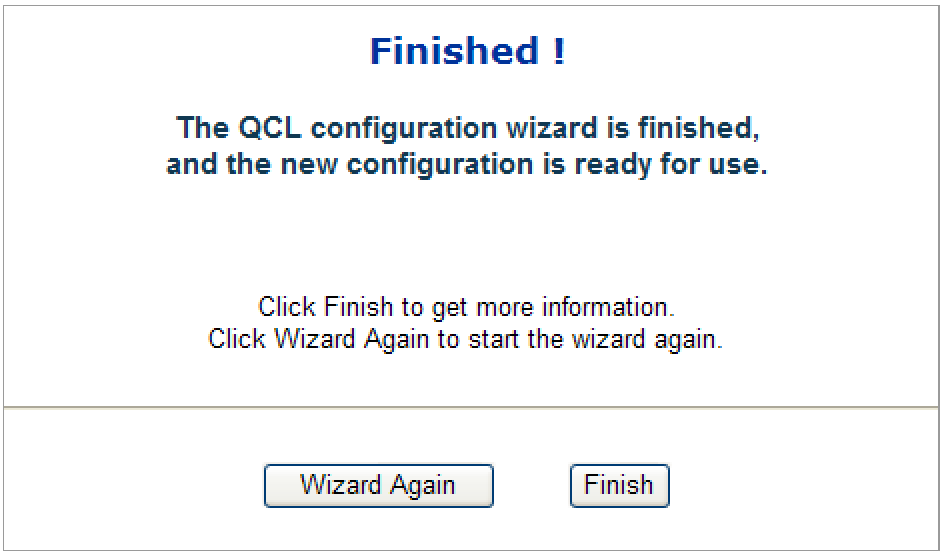
	Port Members							
QCL ID	1	2	3	4	5	6	7	8
1	●	●	●	●	●	●	●	●
2	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○
7	○	○	○	○	○	○	○	○
8	○	○	○	○	○	○	○	○

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

The page includes the folling fileds:

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

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



Finished !

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

Click Finish to get more information.
Click Wizard Again to start the wizard again.

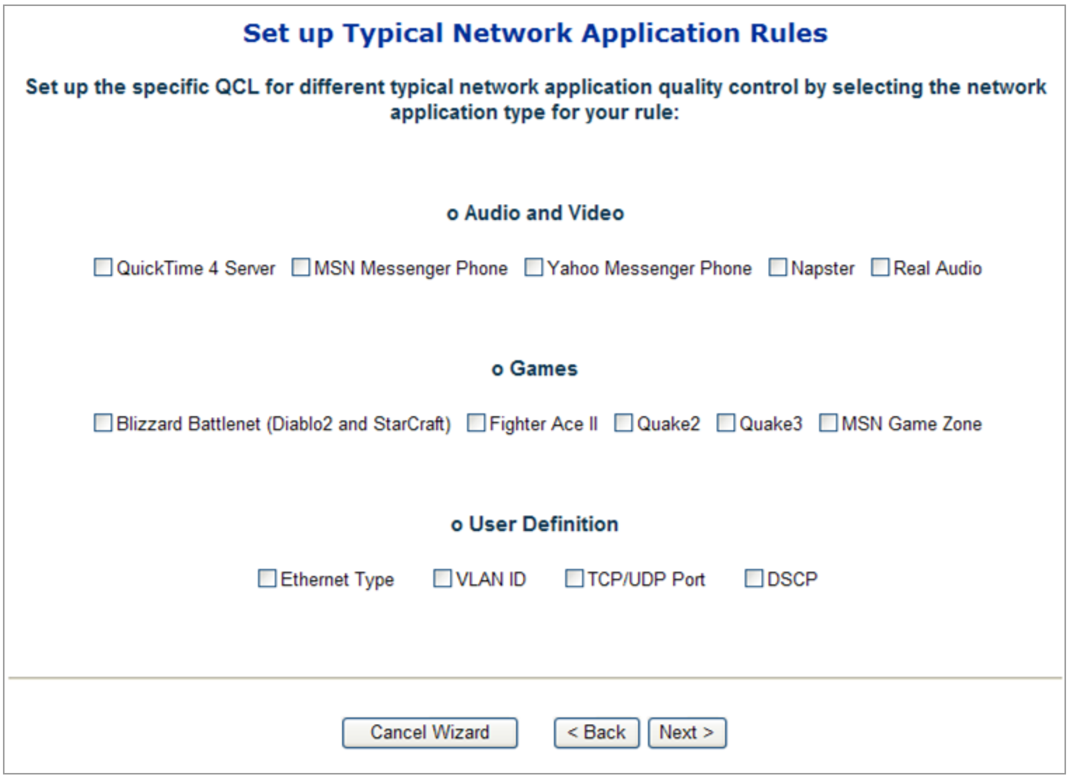
Figure 4-9-3 Set up Policy Rules page screenshot

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:



Set up Typical Network Application Rules

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

o Audio and Video

□ QuickTime 4 Server □ MSN Messenger Phone □ Yahoo Messenger Phone □ Napster □ Real Audio

o Games

□ Blizzard Battlenet (Diablo2 and StarCraft) □ Fighter Ace II □ Quake2 □ Quake3 □ MSN Game Zone

o User Definition

□ Ethernet Type □ VLAN ID □ TCP/UDP Port □ DSCP

Figure 4-9-4 Set up Typical Netowrk Application Rules page screenshot

The page includes the folling fileds:

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

• **User Definition**	Indicates the user definition that applies to the specific QCE. The user definitions are: • **Ethernet Type:** Specify the Ethernet Type filter for this QCE. The allowed range is 0x600 to 0xFFFF. • **VLAN ID:** VLAN ID filter for this QCE. The allowed range is 1 to 4095. • **UDP/TCP Port:** Specify the TCP/UDP port filter for this QCE. The allowed range is 0 to 65535. • **DSCP:** Specify the DSCP filter for this QCE. The allowed range is 0 to 63.

Buttons

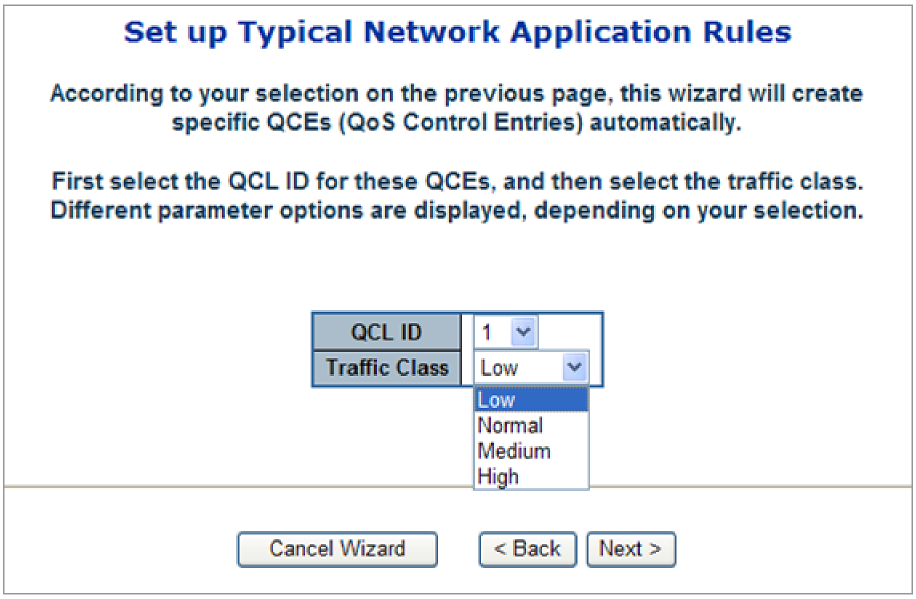
Cancal Wizard : Click to cancel the wizard.

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

Netx > : Click to continue the wizard.

- **STEP-2**

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



Set up Typical Network Application Rules

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 your selection.

QCL ID	1
Traffic Class	Low

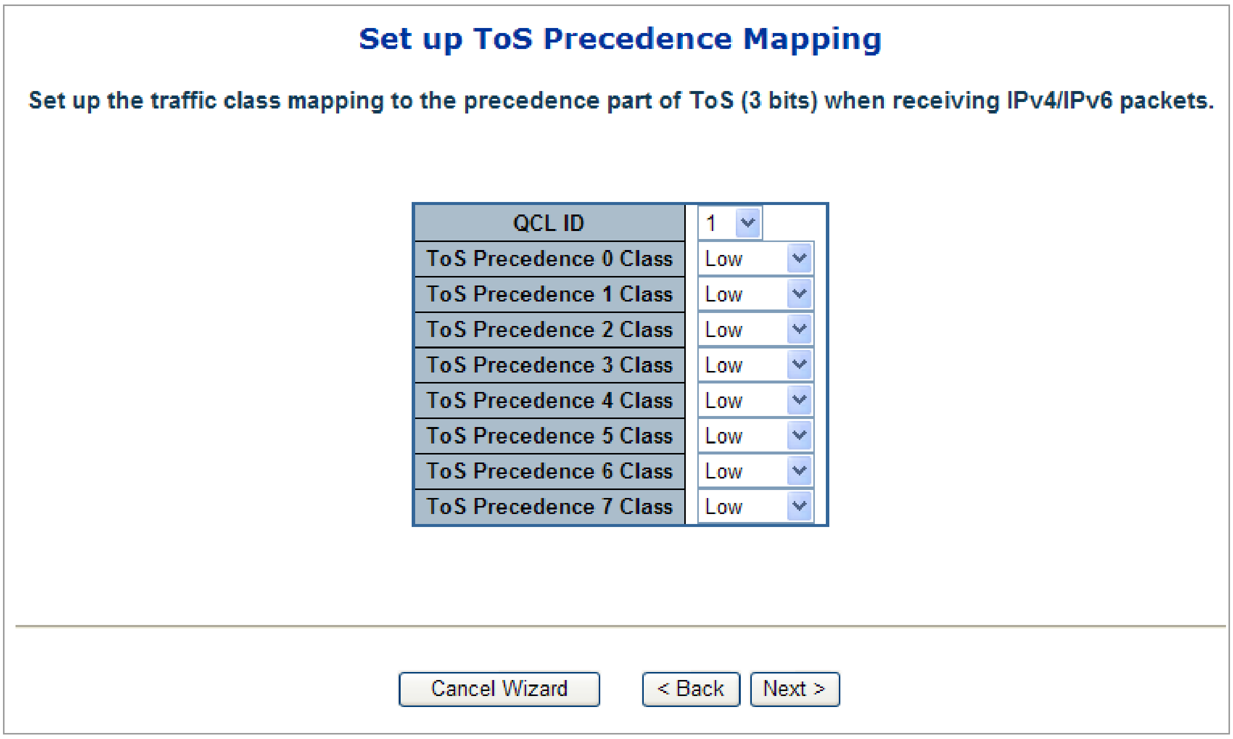
Figure 4-9-5 Set up Typical Netowrk Application Rules page 2 screenshot

The page includes the folling fileds:

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

4.9.2.3 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 screen in Figure 4-9-6 appears.



Set up ToS Precedence Mapping

Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.

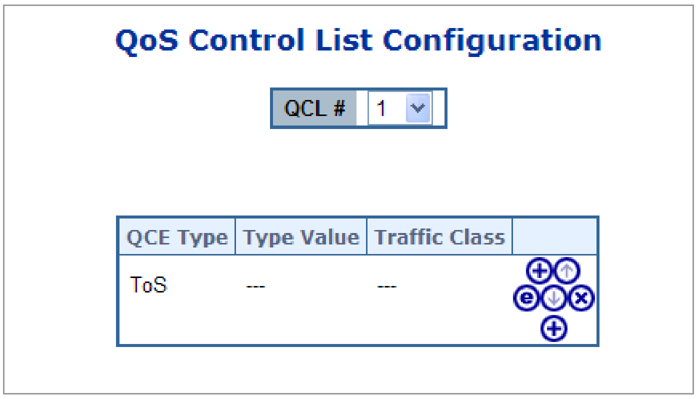
QCL ID	1
ToS Precedence 0 Class	Low
ToS Precedence 1 Class	Low
ToS Precedence 2 Class	Low
ToS Precedence 3 Class	Low
ToS Precedence 4 Class	Low
ToS Precedence 5 Class	Low
ToS Precedence 6 Class	Low
ToS Precedence 7 Class	Low

Figure 4-9-6 Set up ToS Precedence Mapping page screenshot

The page includes the folling fileds:

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

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



QoS Control List Configuration

QCL # 1

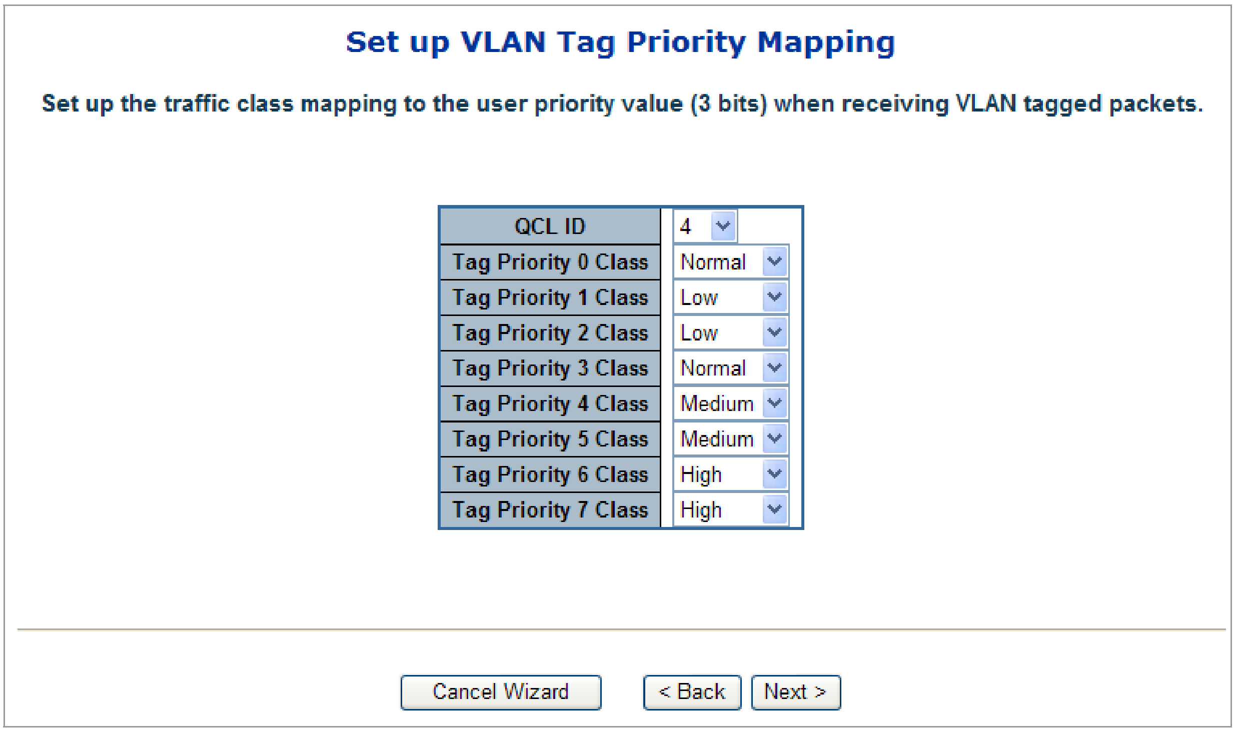
QCE Type	Type Value	Traffic Class
ToS	---	---

Figure 4-9-7 Set up ToS Precedence Mapping page screenshot

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 screen in Figure 4-9-8 appears.



Set up VLAN Tag Priority Mapping

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

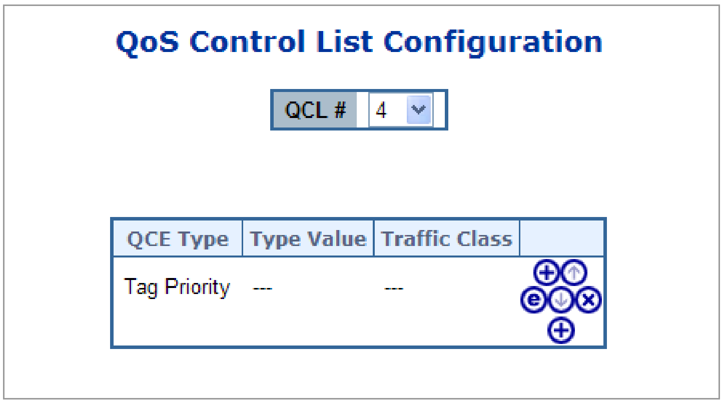
QCL ID	4
Tag Priority 0 Class	Normal
Tag Priority 1 Class	Low
Tag Priority 2 Class	Low
Tag Priority 3 Class	Normal
Tag Priority 4 Class	Medium
Tag Priority 5 Class	Medium
Tag Priority 6 Class	High
Tag Priority 7 Class	High

Figure 4-9-8 Set up VLAN Tag Priority Mapping page screenshot

The page includes the folling fileds:

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

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



QoS Control List Configuration

QCL # 4

QCE Type	Type Value	Traffic Class	
Tag Priority	---	---	

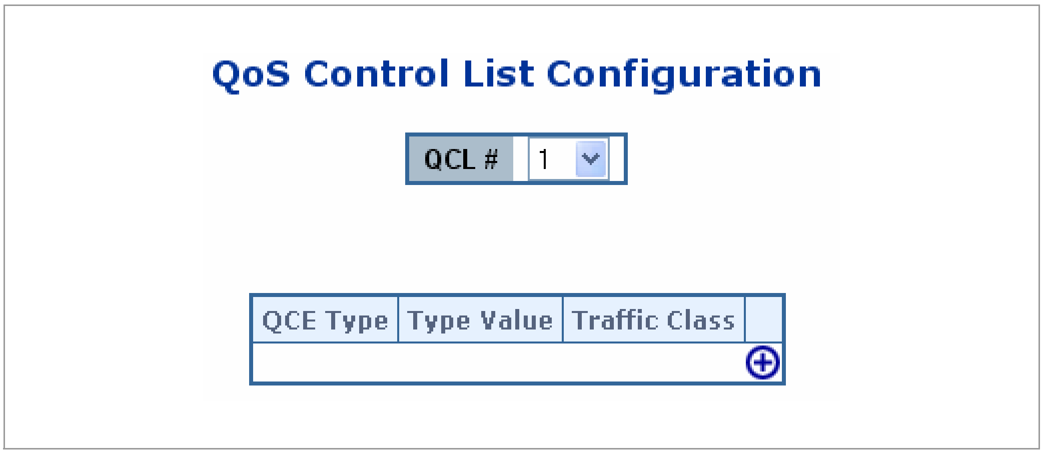
Figure 4-9-9 Set up VLAN Tag Priority Mapping page screenshot

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 4-9-10 appears.



QoS Control List Configuration

QCL # 1

QCE Type	Type Value	Traffic Class	
			⊕

Figure 4-9-10 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.

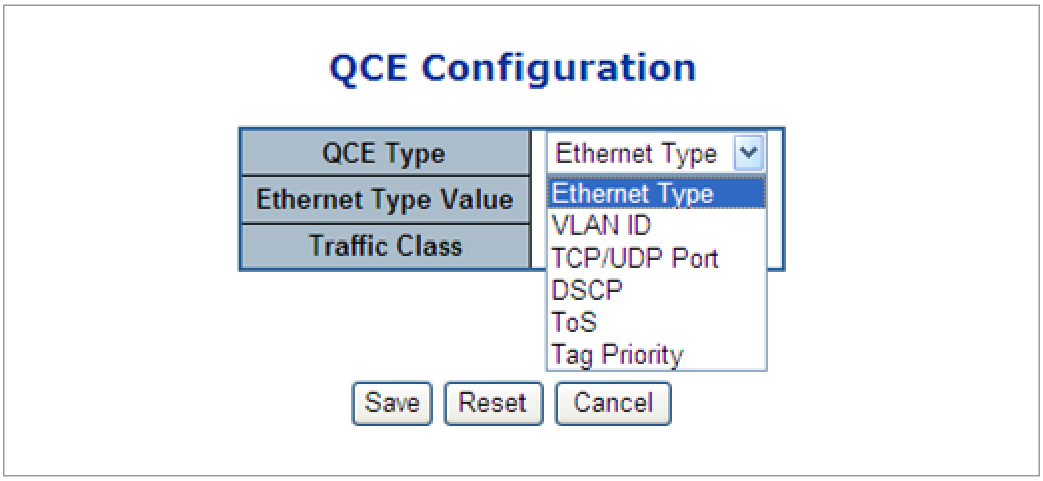
4.9.3.1 QoS Control Entry Configuration

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 4-9-11 appears.



QCE Configuration

QCE Type	Ethernet Type
Ethernet Type Value	
Traffic Class	

Figure 4-9-11 QCE Configuration page screenshot

The page includes the following fields:

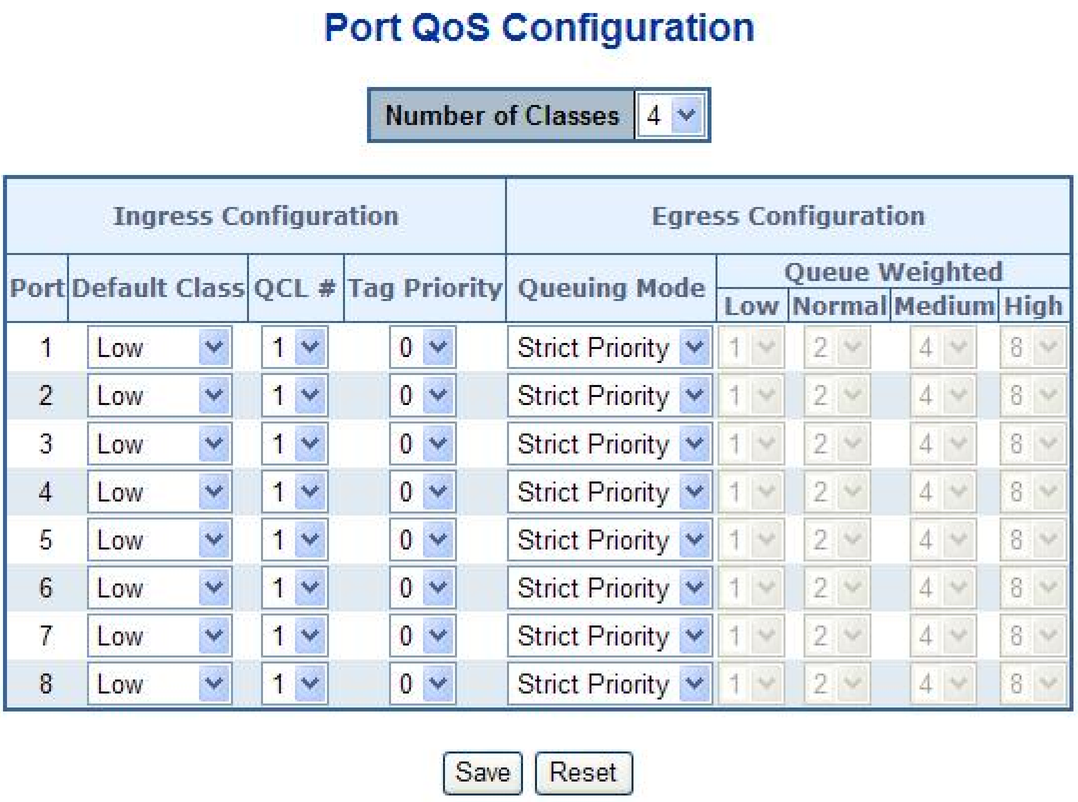
Object	Description
- **QCE Type**	Select the available type for the specific QCE. - **Ethernet Type**: Matches the received frame's EtherType against the QCE Key. - **VLAN ID**: Matches the frame's VID against the QCE Key. - **TCP/UDP Port**: Matches the destination port and the source port against the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

4.9.4 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 4-9-12 appears.



Port QoS Configuration

Number of Classes: 4

Ingress Configuration				Egress Configuration				
					Queue Weighted			
Port	Default Class	QCL #	Tag Priority	Queuing Mode	Low	Normal	Medium	High
1	Low	1	0	Strict Priority	1	2	4	8
2	Low	1	0	Strict Priority	1	2	4	8
3	Low	1	0	Strict Priority	1	2	4	8
4	Low	1	0	Strict Priority	1	2	4	8
5	Low	1	0	Strict Priority	1	2	4	8
6	Low	1	0	Strict Priority	1	2	4	8
7	Low	1	0	Strict Priority	1	2	4	8
8	Low	1	0	Strict Priority	1	2	4	8

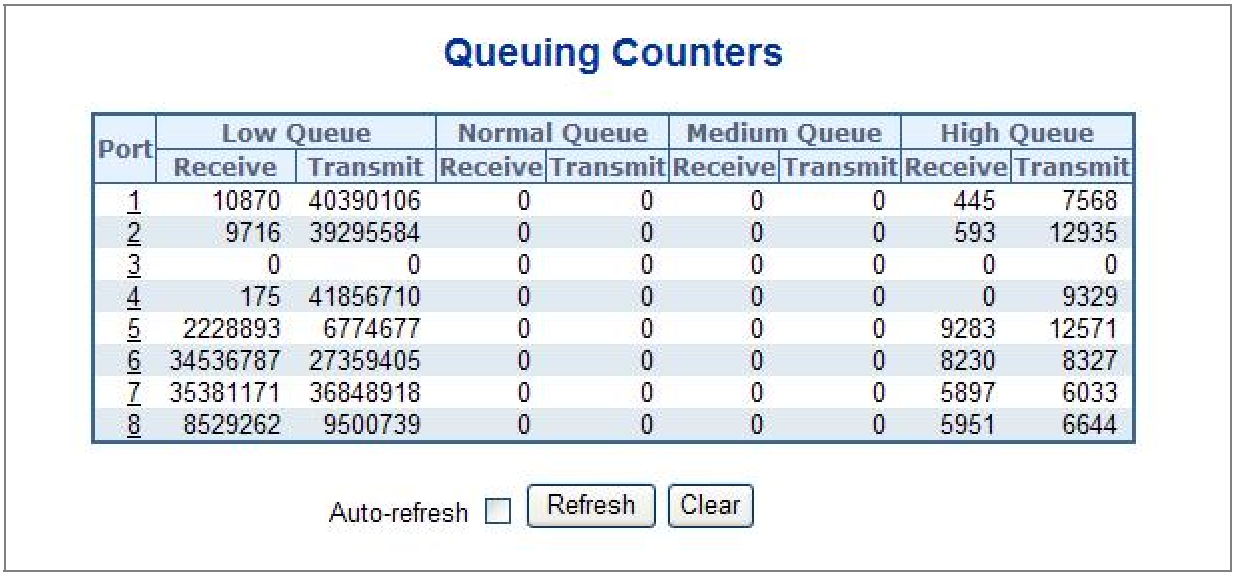
Figure 4-9-12 Port QoS Configuration page screenshot

The page includes the following fields:

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

4.9.5 QoS Statistics

This page provides statistics for the different queues for all switch ports. The ports belong to the currently selected stack unit, as reflected by the page header. The QoS Statistics screen in Figure 4-9-13 appears.



Queuing Counters

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	10870	40390106	0	0	0	0	445	7568
2	9716	39295584	0	0	0	0	593	12935
3	0	0	0	0	0	0	0	0
4	175	41856710	0	0	0	0	0	9329
5	2228893	6774677	0	0	0	0	9283	12571
6	34536787	27359405	0	0	0	0	8230	8327
7	35381171	36848918	0	0	0	0	5897	6033
8	8529262	9500739	0	0	0	0	5951	6644

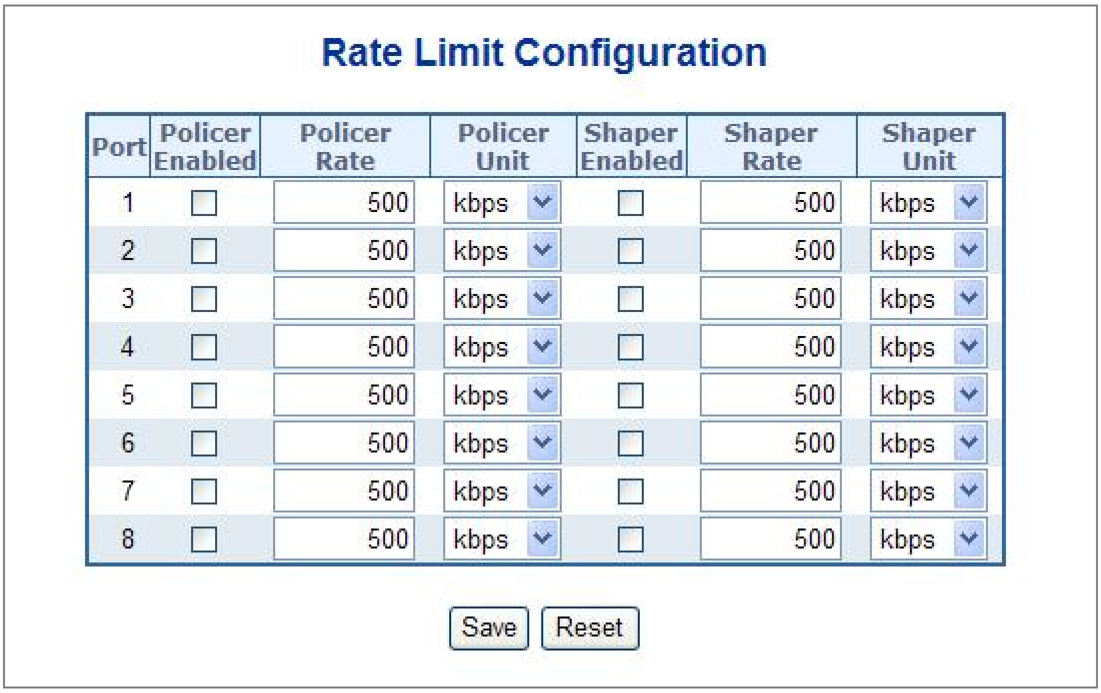
Figure 4-9-13 QoS Statistics page screenshot

The page includes the following fields:

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

4.9.6 Bandwidth Control

Configure the switch port rate limit for Policers and Shapers on this page. The settings relate to the currently selected stack unit, as reflected by the page header. The screen Bandwidth Control in Figure 4-9-14 appears.



Rate Limit Configuration

Port	Policer Enabled	Policer Rate	Policer Unit	Shaper Enabled	Shaper Rate	Shaper Unit
1	□	500	kbps	□	500	kbps
2	□	500	kbps	□	500	kbps
3	□	500	kbps	□	500	kbps
4	□	500	kbps	□	500	kbps
5	□	500	kbps	□	500	kbps
6	□	500	kbps	□	500	kbps
7	□	500	kbps	□	500	kbps
8	□	500	kbps	□	500	kbps

Figure 4-9-14 Bandwidth Control 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".

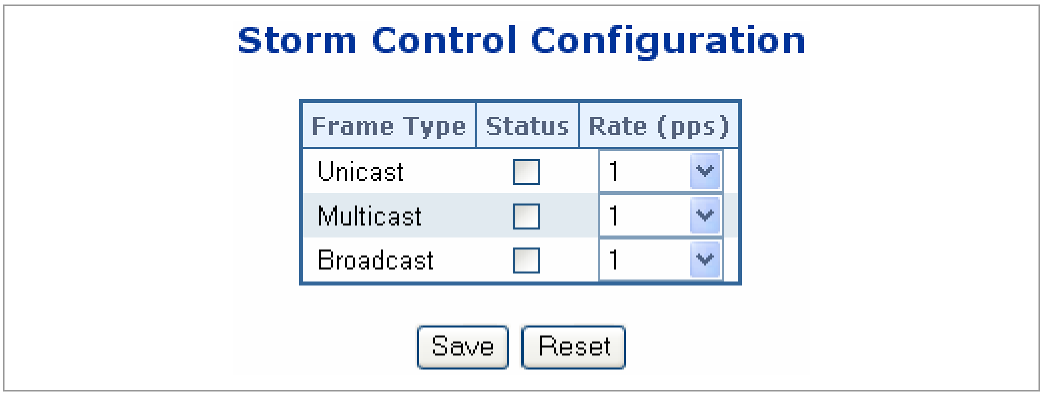
4.9.7 Storm Control Configuration

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

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

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

The Storm Control Configuration screen in Figure 4-9-15 appears.



Storm Control Configuration

Frame Type	Status	Rate (pps)
Unicast	□	1
Multicast	□	1
Broadcast	□	1

Figure 4-9-15 Storm Control Configuration page screenshot

The page includes the following fields:

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

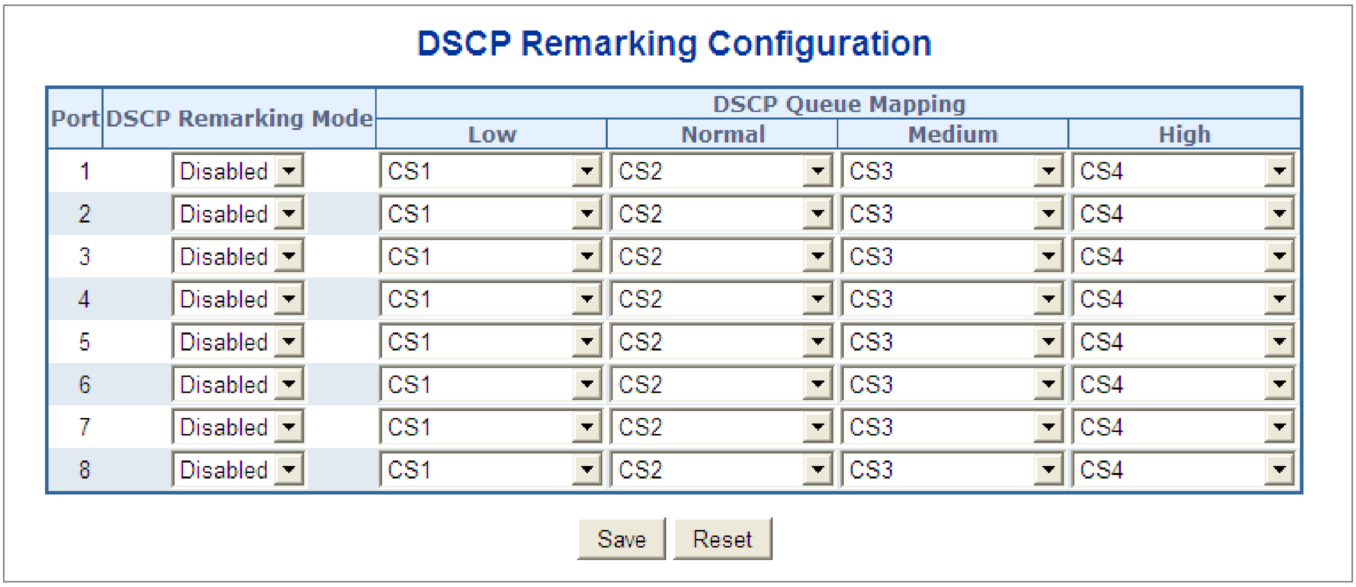
4.9.8 DSCP Remarking

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.



DSCP Remarking Configuration

Port	DSCP Remarking Mode	DSCP Queue Mapping			
		Low	Normal	Medium	High
1	Disabled	CS1	CS2	CS3	CS4
2	Disabled	CS1	CS2	CS3	CS4
3	Disabled	CS1	CS2	CS3	CS4
4	Disabled	CS1	CS2	CS3	CS4
5	Disabled	CS1	CS2	CS3	CS4
6	Disabled	CS1	CS2	CS3	CS4
7	Disabled	CS1	CS2	CS3	CS4
8	Disabled	CS1	CS2	CS3	CS4

Figure 4-9-16 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)

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.

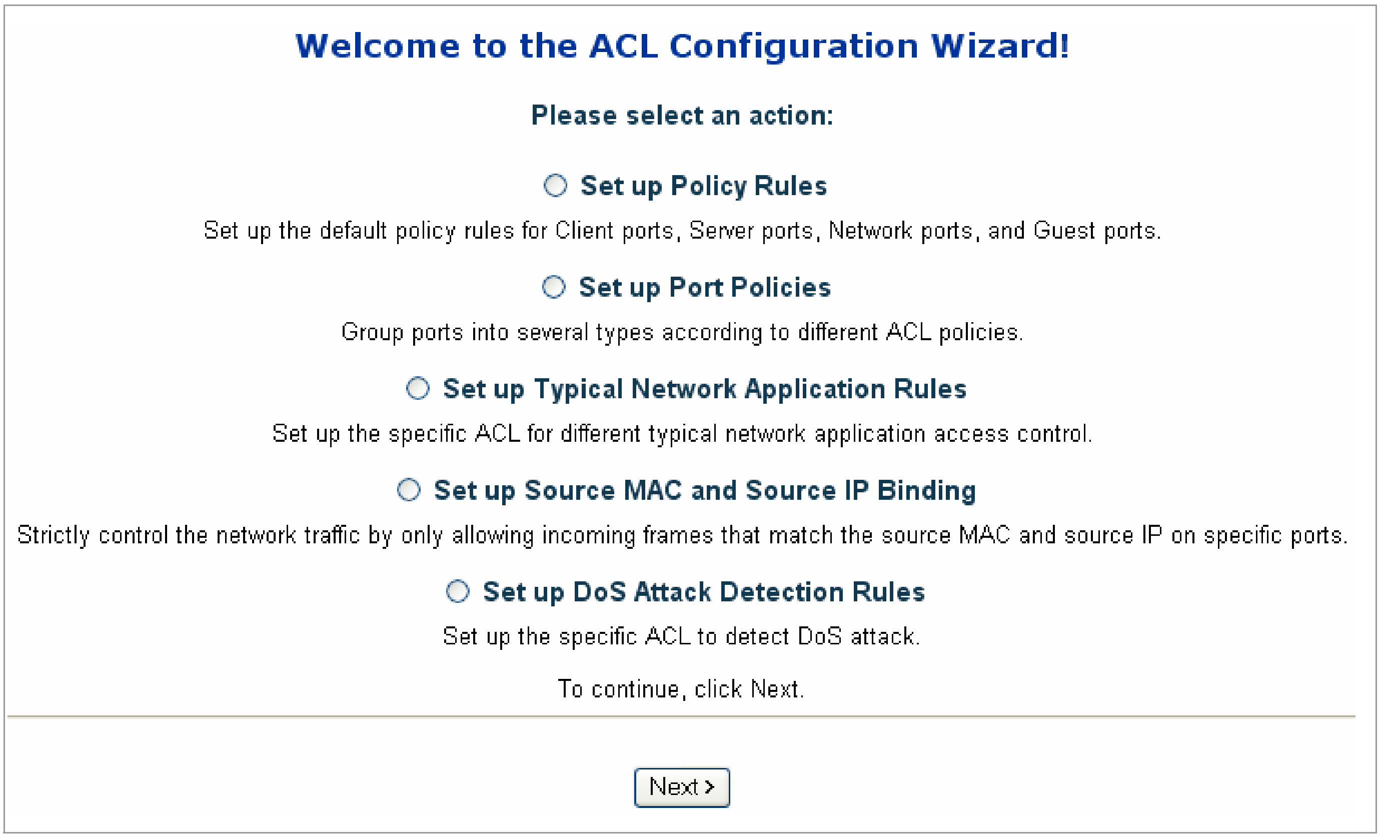
ACE is an acronym for **Access Control Entry**. It describes access permission associated with a particular ACE ID.

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 ACL Configuration wizard

This handy wizard helps you set up an ACL quickly.

The ACL Configuration wizard screen in Figure 4-10-1 appears.



Welcome to the ACL Configuration Wizard!

Please select an action:

○ Set up Policy Rules

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

○ Set up Port Policies

Group ports into several types according to different ACL policies.

○ Set up Typical Network Application Rules

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

○ Set up Source MAC and Source IP Binding

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

○ Set up DoS Attack Detection Rules

Set up the specific ACL to detect DoS attack.

To continue, click Next.

Figure 4-10-1 welcome to the ACL Configuration wizard page screenshot

The page includes the following fields:

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

4.10.1.1 Set up Policy Rules

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

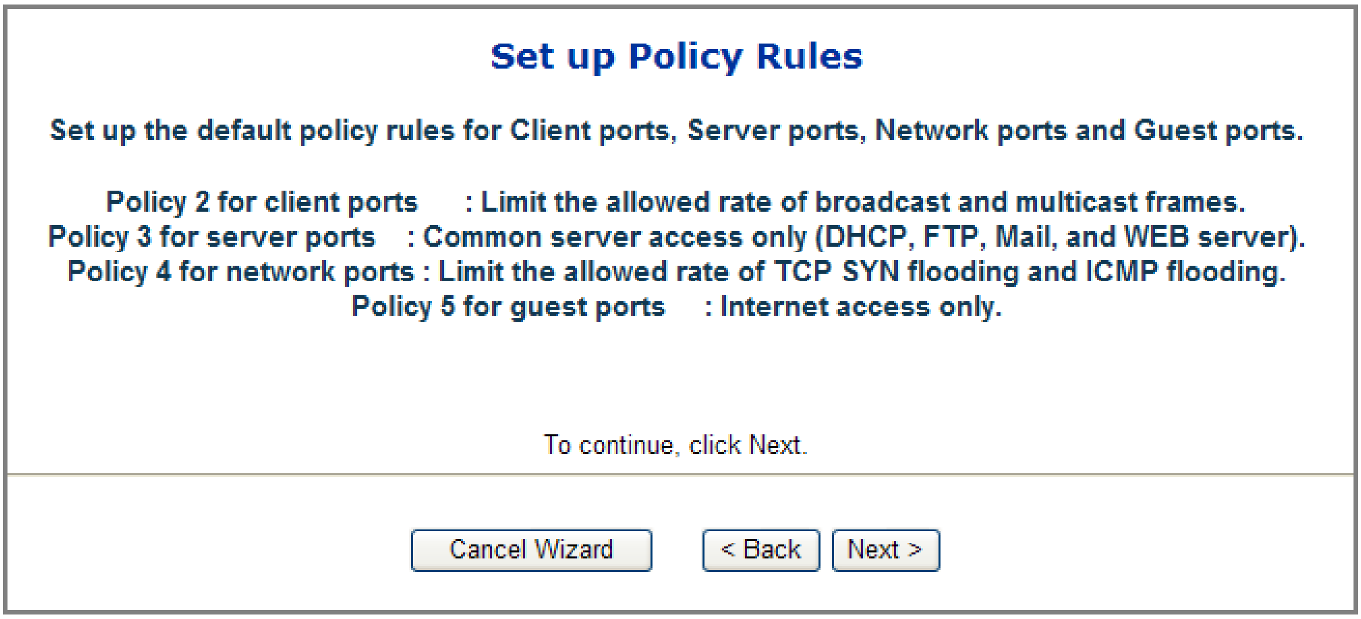
Policy 2 for client ports: Limit the allowed rate of broadcast and multicast frames.

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

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

Policy 5 for guest ports: Internet access only.

The screen in Figure 4-10-2 appears.



Set up Policy Rules

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

Policy 2 for client ports : Limit the allowed rate of broadcast and multicast frames.
Policy 3 for server ports : Common server access only (DHCP, FTP, Mail, and WEB server).
Policy 4 for network ports : Limit the allowed rate of TCP SYN flooding and ICMP flooding.
Policy 5 for guest ports : Internet access only.

To continue, click Next.

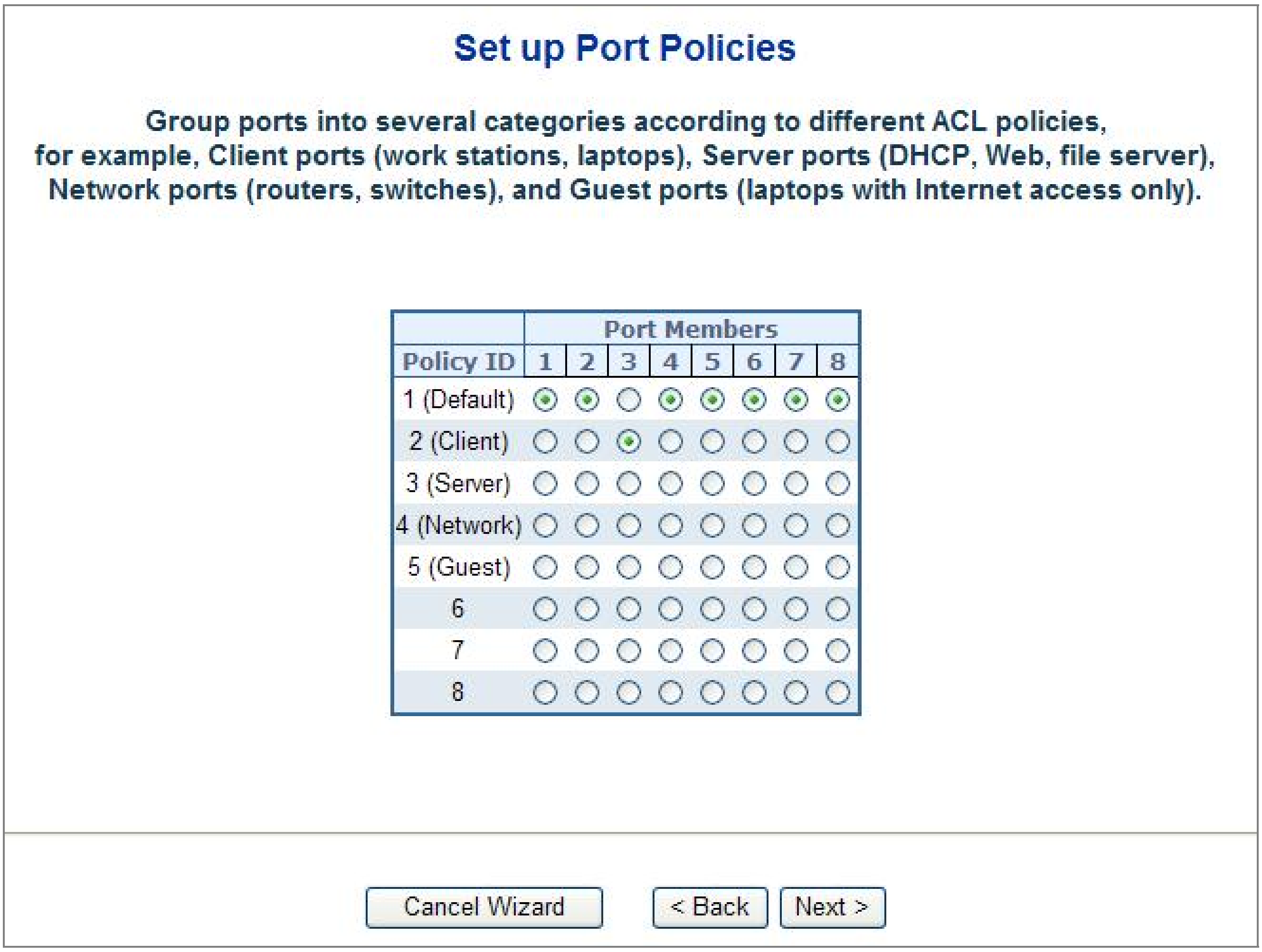
Figure 4-10-2 Set up Policy Rules page screenshot

4.10.1.2 Set up Port Policies

Group ports into several types according to different ACL policies.

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

The screen in Figure 4-10-3 appears.



Set up Port Policies

Group ports into several categories according to different ACL policies, for example, Client ports (work stations, laptops), Server ports (DHCP, Web, file server), Network ports (routers, switches), and Guest ports (laptops with Internet access only).

	Port Members							
Policy ID	1	2	3	4	5	6	7	8
1 (Default)	●	●	○	●	●	●	●	●
2 (Client)	○	○	●	○	○	○	○	○
3 (Server)	○	○	○	○	○	○	○	○
4 (Network)	○	○	○	○	○	○	○	○
5 (Guest)	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○
7	○	○	○	○	○	○	○	○
8	○	○	○	○	○	○	○	○

Figure 4-10-3 Set up Port Policies page screenshot

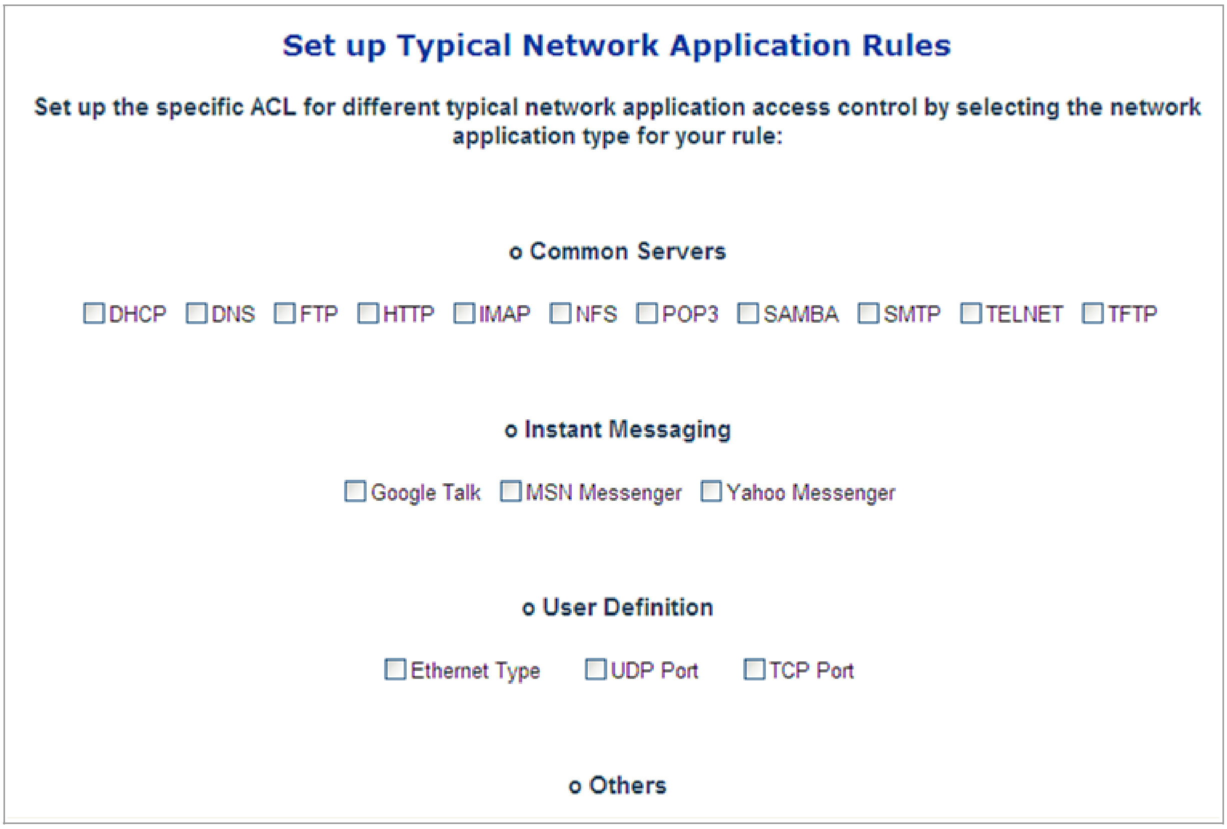
The page includes the following fields:

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

4.10.1.3 Set up Typical Network Application Rules

Set up the specific ACL for different typical network application access control. The screen in Figure 4-10-4 appears.

- **STEP-1: Selecting the Network Application Type:**



Set up Typical Network Application Rules

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

○ Common Servers

□DHCP □DNS □FTP □HTTP □IMAP □NFS □POP3 □SAMBA □SMTP □TELNET □TFTP

○ Instant Messaging

□Google Talk □MSN Messenger □Yahoo Messenger

○ User Definition

□Ethernet Type □UDP Port □TCP Port

○ Others

Figure 4-10-4 Set up Typical network Application Rules page screenshot

The page includes the following fields:

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

	range is **0** to **65535**.
- **Others**	Indicates the other application that applies to the specific ACE. The other applications are: **HTTPS**, **ICMP**, **Multicast IP Stream**, **NetBIOS**, **PING Request**, **Ping Reply**, **SNMP**, **SNMP Traps**.

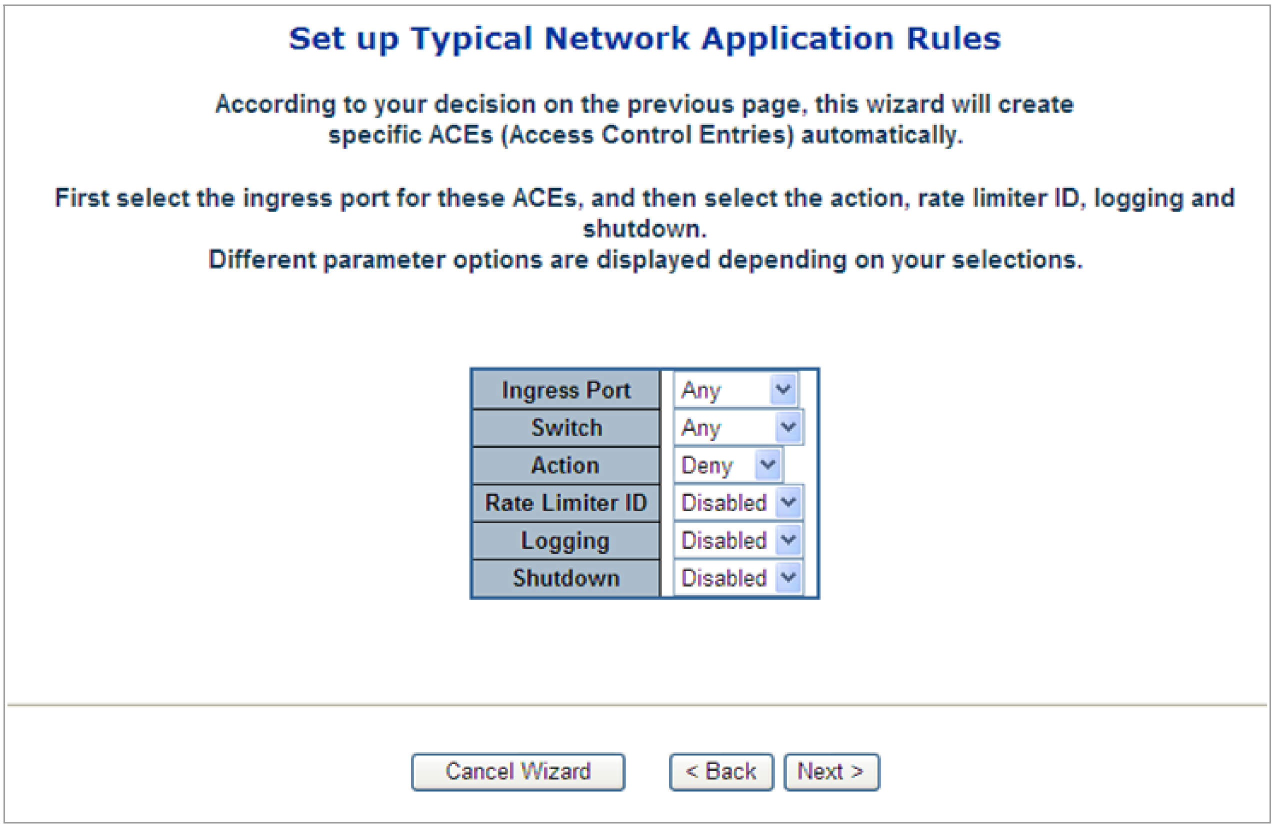
■ STEP-2: Define and Apply the Typeical Netowrk Application Rules:

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

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

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

The screen in Figure 4-10-5 appears.



Set up Typical Network Application Rules

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

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

Different parameter options are displayed depending on your selections.

Ingress Port	Any
Switch	Any
Action	Deny
Rate Limiter ID	Disabled
Logging	Disabled
Shutdown	Disabled

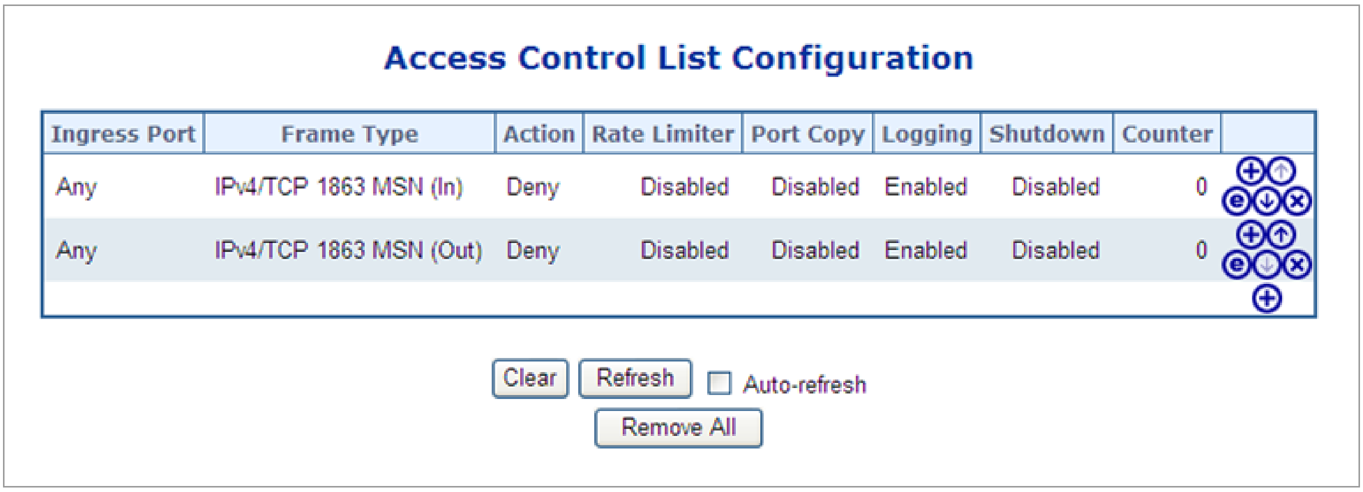
Figure 4-10-5 Set up Typical network Application Rules screenshot

The page includes the following fields:

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

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

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



Access Control List Configuration

Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Logging	Shutdown	Counter	
Any	IPv4/TCP 1863 MSN (In)	Deny	Disabled	Disabled	Enabled	Disabled	0	
Any	IPv4/TCP 1863 MSN (Out)	Deny	Disabled	Disabled	Enabled	Disabled	0	

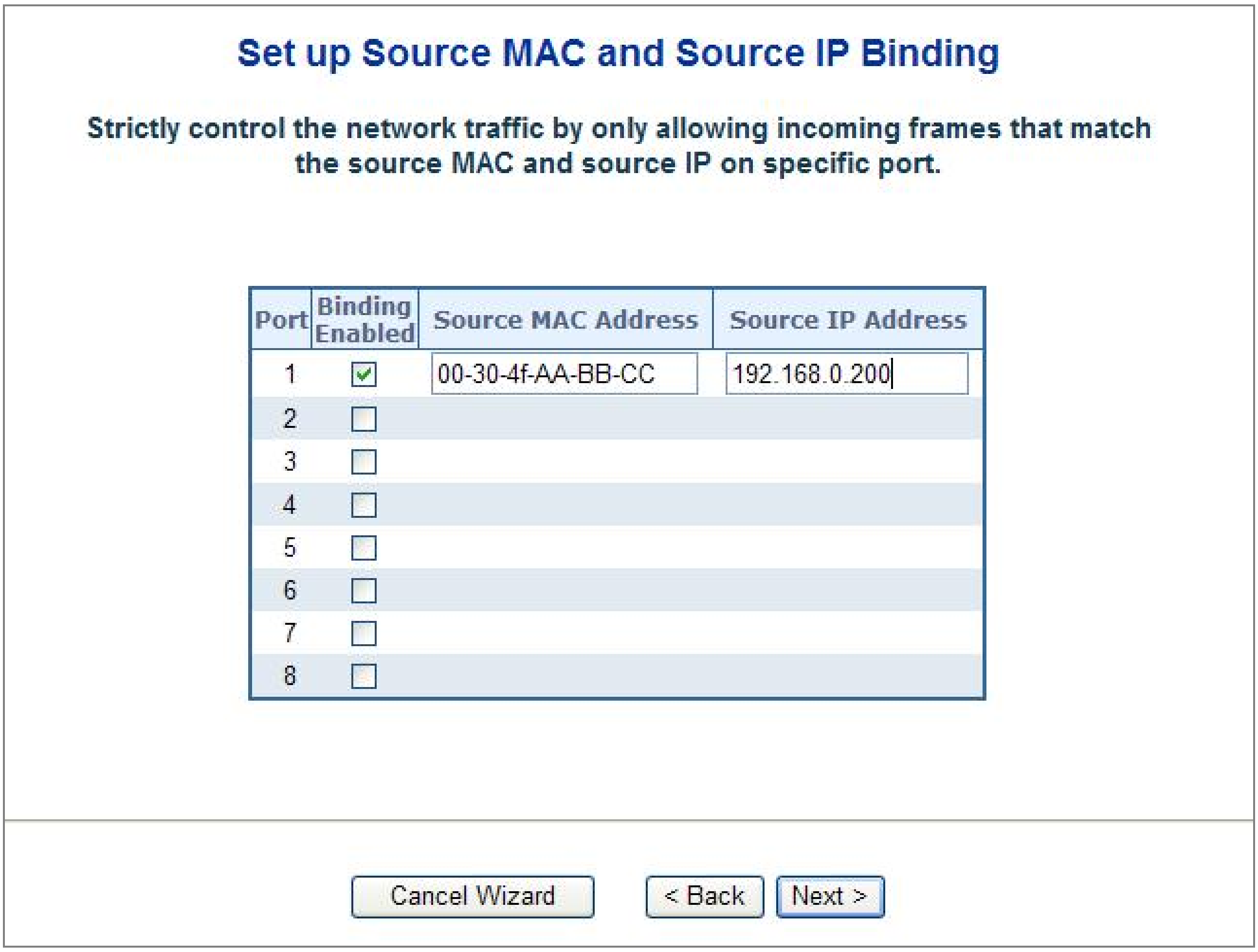
Figure 4-10-6 Access Control List Configuration page screenshot

4.10.1.4 Set up Source MAC and Source IP Binding

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

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

The screen in Figure 4-10-7 appears.



Set up Source MAC and Source IP Binding

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

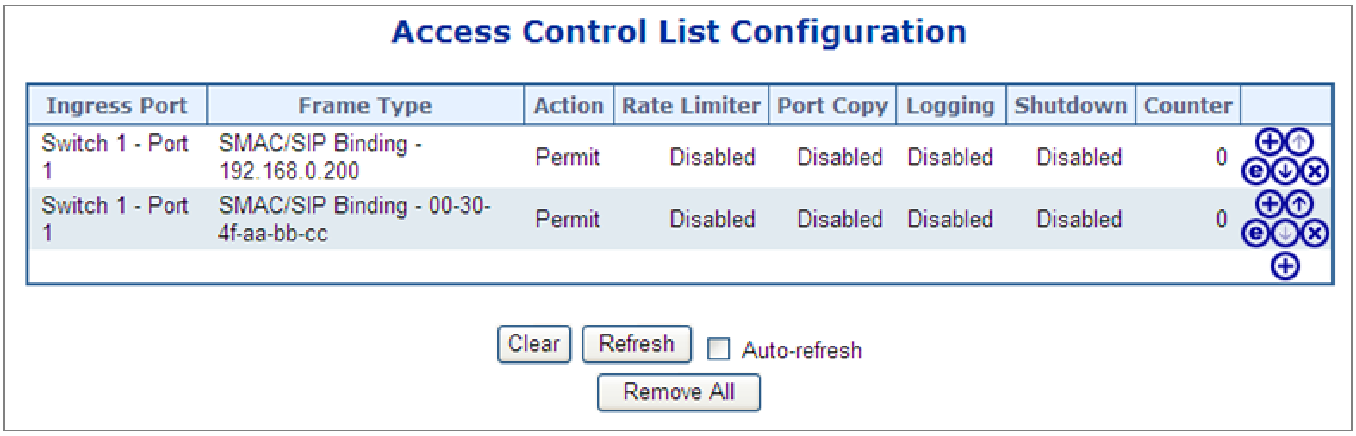
Port	Binding Enabled	Source MAC Address	Source IP Address
1	☑	00-30-4f-AA-BB-CC	192.168.0.200
2	□		
3	□		
4	□		
5	□		
6	□		
7	□		
8	□		

Figure 4-10-7 Set up Source MAC and Secure IP Binding page screenshot

The page includes the following fields:

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

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



Access Control List Configuration

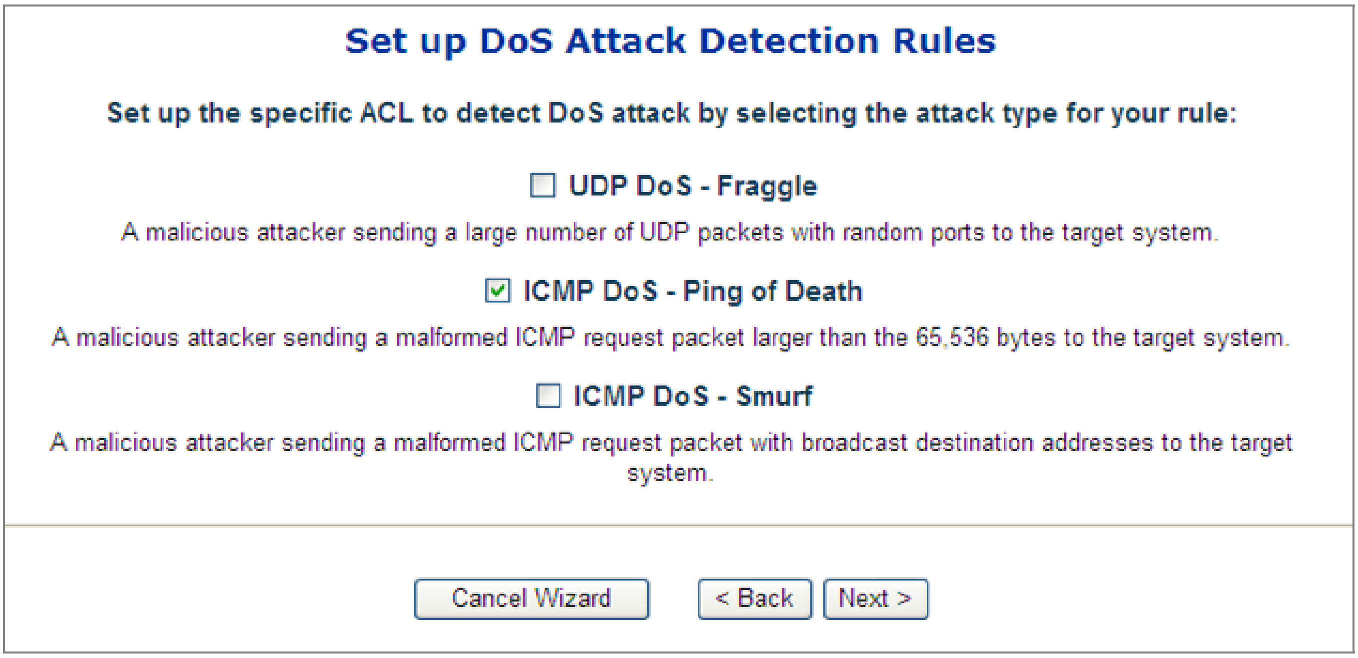
Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Logging	Shutdown	Counter	
Switch 1 - Port 1	SMAC/SIP Binding - 192.168.0.200	Permit	Disabled	Disabled	Disabled	Disabled	0	⊕ ↑ e ↓ ×
Switch 1 - Port 1	SMAC/SIP Binding - 00-30-4f-aa-bb-cc	Permit	Disabled	Disabled	Disabled	Disabled	0	⊕ ↑ e ↓ ×
								⊕

Figure 4-10-8 Access Control List Configuration page screenshot

4.10.1.5 Set up DoS Attack Detection Rules

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

The screen in Figure 4-10-9 appears.



Set up DoS Attack Detection Rules

Set up the specific ACL to detect DoS attack by selecting the attack type for your rule:

□ UDP DoS - Fraggle

A malicious attacker sending a large number of UDP packets with random ports to the target system.

☑ ICMP DoS - Ping of Death

A malicious attacker sending a malformed ICMP request packet larger than the 65,536 bytes to the target system.

□ ICMP DoS - Smurf

A malicious attacker sending a malformed ICMP request packet with broadcast destination addresses to the target system.

Figure 4-10-9 Set up DoS Attack Detection Rules page screenshot

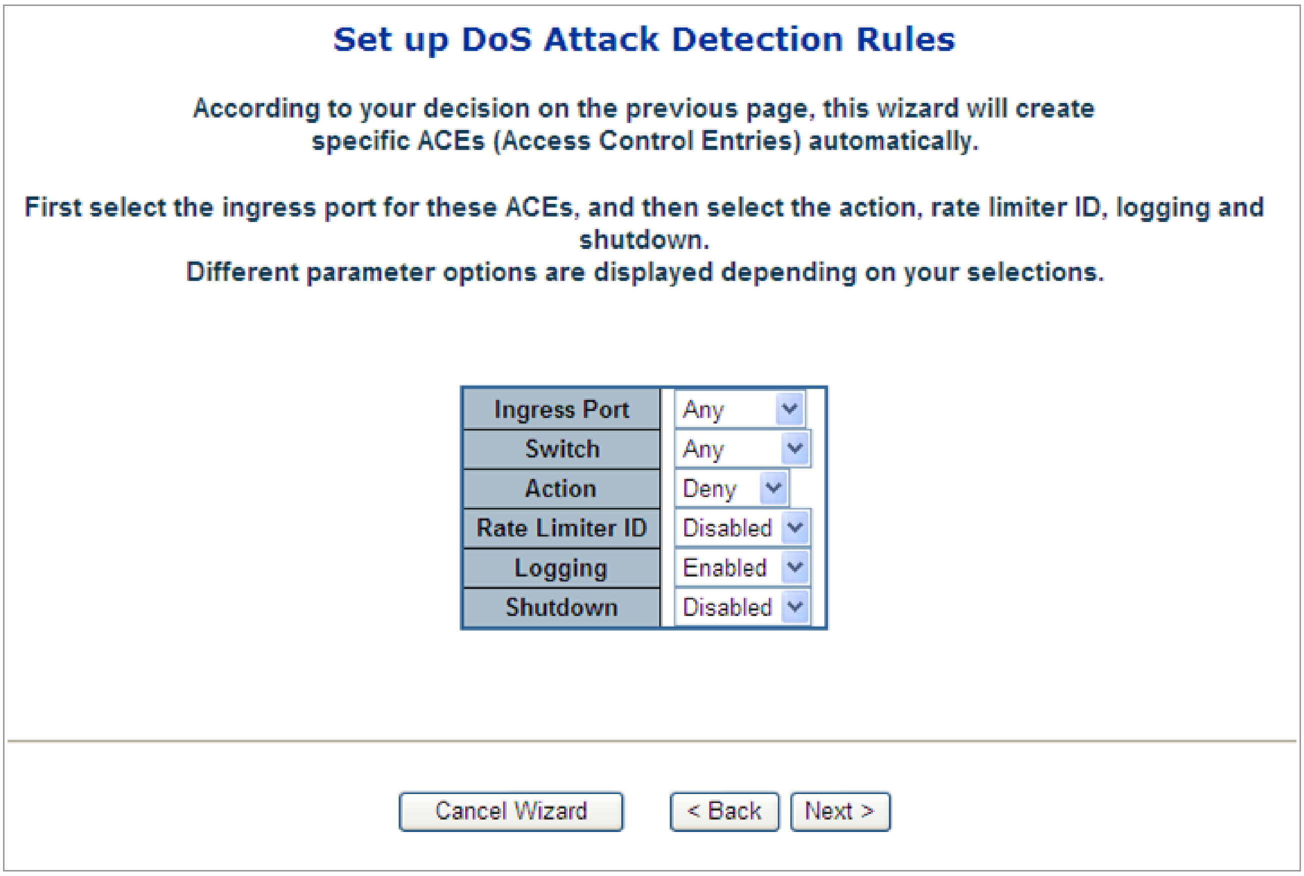
The page includes the following fields:

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

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

4.10.1.6 Set up DoS Attack Detection Rules

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



Set up DoS Attack Detection Rules

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

First select the ingress port for these ACEs, and then select the action, rate limiter ID, logging and shutdown.
Different parameter options are displayed depending on your selections.

Ingress Port	Any
Switch	Any
Action	Deny
Rate Limiter ID	Disabled
Logging	Enabled
Shutdown	Disabled

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

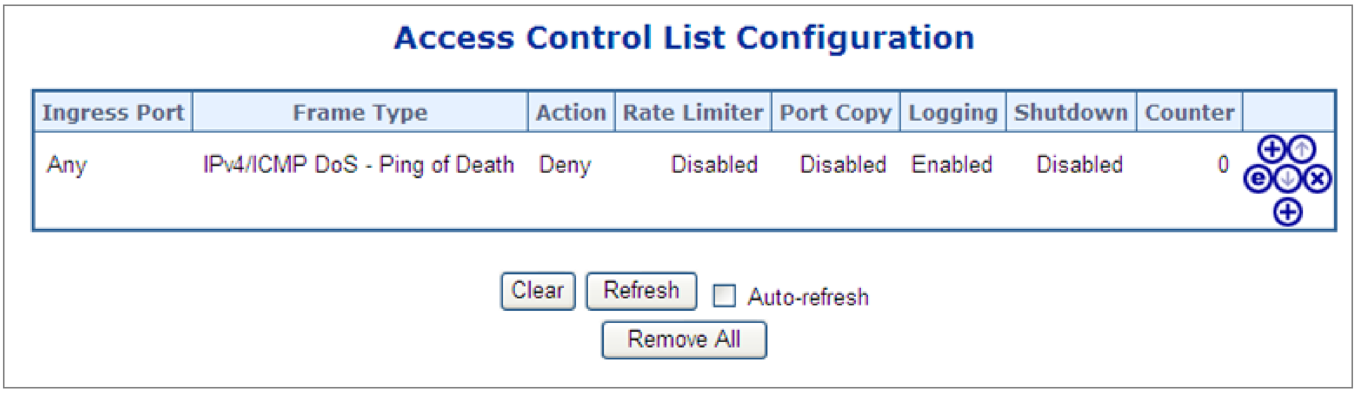
The page includes the following fields:

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

Note

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

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



Access Control List Configuration

Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Logging	Shutdown	Counter	
Any	IPv4/ICMP DoS - Ping of Death	Deny	Disabled	Disabled	Enabled	Disabled	0	

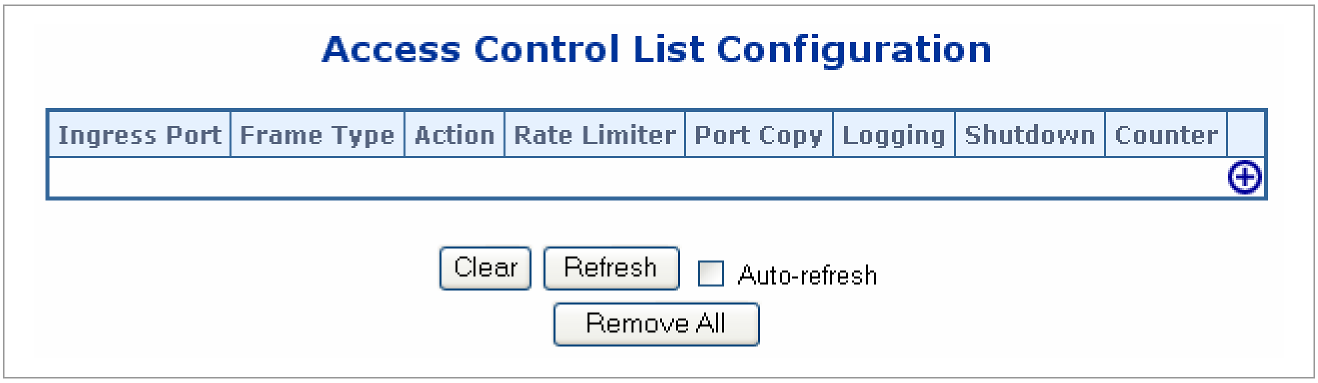
Figure 4-10-11 Access Control List Configuration page screenshot

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 4-10-12 appears.



Access Control List Configuration

Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Logging	Shutdown	Counter	
								⊕

Figure 4-10-12 Access Control List Configuration page screenshot

The page includes the following fields:

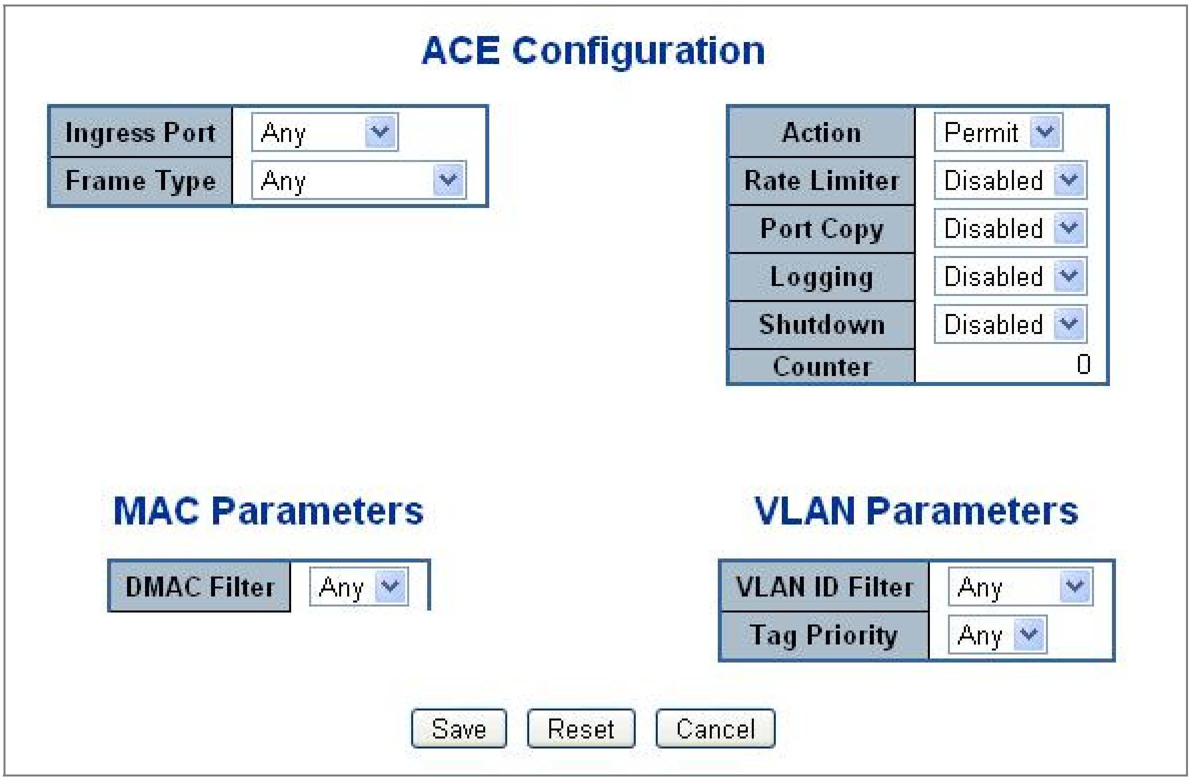
Object	Description
• **Ingress Port**	Indicates the ingress port of the ACE. Possible values are: • **Any:** The ACE will match any ingress port. • **Policy**: The ACE will match ingress ports with a specific policy. • **Port:** The ACE will match a specific ingress port.
• **Frame Type**	Indicates the 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.

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.

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



ACE Configuration

Ingress Port	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Port Copy	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

DMAC Filter	Any

VLAN Parameters

VLAN ID Filter	Any
Tag Priority	Any

Figure 4-10-13 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.
• **Switch**	Select the switch to which this ACE applies. ■ **Any**: The ACE applies to any port. ■ Switch n: The ACE applies to this switch number, where n is the number of the **switch**.
• **Frame Type**	Select the frame type for this ACE. ■ **Any**: Any frame can match this ACE. ■ **Ethernet Type**: Only Ethernet Type frames can match this ACE.

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

■ **MAC Parameters**

The page includes the following fields:

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

The page includes the following fields:

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.

The page includes the following fields:

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.

The page includes the following fields:

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

The page includes the following fields:

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

The page includes the following fields:

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**	When "Specific" is selected for the TCP/UDP destination filter, you can enter a

Number	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.

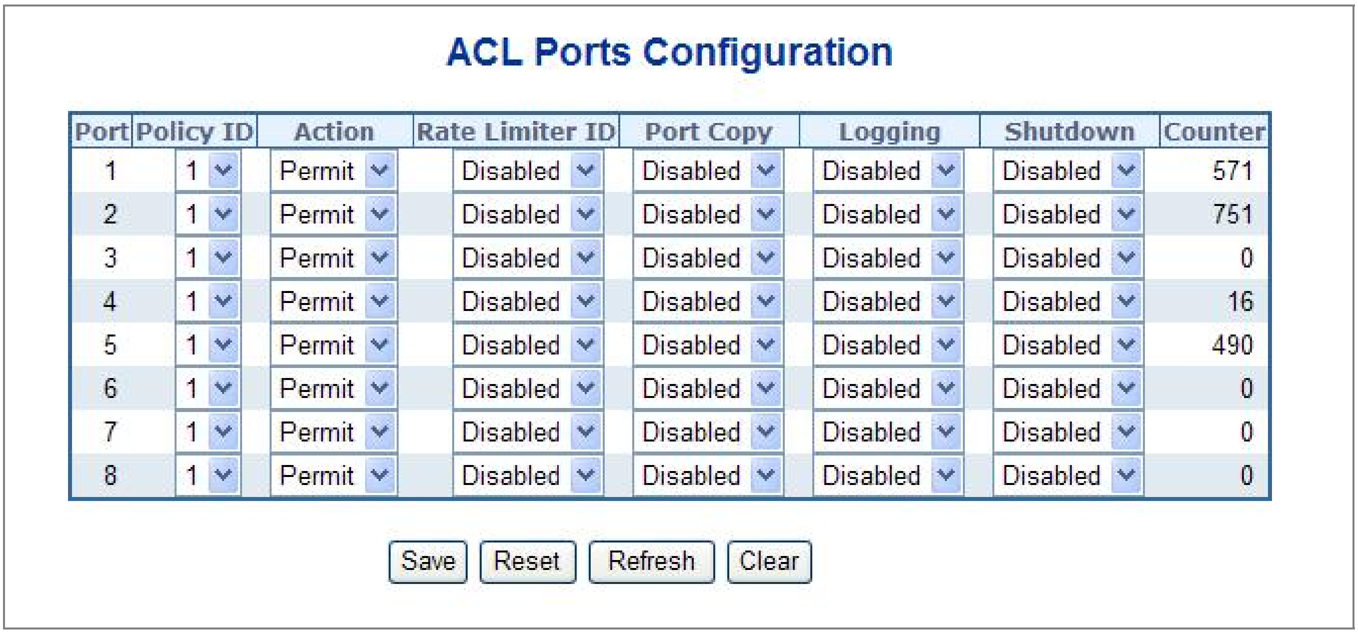
The page includes the following fields:

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

4.10.4 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 4-10-14 appears.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Logging	Shutdown	Counter
1	1	Permit	Disabled	Disabled	Disabled	Disabled	571
2	1	Permit	Disabled	Disabled	Disabled	Disabled	751
3	1	Permit	Disabled	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled	Disabled	Disabled	16
5	1	Permit	Disabled	Disabled	Disabled	Disabled	490
6	1	Permit	Disabled	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	Disabled	Disabled	0
8	1	Permit	Disabled	Disabled	Disabled	Disabled	0

Figure 4-10-14 ACL Ports Configuration page screenshot

The page includes the following fields:

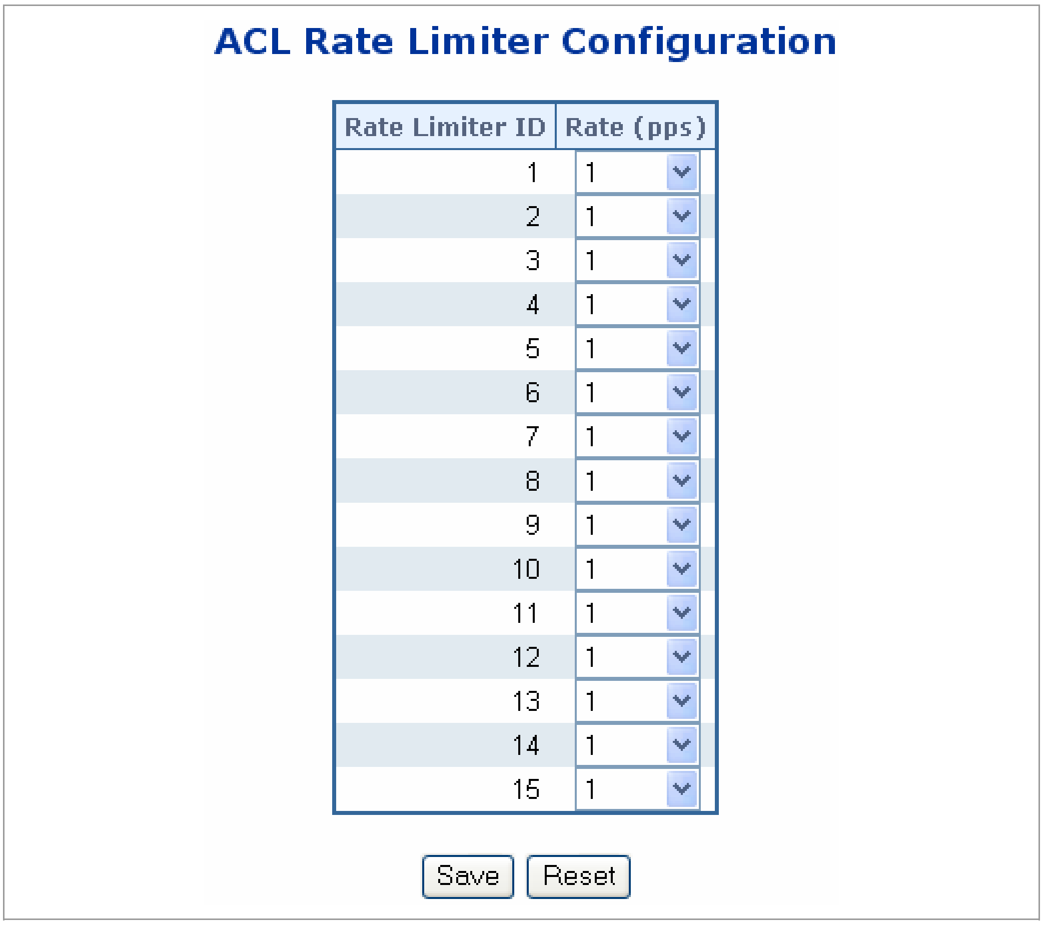
Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Policy ID**	Select the policy to apply to this port. The allowed values are **1** through **8**. The default value is 1.
• **Action**	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
• **Rate Limiter ID**	Select which rate limiter to apply to this port. The allowed values are **Disabled** or the values **1** through **15**. The default value is "Disabled".
• **Port Copy**	Select which port frames are copied to. The allowed values are **Disabled** or a specific port number. The default value is "Disabled".
• **Logging**	Specify the logging operation of this port. The allowed values are: • **Enabled**: Frames received on the port are stored in the System Log. • **Disabled**: Frames received on the port are not logged.

	The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.
• **Shutdown**	Specify the port shut down operation of this port. The allowed values are: • **Enabled**: If a frame is received on the port, the port will be disabled. • **Disabled**: Port shut down is disabled. The default value is "Disabled".
• **Counter**	Counts the number of frames that match this ACE.

4.10.5 ACL Rate Limiter Configuration

Configure the rate limiter for the ACL of the Managed Switch.

The ACL Rate Limiter Configuration screen in Figure 4-10-15 appears.



ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
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

Figure 4-10-15 ACL Rate Limiter Configuration page screenshot

The page includes the following fields:

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

4.11 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.

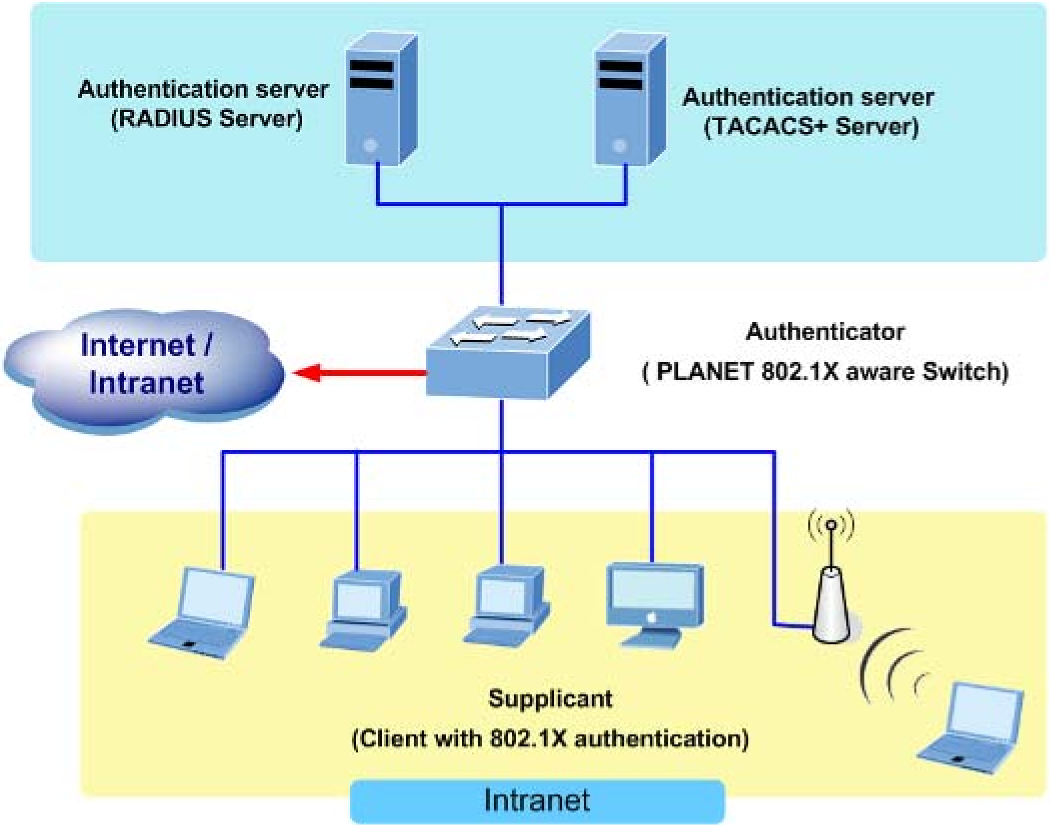


Figure 4-11-1

- ***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

Note

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.

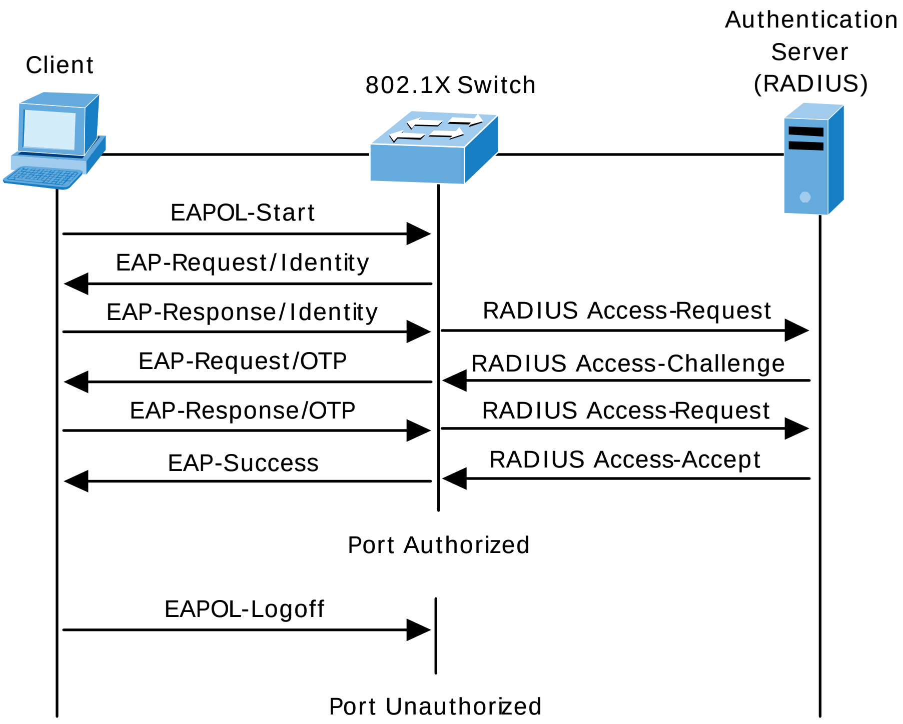


Figure 4-11-2 EAP message exchange

■ **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

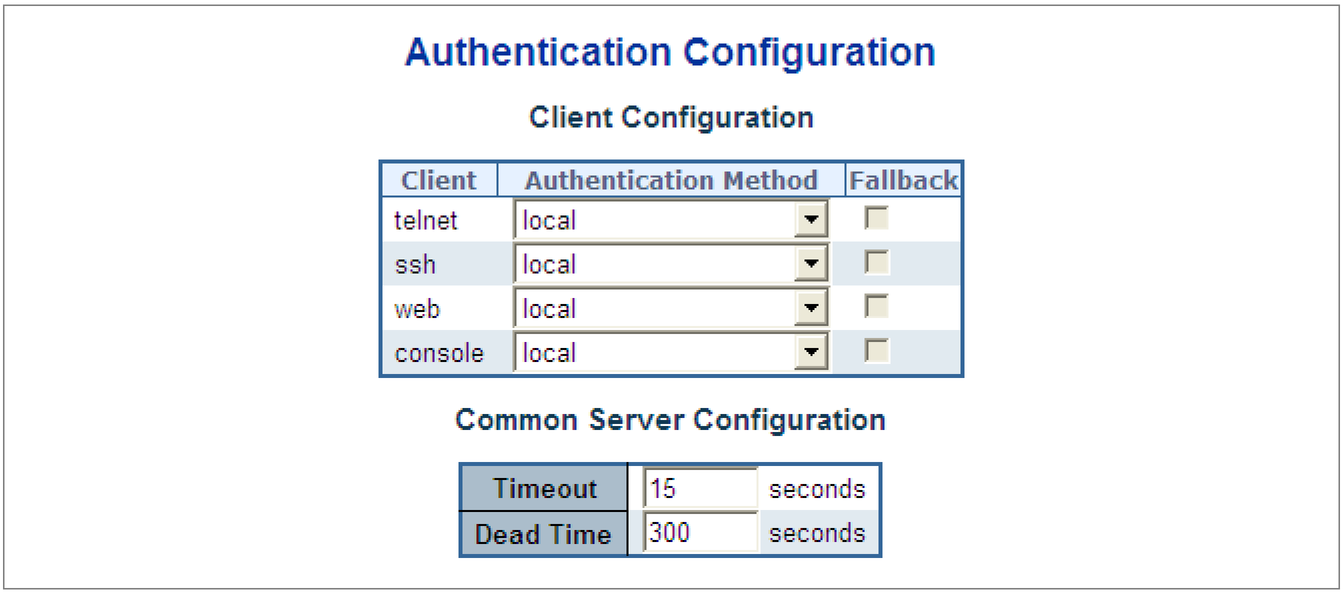
If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication 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.



Authentication Configuration

Client Configuration

Client	Authentication Method	Fallback
telnet	local	□
ssh	local	□
web	local	□
console	local	□

Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

Figure 4-11-3 Client Configuration page screenshot

The page includes the following fields:

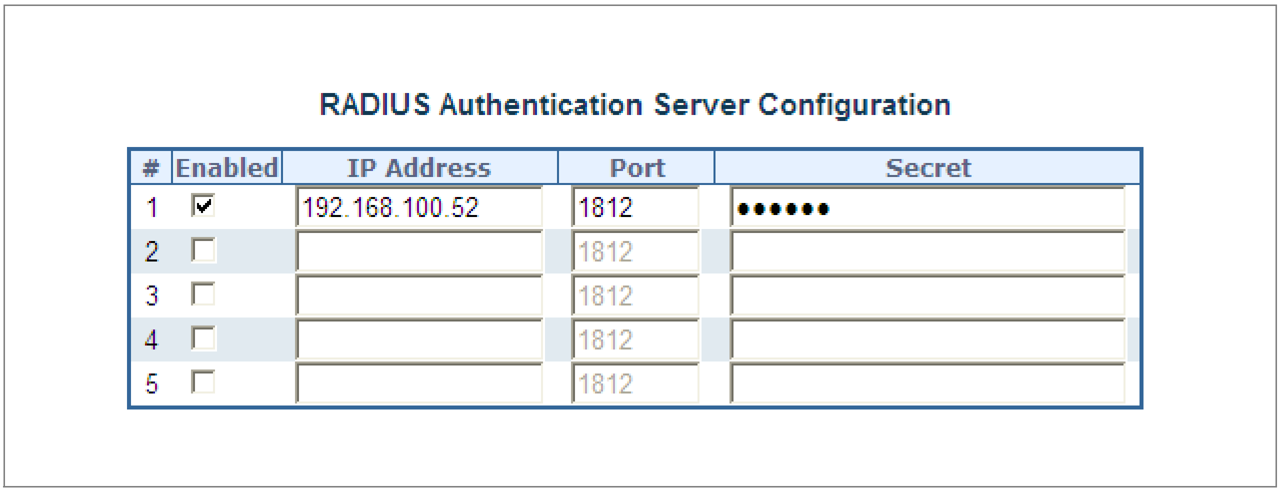
Client Configuration:

Object	Description
• **Client**	The 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'.

Common Server Configuration:

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

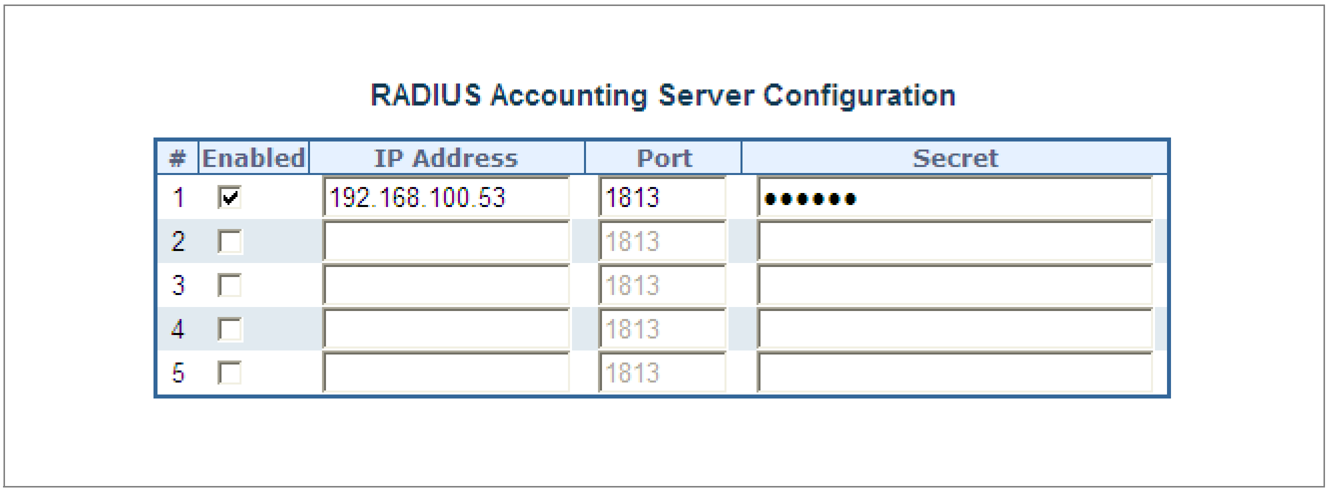
#	Enabled	IP Address	Port	Secret
1	☑	192.168.100.52	1812	••••••
2	□		1812	
3	□		1812	
4	□		1812	
5	□		1812	

Figure 4-11-4 RADIUS Authentication Server Configuration page screenshot

RADIUS Authentication Server Configuation:

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**	The IP address of the RADIUS Authentication Server 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 switchstack.



RADIUS Accounting Server Configuration

#	Enabled	IP Address	Port	Secret
1	☑	192.168.100.53	1813	••••••
2	□		1813	
3	□		1813	
4	□		1813	
5	□		1813	

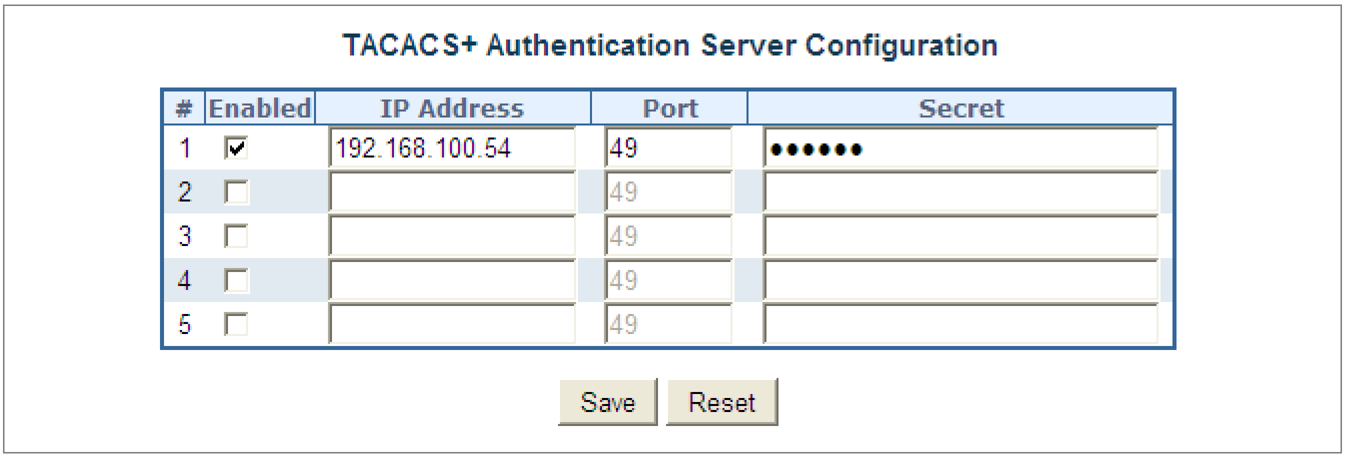
Figure 4-11-5 RADIUS Accounting Server Configuration page screenshot

The page includes the following fields:

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**	The IP address of the RADIUS Accounting Server 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 switchstack.

TACACS+ Authentication Server Configuration

TACACS+ is an acronym for **Terminal Acess Controller Access Control System Plus**. 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.



TACACS+ Authentication Server Configuration

#	Enabled	IP Address	Port	Secret
1	☑	192.168.100.54	49	••••••
2	□		49	
3	□		49	
4	□		49	
5	□		49	

Figure 4-11-6 TACACS+ Authentication Server Configuration page screenshot

The page includes the following fields:

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**	The IP address of the TACACS+ Authentication Server 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 switchstack.

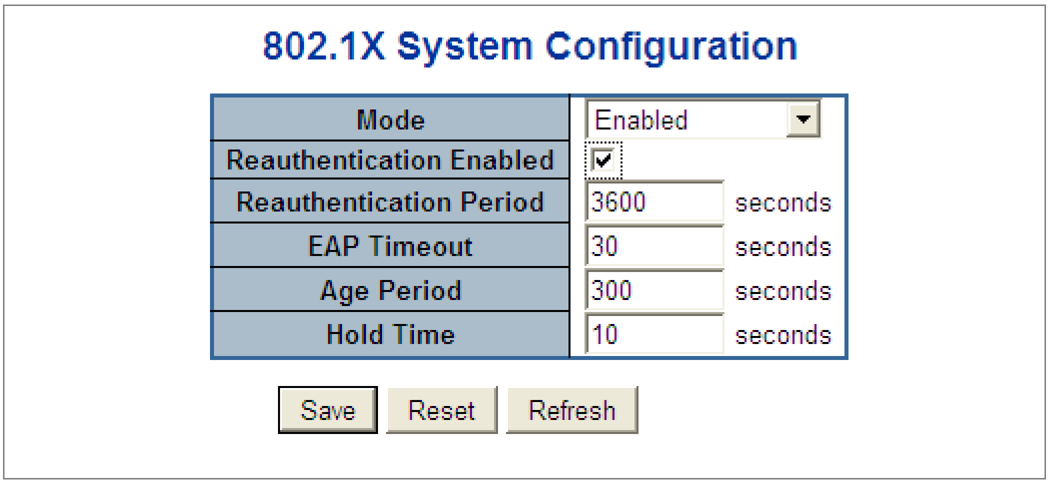
4.11.3 802.1X System Configuration

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

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

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

The 802.1X System Configuration screen in Figure 4-11-7 appears.



802.1X System Configuration

Mode	Enabled
Reauthentication Enabled	☑
Reauthentication Period	3600 seconds
EAP Timeout	30 seconds
Age Period	300 seconds
Hold Time	10 seconds

Figure 4-11-7 802.1X System Configuration page screenshot

The page includes the following fields:

Object	Description
- **Mode**	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switchstack. If globally disabled, all ports are allowed forwarding of frames.
- **Reauthentication Enabled**	If checked, clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age Period below).
- **Reauthentication**	Determines the period, in seconds, after which a connected client must be

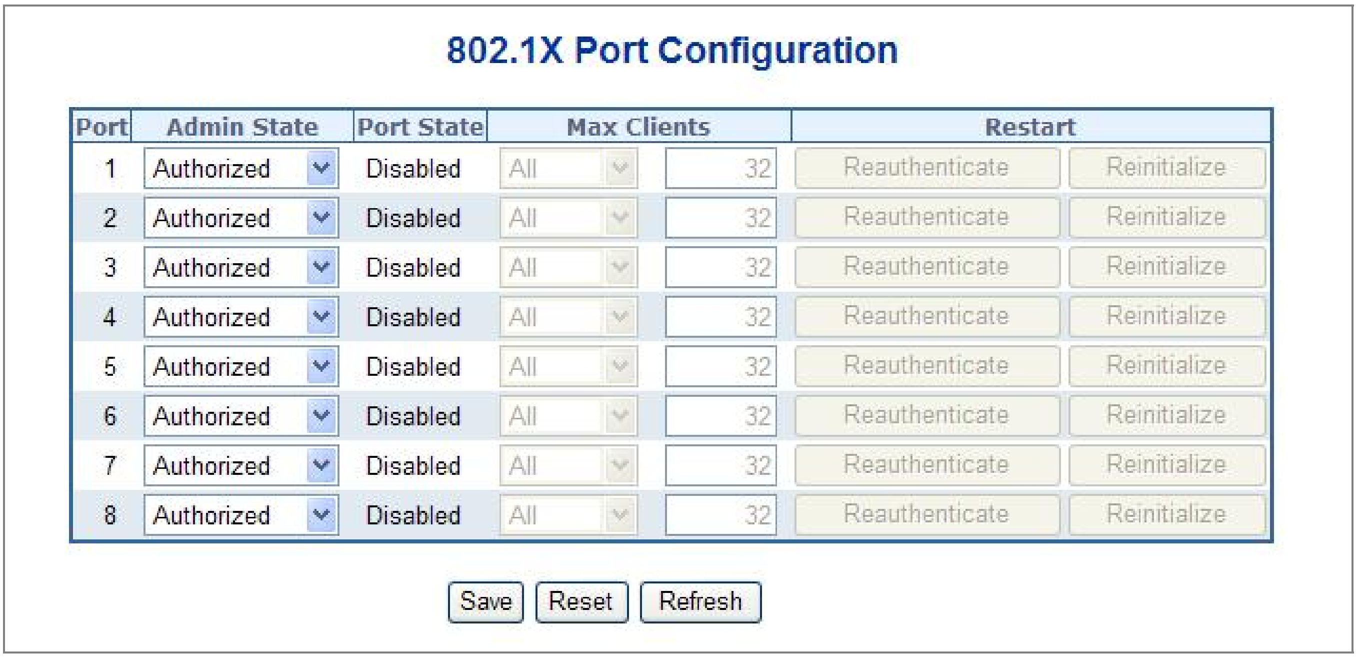
Period	reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
• **EAP Timeout**	Determines the time the switch shall wait for the supplicant response before retransmitting a packet. Valid values are in the range 1 to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

4.11.4 802.1X and MAC-Based Authentication Port Configuration

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

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

The 802.1X Port Configuration screen in Figure 4-11-8 appears.



802.1X Port Configuration

Port	Admin State	Port State	Max Clients		Restart	
1	Authorized	Disabled	All	32	Reauthenticate	Reinitialize
2	Authorized	Disabled	All	32	Reauthenticate	Reinitialize
3	Authorized	Disabled	All	32	Reauthenticate	Reinitialize
4	Authorized	Disabled	All	32	Reauthenticate	Reinitialize
5	Authorized	Disabled	All	32	Reauthenticate	Reinitialize
6	Authorized	Disabled	All	32	Reauthenticate	Reinitialize
7	Authorized	Disabled	All	32	Reauthenticate	Reinitialize
8	Authorized	Disabled	All	32	Reauthenticate	Reinitialize

Figure 4-11-8 802.1X Port Configuration page screenshot

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

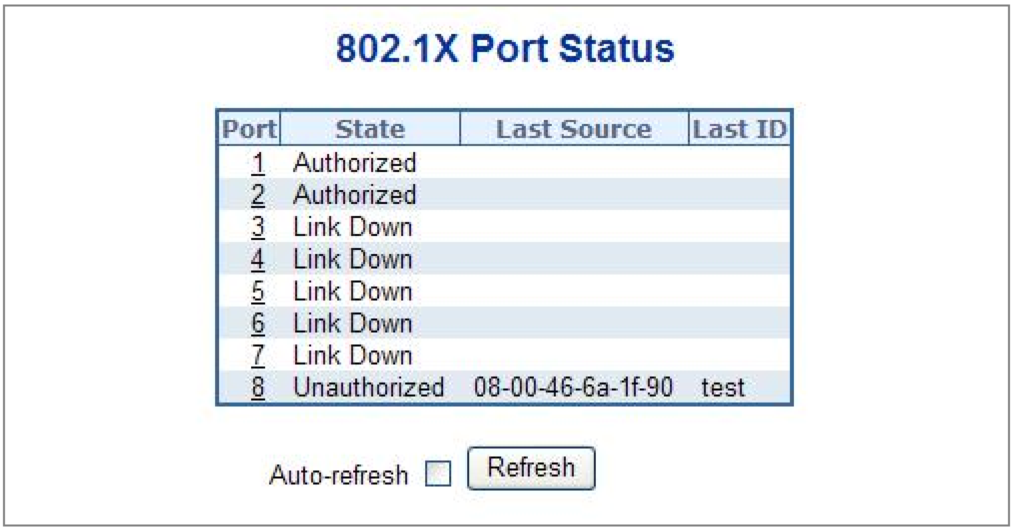
Object	Description
• **Port**	The port number for which the configuration below applies.
• **Admin State**	Sets the authentication mode to one of the following options (only used when 802.1X or MAC-based authentication is globally enabled): • **Auto:** Requires an 802.1X-aware client (supplicant) to be authorized by the authentication server. Clients that are not 802.1X-aware will be denied access. • **Authorized:** Forces the port to grant access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Success frame when the port links up. • **Unauthorized:** Forces the port to deny access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Failure frame when the port links up. • **MAC-Based:** Enables MAC-based authentication on the port. The switch

	doesn't transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic against an unsuccessfully authenticated client will be dropped. Clients that are not (yet) successfully authenticated will not be allowed to transmit frames of any kind.
• **Port State**	The current state of the port. It can undertake one of the following values: • **802.1X Disabled:** 802.1X and MAC-based authentication is globally disabled. • **Link Down:** 802.1X or MAC-based authentication is enabled, but there is no link on the port. • **Authorized:** The port is authorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto" and the supplicant is authenticated or the Admin State is "Authorized". • **Unauthorized:** The port is unauthorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto", but the supplicant is not (yet) authenticated or the Admin State is "Unauthorized". • **X Auth/Y Unauth:** X clients are currently authorized and Y are unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to "MAC-Based".
• **Max Clients**	**This setting applies to ports running MAC-based authentication, only**. The maximum number of clients allowed on a given port can be configured through the list-box and edit-control for this setting. Choosing the value "All" from the list-box allows the port to consume up to 104 client state-machines. Choosing the value "Specific" from the list-box opens up for entering a specific number of maximum clients on the port (1 to 104). The stackswitch is "born" with a pool of state-machines, from which all ports draw whenever a new client is seen on the port. When a given port's maximum is reached (both authorized and unauthorized clients count), further new clients are disallowed access. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available state-machines.

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

4.11.5 802.1X Port Status

This page provides an overview of the current IEEE 802.1X port states for the selected switch. The 802.1X Port Status screen in Figure 4-11-9 appears.



802.1X Port Status

Port	State	Last Source	Last ID
1	Authorized		
2	Authorized		
3	Link Down		
4	Link Down		
5	Link Down		
6	Link Down		
7	Link Down		
8	Unauthorized	08-00-46-6a-1f-90	test

Auto-refresh □ Refresh

Figure 4-11-9 802.1X Status page screenshot

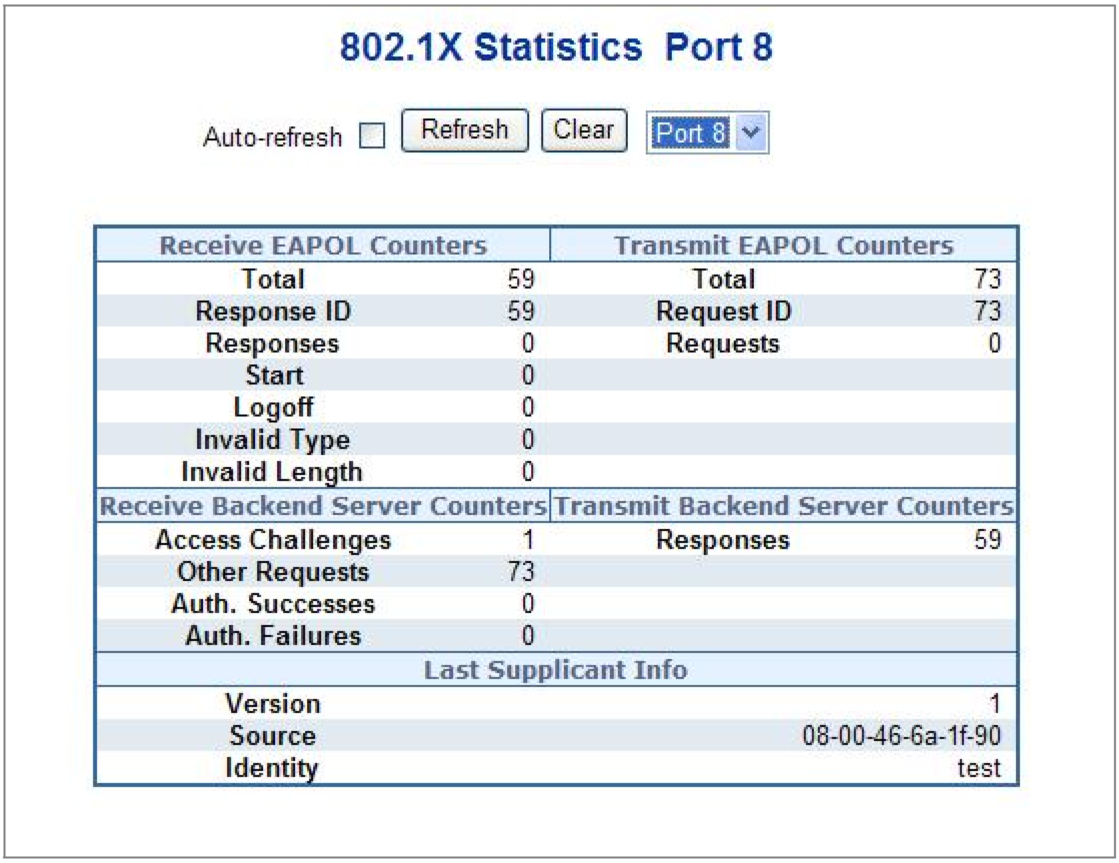
The page includes the following fields:

Object	Description
• **Port**	The switch port number. Click to navigate to detailed 802.1X statistics for this port.
• **State**	The current state of the port. Refer to IEEE 802.1X Port State for a description of the individual states.

- **Last Source**	The source MAC address carried in the most recently received EAPOL frame for port-based authentication, and the most recently received frame from a new client for MAC-based authentication.
- **Last ID**	The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame for port-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

4.11.6 802.1X Statistics

This page provides detailed IEEE 802.1X statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows selected RADIUS statistics, only. Use the port select box to select which port details to be displayed. The 802.1X and MAC-Based Authentication Statistics screen in Figure 4-11-10 appears.



802.1X Statistics Port 8

Auto-refresh □ Refresh Clear Port 8

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	59	Total	73
Response ID	59	Request ID	73
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		**Transmit Backend Server Counters**	
Access Challenges	1	Responses	59
Other Requests	73		
Auth. Successes	0		
Auth. Failures	0		
Last Supplicant Info			
Version			1
Source			08-00-46-6a-1f-90
Identity			test

Figure 4-11-10 802.1X Statistics Port 1 page screenshot

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

- **EAPOL Counters**

These counters are not available for MAC-based ports.

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

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

- **RADIUS Counters**

RADIUS Server frame counter statistics.

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

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

RADIUS Counters			
Direction	**Name**	**IEEE Name**	**Description**
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	**Port-based**: Counts the number of times that the switch receives the first request from the RADIUS server following the first response

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

- ### Last Supplicant/Client Info

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

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

Last Supplicant/Client Info

Name	IEEE Name	Description
Version	dot1xAuthLastEapolFrameVersion	**Port-based**: The protocol version number carried in the most recently received EAPOL frame.

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

Clients attached to this port

This table is only available for MAC-based ports

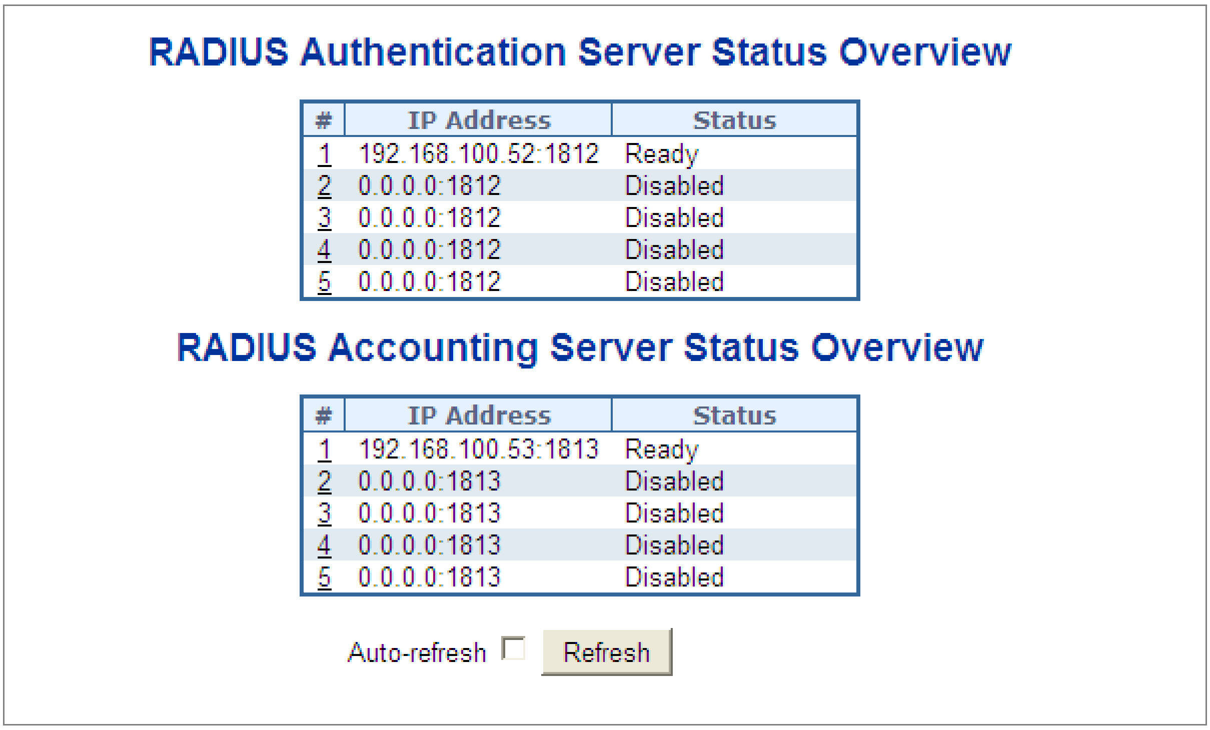
Each row in the table represents a MAC-based client on the port, and there are three parameters for each client:

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

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

4.11.7 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.



RADIUS Authentication Server Status Overview

#	IP Address	Status
1	192.168.100.52:1812	Ready
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	192.168.100.53:1813	Ready
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Figure 4-11-11 RADIUS Authentication Servers Status Overview page screenshot

RADIUS Authentication Servers

The page includes the following fields:

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.

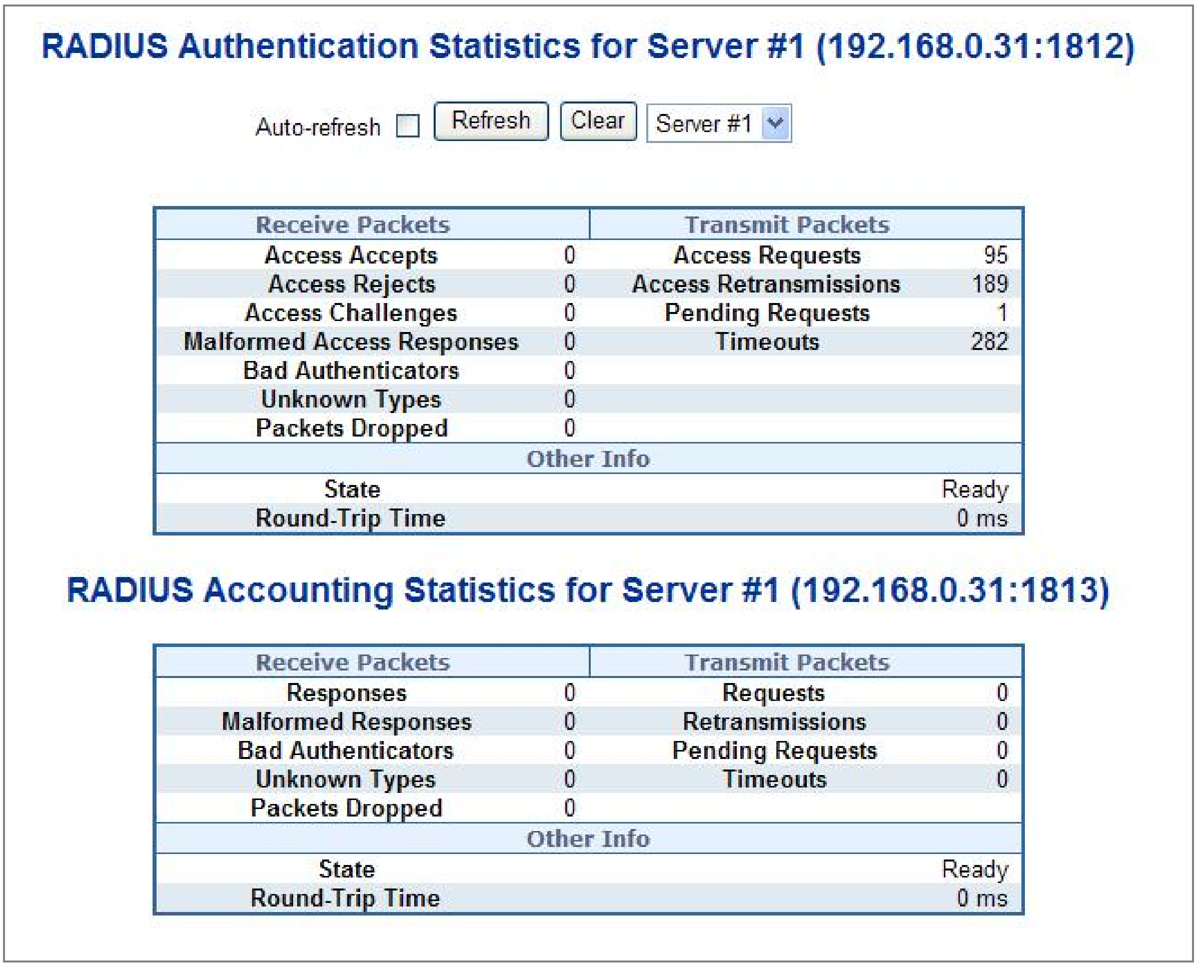
RADIUS Accounting Servers

The page includes the following fields:

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.

4.11.8 RADIUS Detail

This page provides detailed statistics for a particular RADIUS server. The RADIUS Authentication Statistics screen in Figure 4-11-12 appears.



RADIUS Authentication Statistics for Server #1 (192.168.0.31:1812)

Auto-refresh □ Refresh Clear Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	95
Access Rejects	0	Access Retransmissions	189
Access Challenges	0	Pending Requests	1
Malformed Access Responses	0	Timeouts	282
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
State			Ready
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1 (192.168.0.31:1813)

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
State			Ready
Round-Trip Time			0 ms

Figure 4-11-12 RADIUS Authentication Servers Status Overview page screenshot

RADIUS Authentication Statistics

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.

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**	radiusAuthClientExtAccessRejects	The number of RADIUS 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 Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent 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 Statistics

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.

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

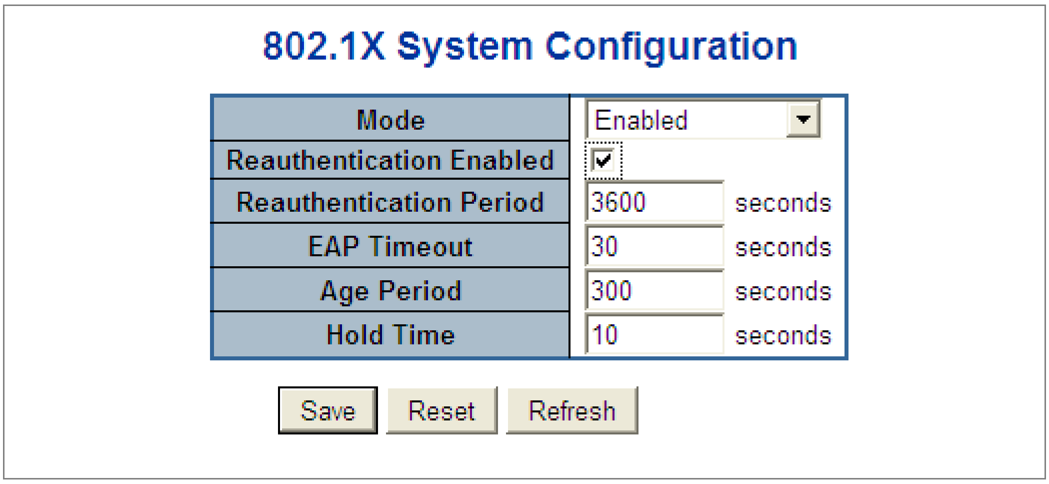
This section contains information about the state of the server and the latest round-trip time.

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.

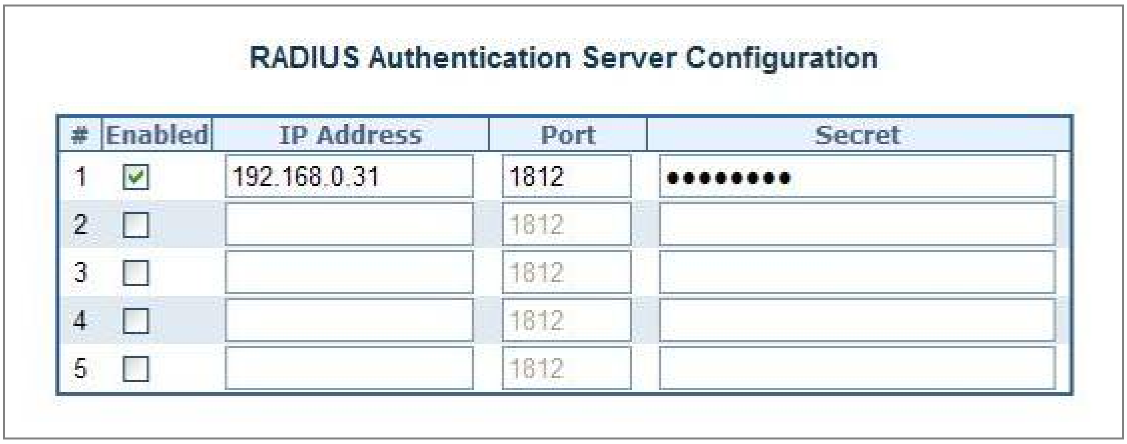
1. Enable the 802.1x Authentication Mode and configure the IP Address of remote RADIUS server and secret key.



802.1X System Configuration

Mode	Enabled
Reauthentication Enabled	☑
Reauthentication Period	3600 seconds
EAP Timeout	30 seconds
Age Period	300 seconds
Hold Time	10 seconds

Figure 4-11-13 802.1x System Configuration page screenshot



RADIUS Authentication Server Configuration

#	Enabled	IP Address	Port	Secret
1	☑	192.168.0.31	1812	●●●●●●●●
2	☐		1812	
3	☐		1812	
4	☐		1812	
5	☐		1812	

Figure 4-11-14 RADIUS Authentication Server Configuration page screenshot

2. Add New RADIUS Cleint on the Windows 2003 server

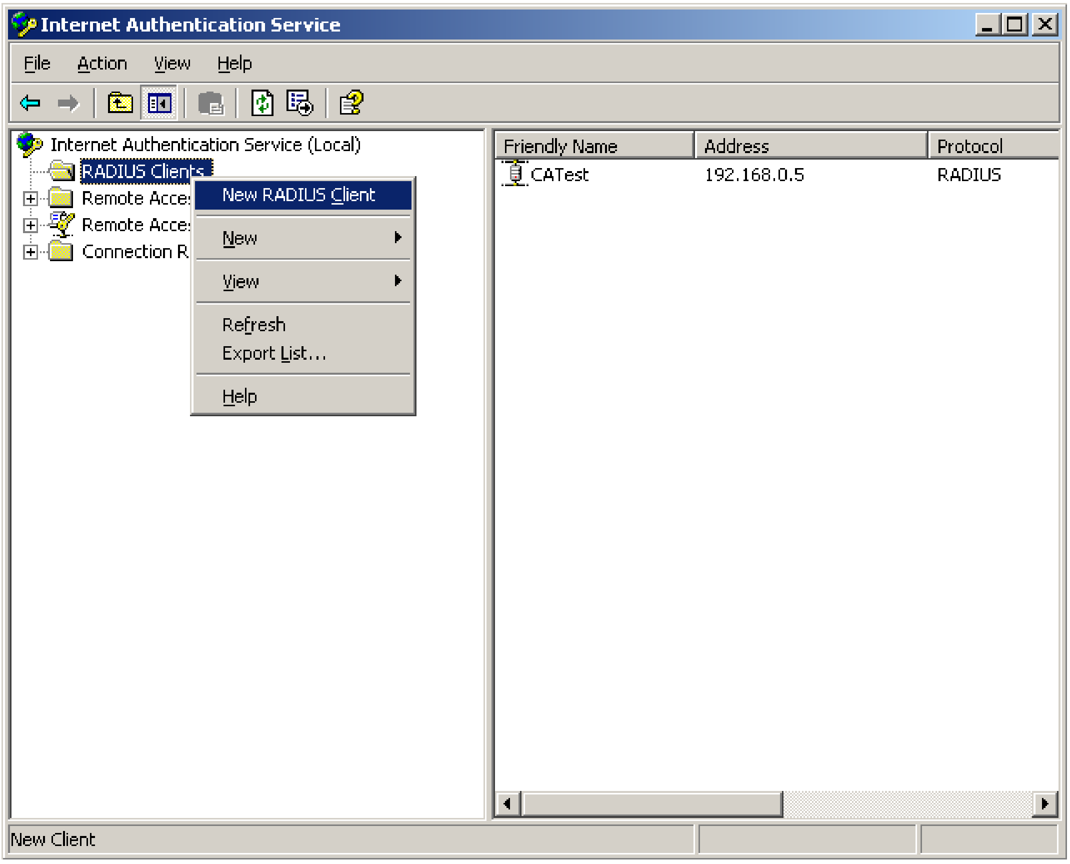
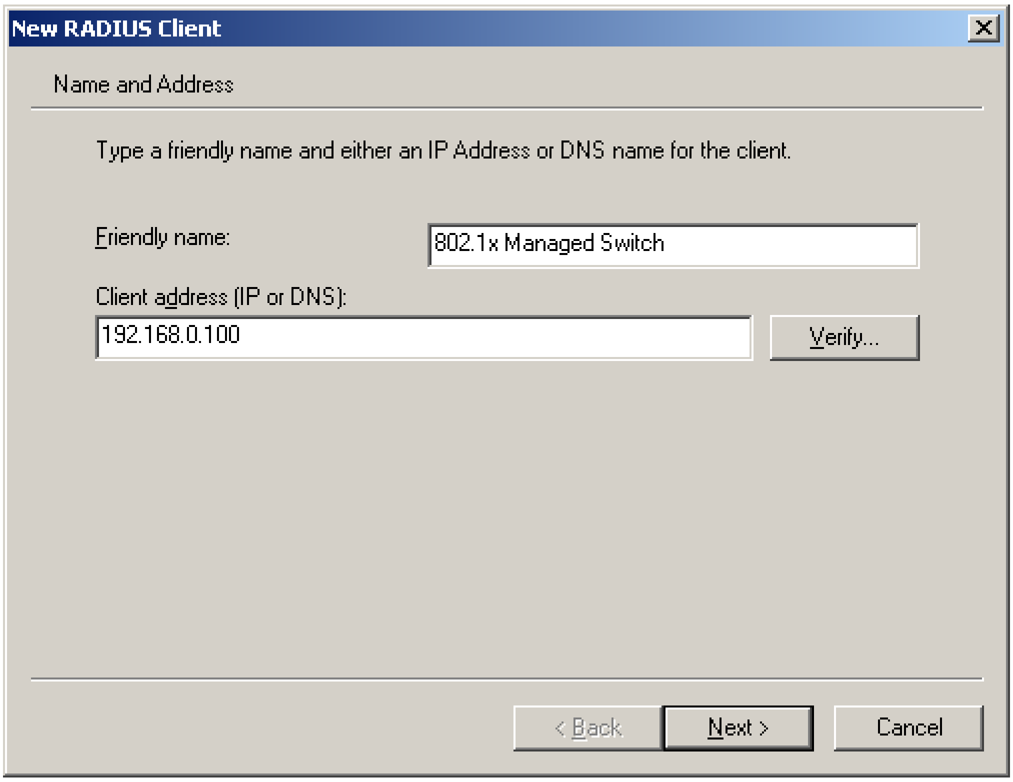


Figure 4-11-15 Windows Server – add new RADIUS client setting

3. Assign the client IP address to the Managed switch



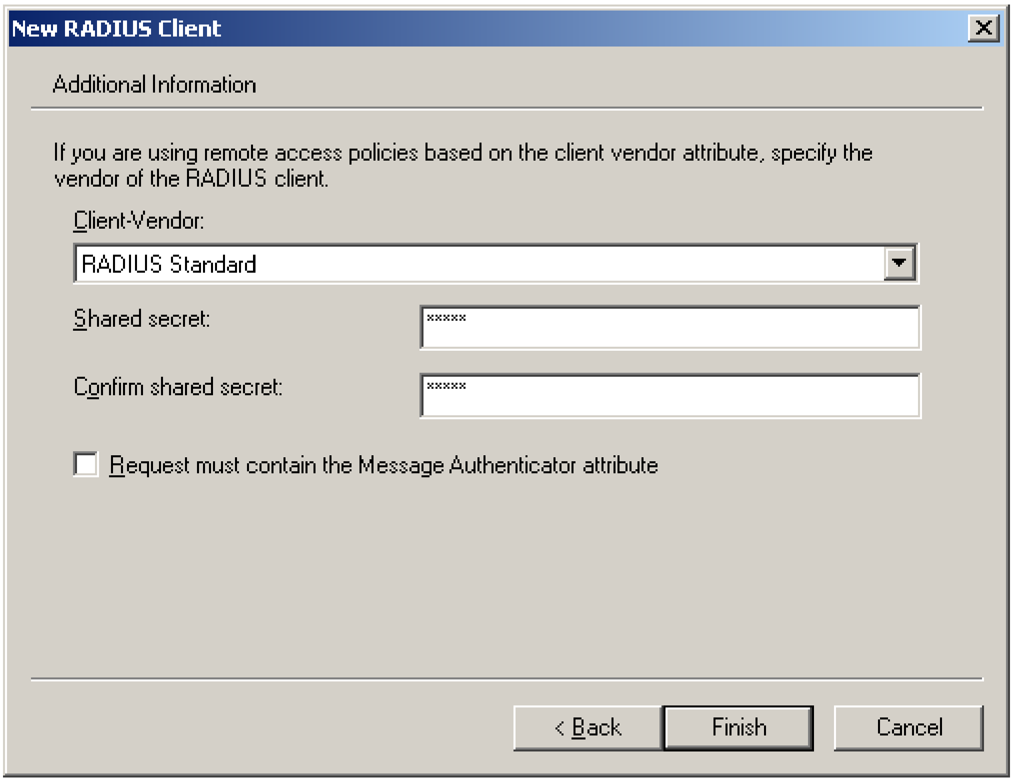
Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: 802.1x Managed Switch

Client address (IP or DNS): 192.168.0.100

Figure 4-11-16 Windows Server RADIUS Server setting

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



New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

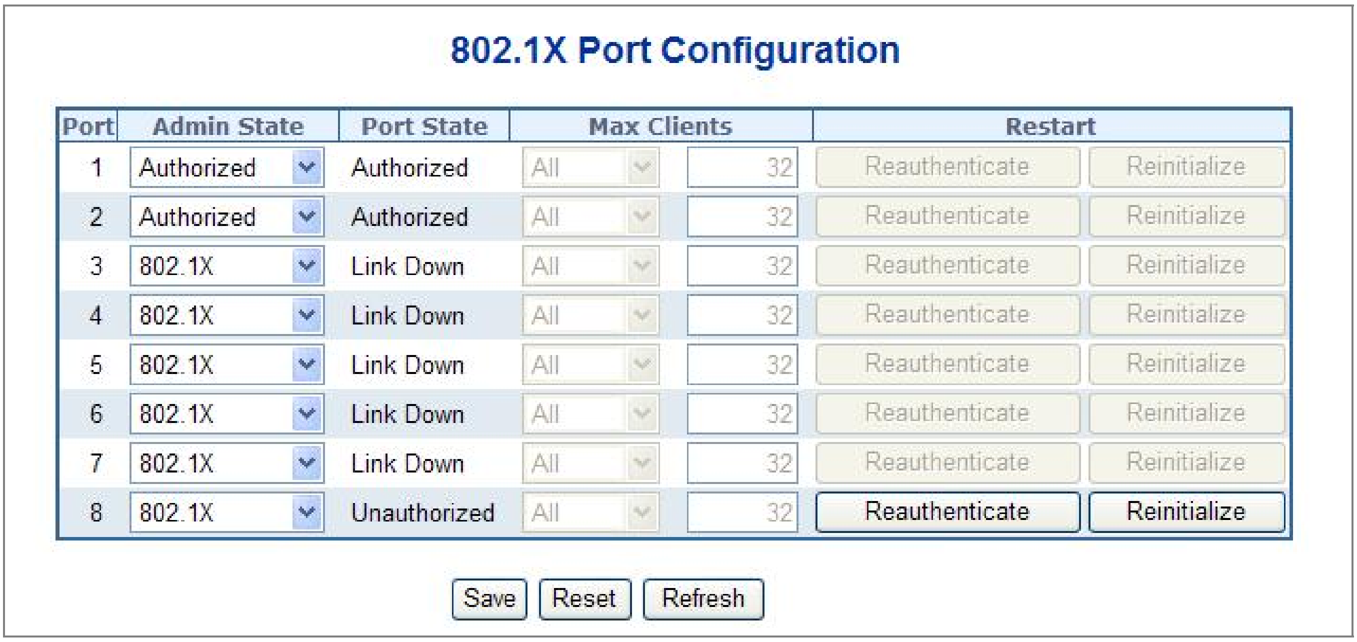
Shared secret: *****

Confirm shared secret: *****

□ Request must contain the Message Authenticator attribute

Figure 4-11-17 Windows Server RADIUS Server setting

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



802.1X Port Configuration

Port	Admin State	Port State	Max Clients		Restart	
1	Authorized	Authorized	All	32	Reauthenticate	Reinitialize
2	Authorized	Authorized	All	32	Reauthenticate	Reinitialize
3	802.1X	Link Down	All	32	Reauthenticate	Reinitialize
4	802.1X	Link Down	All	32	Reauthenticate	Reinitialize
5	802.1X	Link Down	All	32	Reauthenticate	Reinitialize
6	802.1X	Link Down	All	32	Reauthenticate	Reinitialize
7	802.1X	Link Down	All	32	Reauthenticate	Reinitialize
8	802.1X	Unauthorized	All	32	Reauthenticate	Reinitialize

Figure 4-11-18 802.1x Port Configuration page screenshot

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:

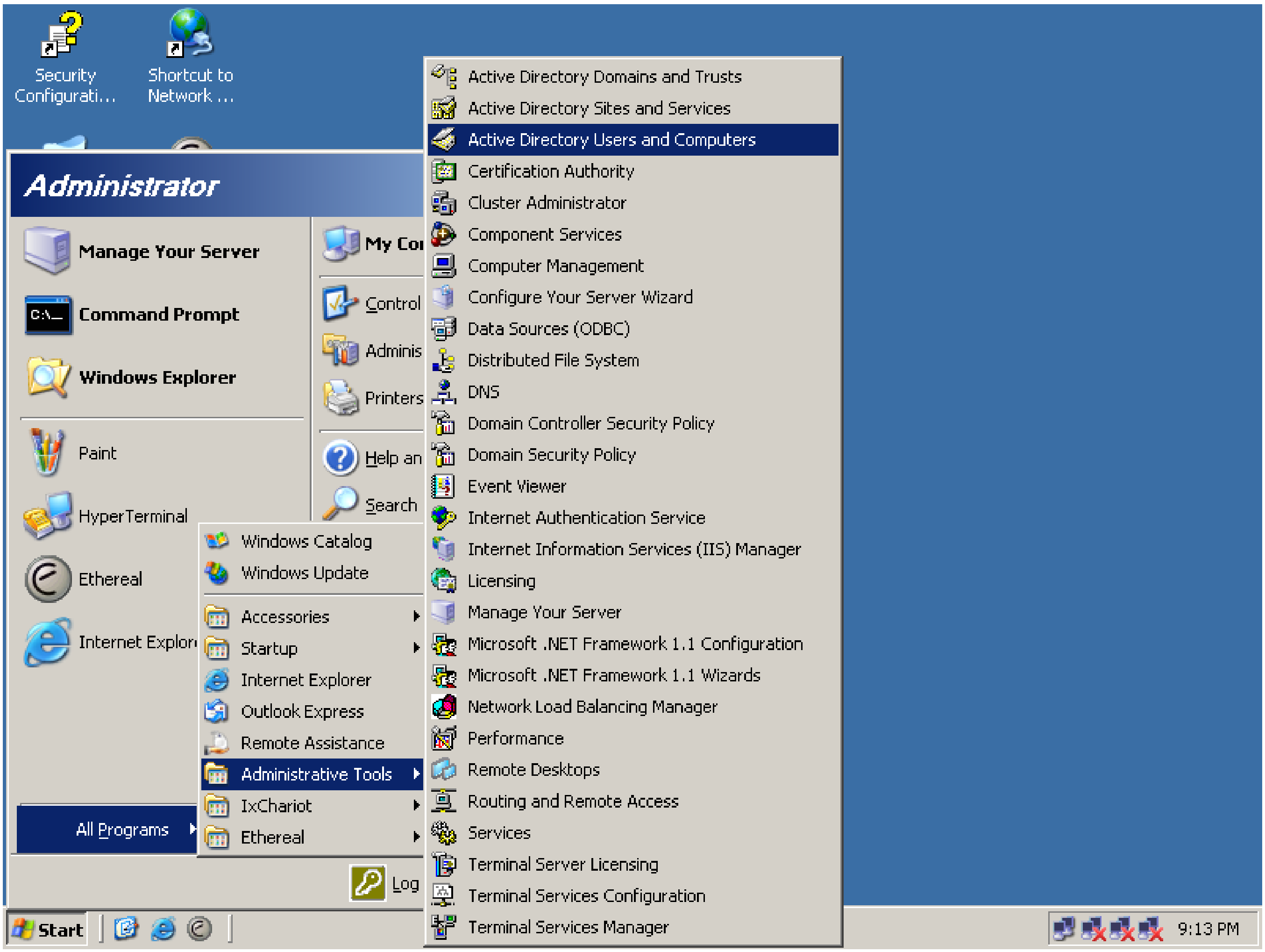
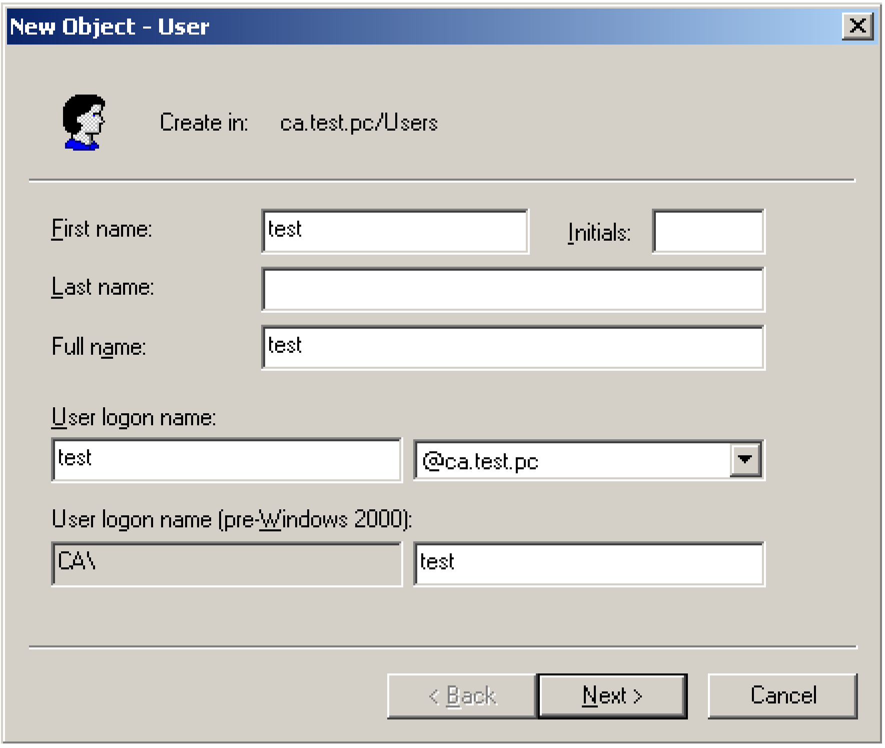


Figure 4-11-19 Windows 2003 AD server setting path

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:



New Object - User

Create in: ca.test.pc/Users

First name: test

Initials:

Last name:

Full name: test

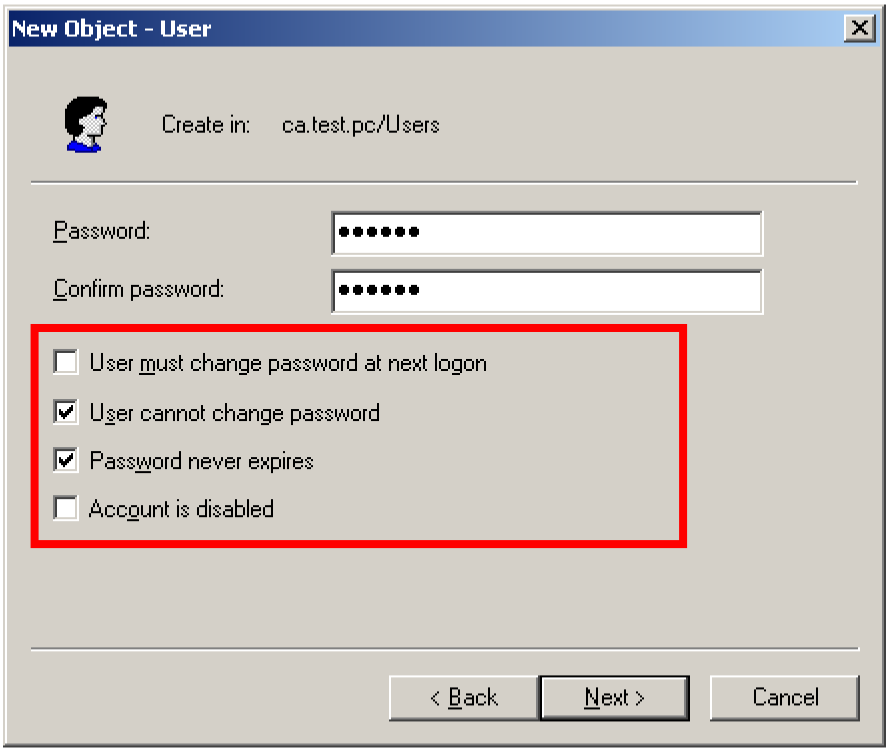
User logon name:

test @ca.test.pc

User logon name (pre-Windows 2000):

CA\ test

Figure 4-11-20 Add User Properties screen



New Object - User

Create in: ca.test.pc/Users

Password: ●●●●●●

Confirm password: ●●●●●●

☐ User must change password at next logon

☑ User cannot change password

☑ Password never expires

☐ Account is disabled

Figure 4-11-21 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.

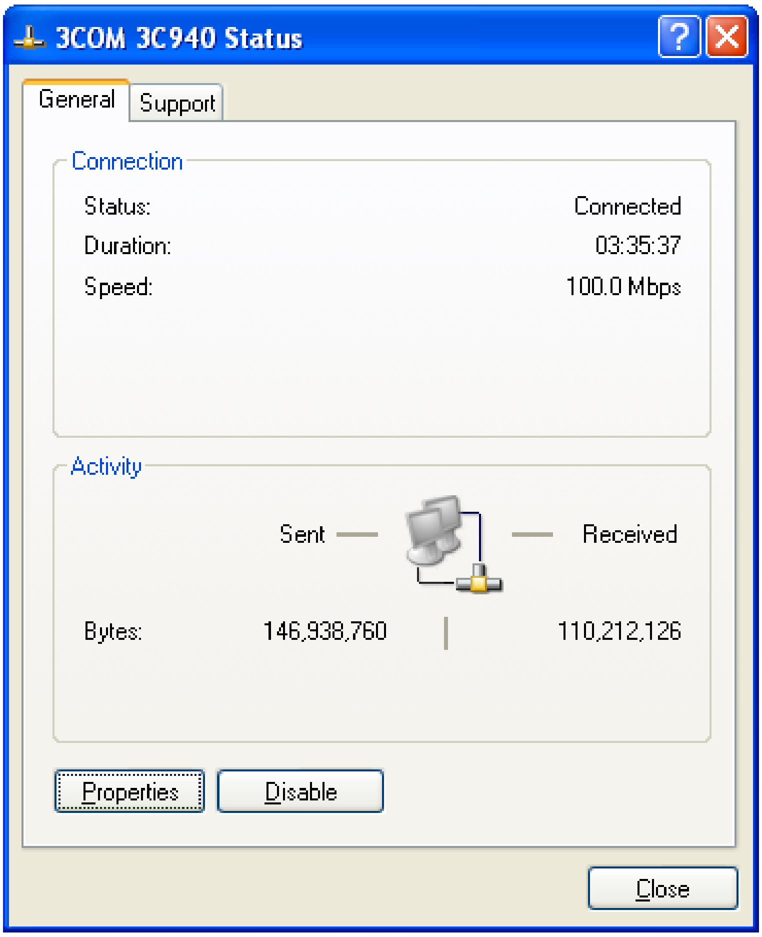
4.11.10 802.1X Client Configuration

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.



3COM 3C940 Status

Connection

Status: Connected

Duration: 03:35:37

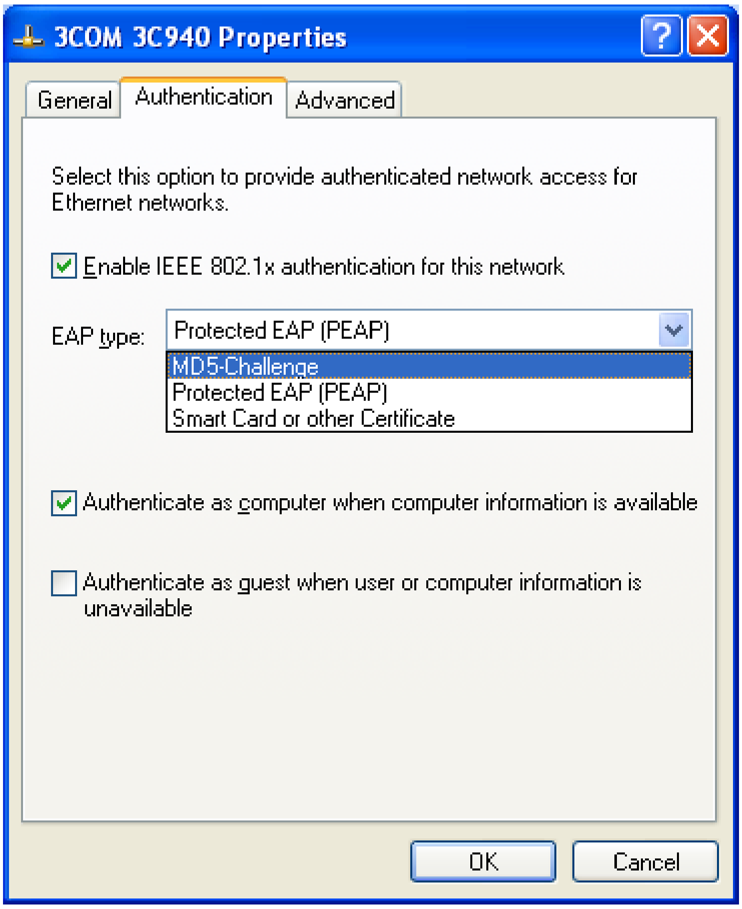
Speed: 100.0 Mbps

Activity

Bytes: Sent 146,938,760 Received 110,212,126

Figure 4-11-22

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.



3COM 3C940 Properties

Select this option to provide authenticated network access for Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

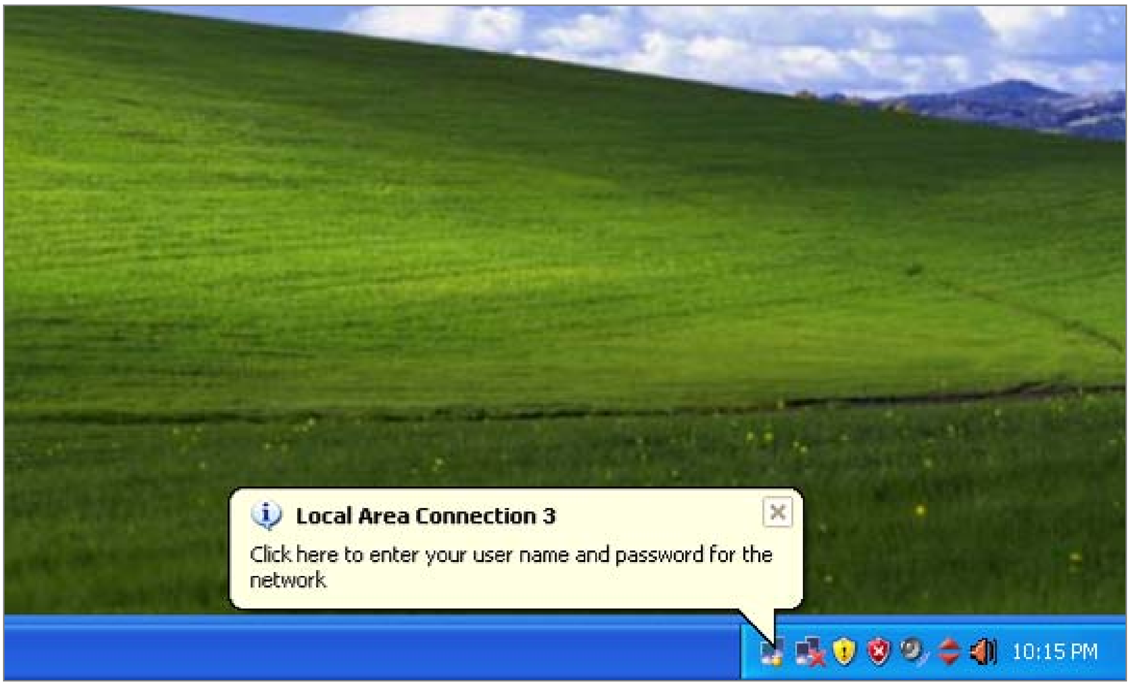
MD5-Challenge
Protected EAP (PEAP)
Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

Figure 4-11-23

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.

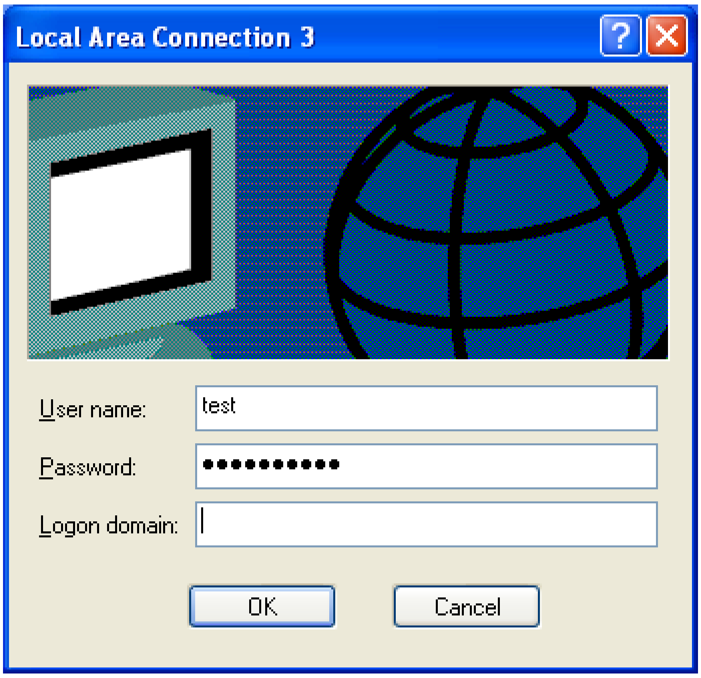


Local Area Connection 3

Click here to enter your user name and password for the network

Figure 4-11-24 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.



User name: test

Password: ●●●●●●●●●●●

Logon domain:

Figure 4-11-25

4.12 Security

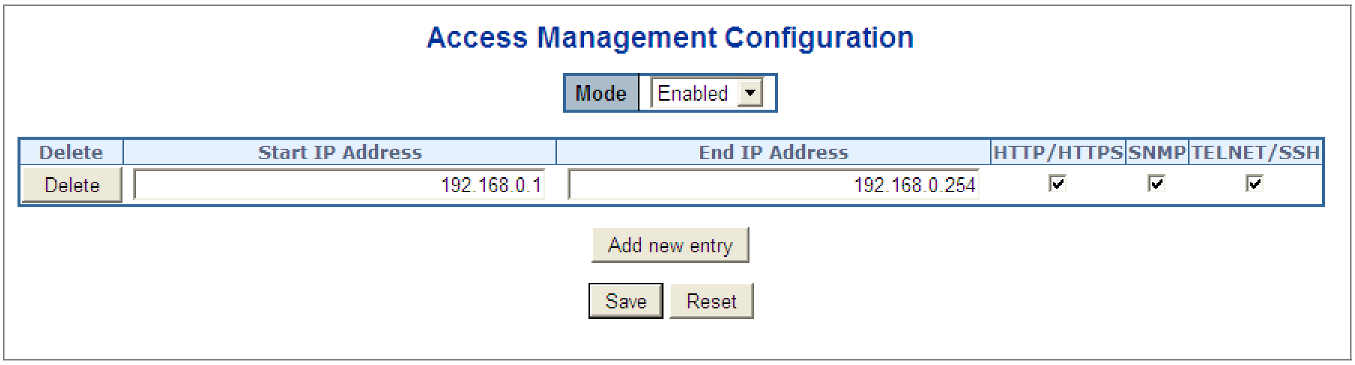
This section is to control the access of the Managed Switch, includes the user access and management control.

The Security page contains links to the following main topics:

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

4.12.1 Access Management

Configure access management table on this page. The maximum entry number is **16**.



Access Management Configuration

Mode: Enabled

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	192.168.0.1	192.168.0.254	☑	☑	☑

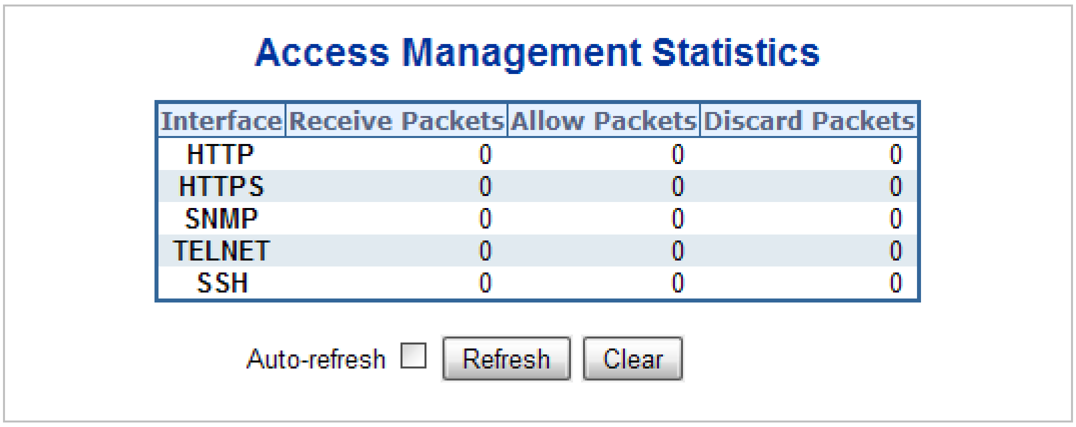
Figure 4-12-1 Access Management Configuration page screenshot

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.

4.12.2 Access Managemenet Statistics

This page provides statistics for access management.



Access Management Statistics

Interface	Receive Packets	Allow Packets	Discard Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Figure 4-12-2 Access Management Statistics page screenshot

The page includes the following fields:

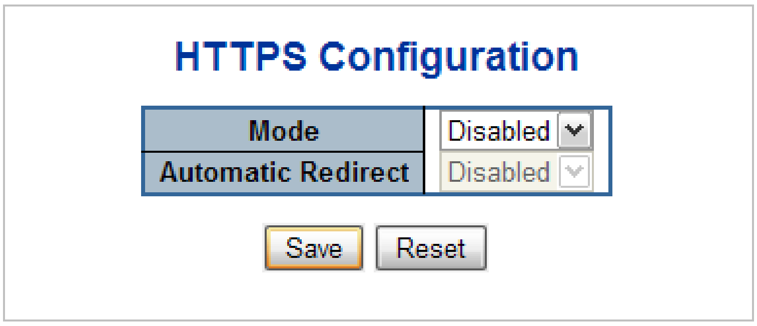
Object	Description
• **Interface**	The interface that allowed remote host can access the switch.
• **Receive Packets**	The received packets number from the interface under access management mode is enabled.
• **Allow Packets**	The allowed packets number from the interface under access management mode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

4.12.3 HTTPs

Configure HTTPS on this page.

HTTPS is an acronym for **Hypertext Transfer Protocol over Secure** 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.



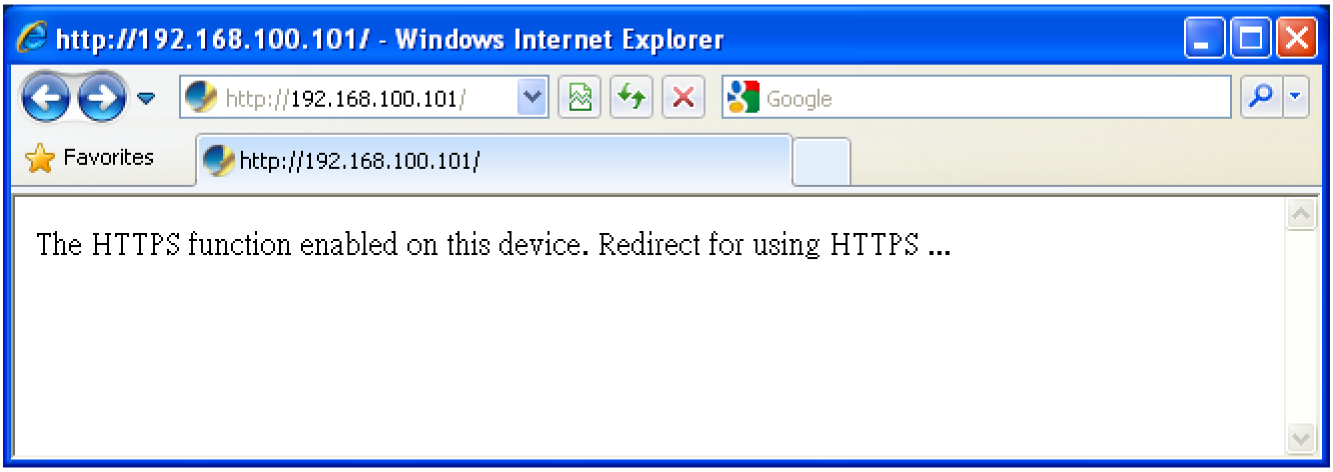
HTTPS Configuration

Mode	Disabled
Automatic Redirect	Disabled

Figure 4-12-3 HTTPs Configuration page screenshot

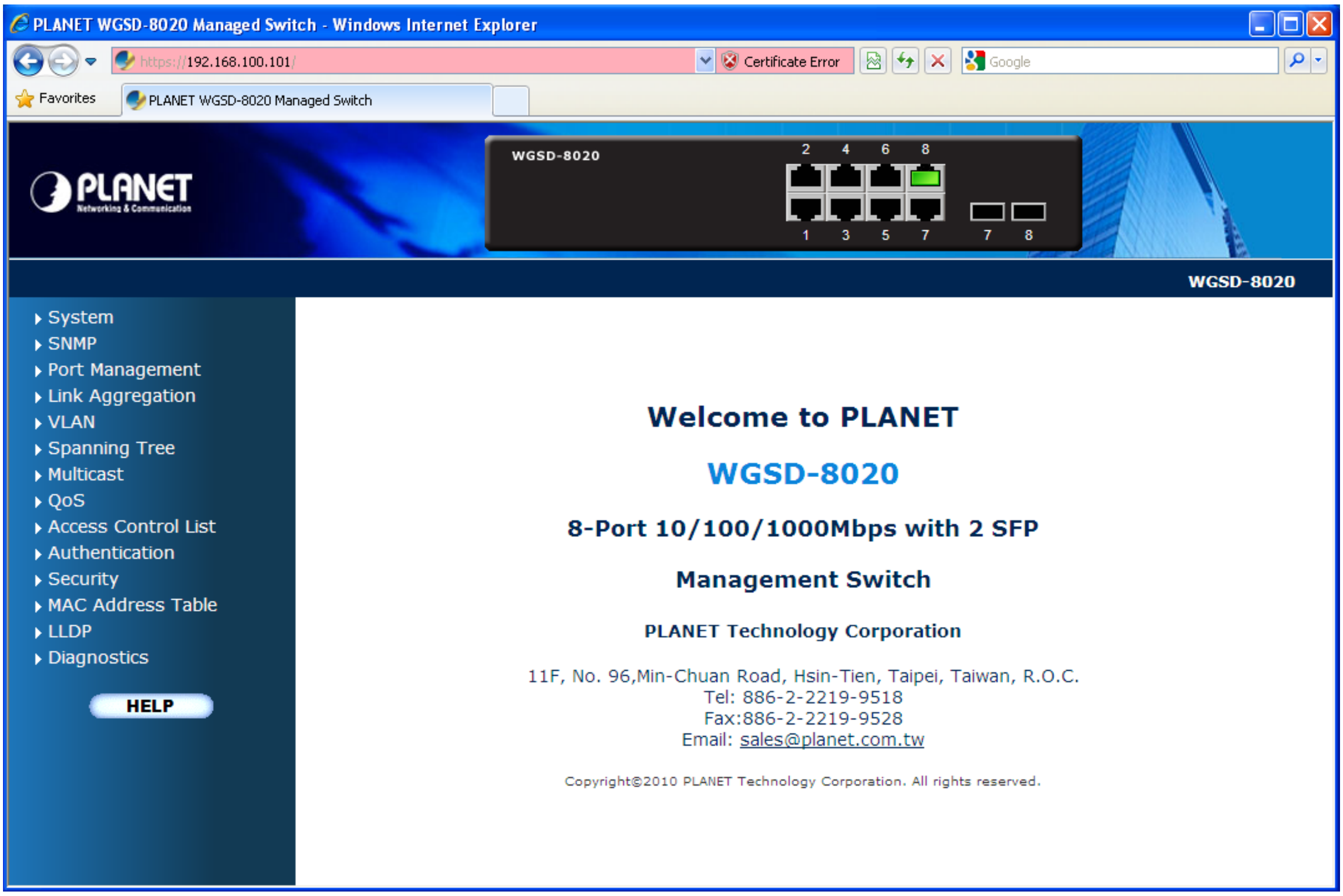
The page includes the following fields:

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.



The HTTPS function enabled on this device. Redirect for using HTTPS ...

Figure 4-12-4 HTTPs Redirect page screenshot



Welcome to PLANET

WGSD-8020

8-Port 10/100/1000Mbps with 2 SFP

Management Switch

PLANET Technology Corporation

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

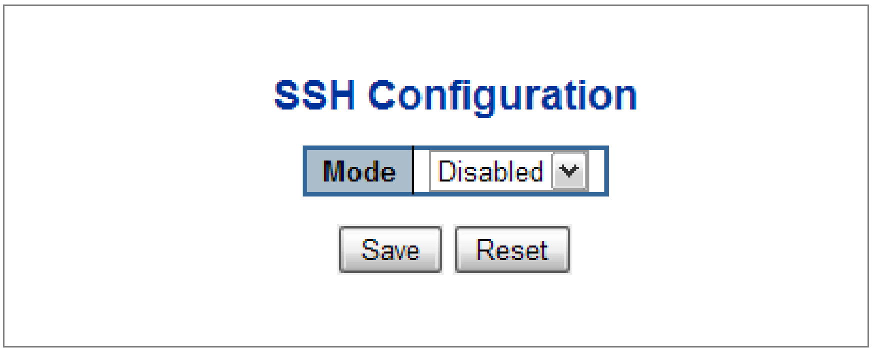
Copyright©2010 PLANET Technology Corporation. All rights reserved.

Figure 4-12-5 HTTPs login page screenshot

4.12.4 SSH

Configure SSH on this page.

SSH is an acronym for **Secure SHell**. 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).


SSH Configuration

Mode	Disabled

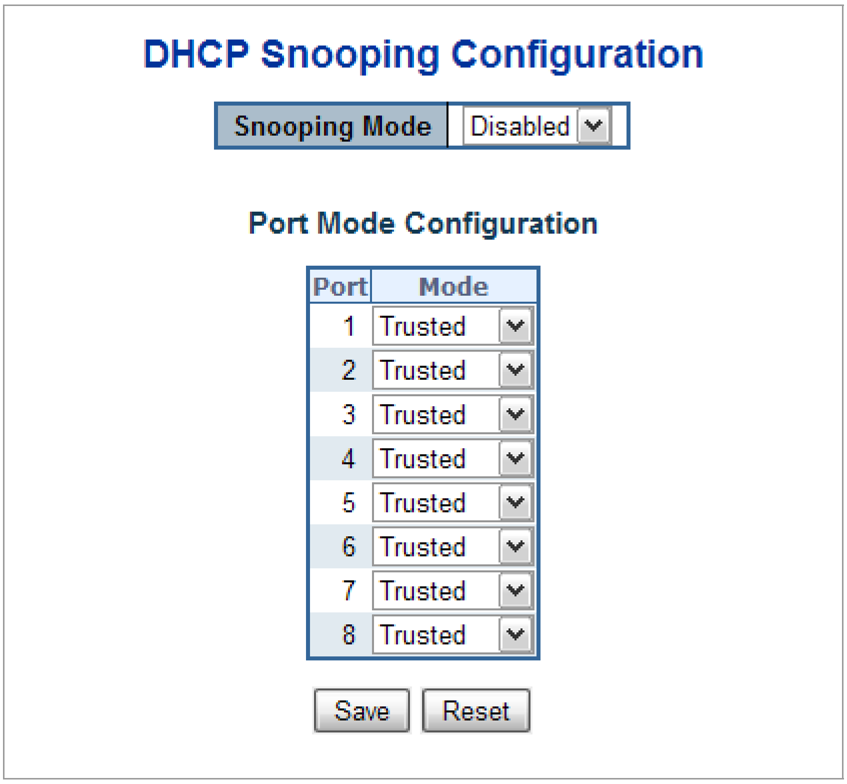
Figure 4-12-6 SSH Configuration page screenshot

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.

4.12.5 DHCP Snooping

Configure DHCP Snooping on this page. 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.



DHCP Snooping Configuration

Snooping Mode: Disabled

Port Mode Configuration

Port	Mode
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted

Figure 4-12-7 DHCP Snooping Configuration page screenshot

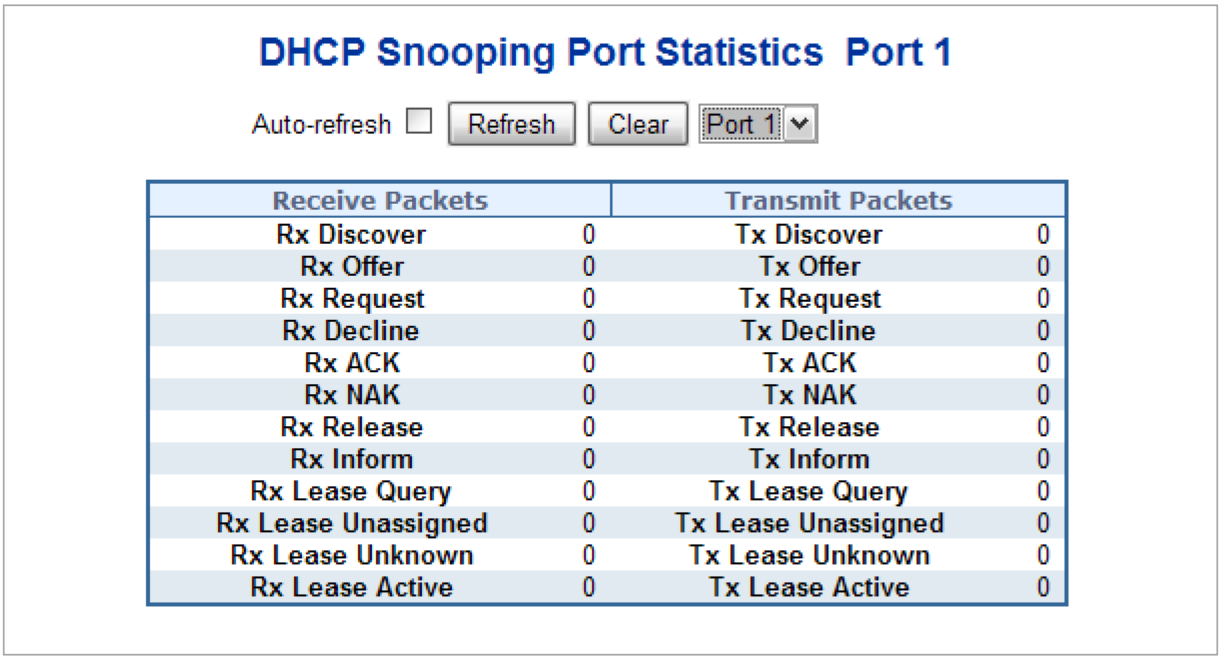
The page includes the following fields:

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.

4.12.6 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.



DHCP Snooping Port Statistics Port 1

Auto-refresh □ Refresh Clear Port 1

Receive Packets		Transmit Packets	
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

Figure 4-12-8 DHCP Snooping Port Statistics page screenshot

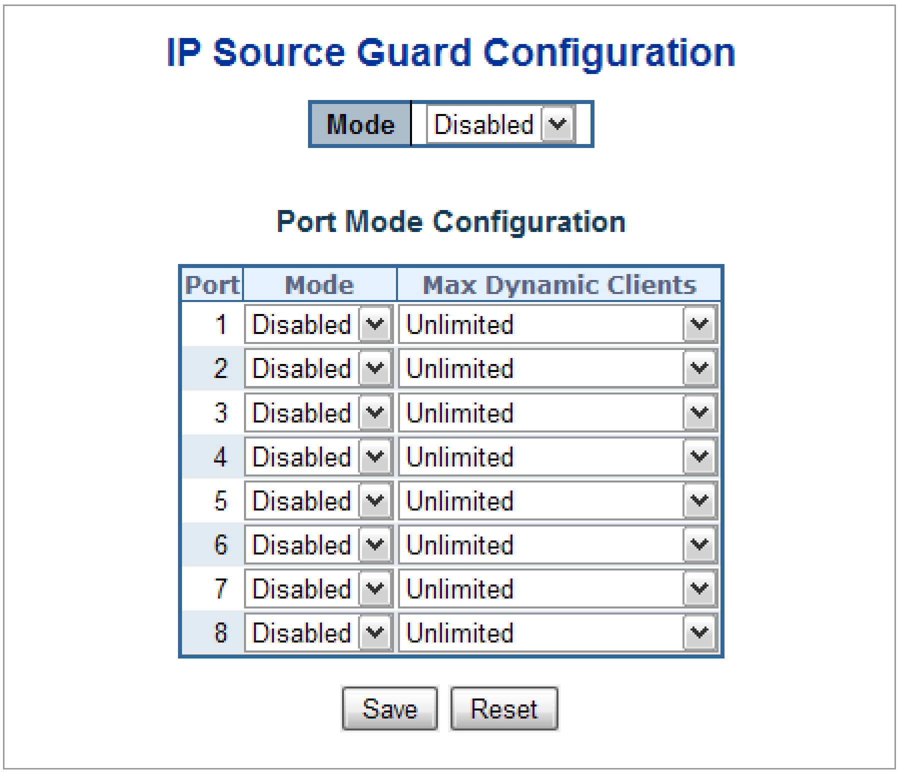
The page includes the following fields:

Object	Description
• **Rx and Tx Discover**	TThe number of discover (option 53 with value 1) packets received and transmitted.
• **Rx and Tx Offer**	TThe number of offer (option 53 with value 2) packets received and transmitted.
• **Rx and Tx Request**	TThe number of request (option 53 with value 3) packets received and transmitted.
• **Rx and Tx Decline**	TThe number of decline (option 53 with value 4) packets received and transmitted.
• **Rx and Tx ACK**	TThe number of ACK (option 53 with value 5) packets received and transmitted.
• **Rx and Tx NAK**	TThe number of NAK (option 53 with value 6) packets received and transmitted.
• **Rx and Tx Release**	TThe number of release (option 53 with value 7) packets received and transmitted.
• **Rx and Tx Inform**	TThe number of inform (option 53 with value 8) packets received and

	transmitted.
• **Rx and Tx Lease Query**	TThe number of lease query (option 53 with value 10) packets received and transmitted.
• **Rx and Tx Lease Unassigned**	TThe number of lease unassigned (option 53 with value 11) packets received and transmitted.
• **Rx and Tx Lease Unknown**	TThe number of lease unknown (option 53 with value 12) packets received and transmitted.
• **Rx and Tx Lease Active**	TThe number of lease active (option 53 with value 13) packets received and transmitted.

4.12.7 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.



IP Source Guard Configuration

Mode: Disabled

Port Mode Configuration

Port	Mode	Max Dynamic Clients
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited

Figure 4-12-9 IP Source Guard Configuration page screenshot

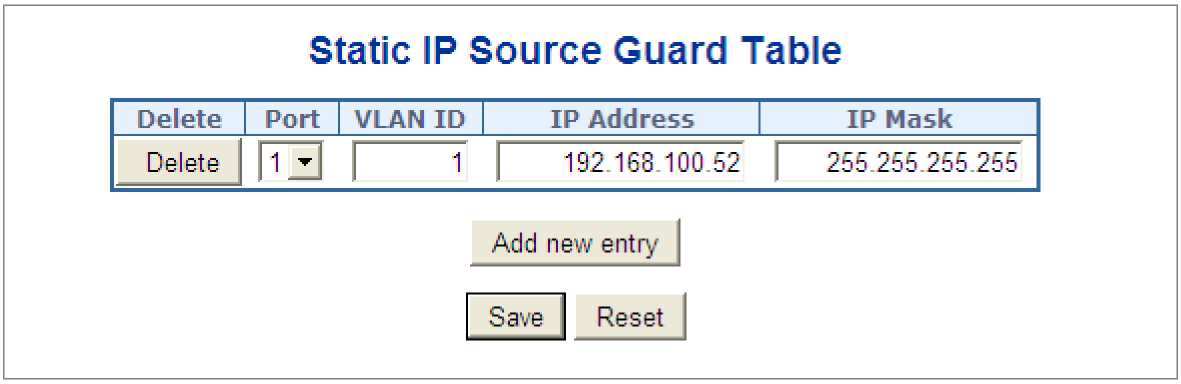
The page includes the following fields:

Object	Description
• **Mode of IP Source Guard Configuration**	Enable the Global IP Source Guard or disable the Global IP Source Guard.

• **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, 3, and unlimited.

4.12.8 IP Source Guard Static Table

Configure IP Spurce Guard Static Table on this page.



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	IP Mask
Delete	1	1	192.168.100.52	255.255.255.255

Figure 4-12-10 IP Source Guard Static Table page screenshot

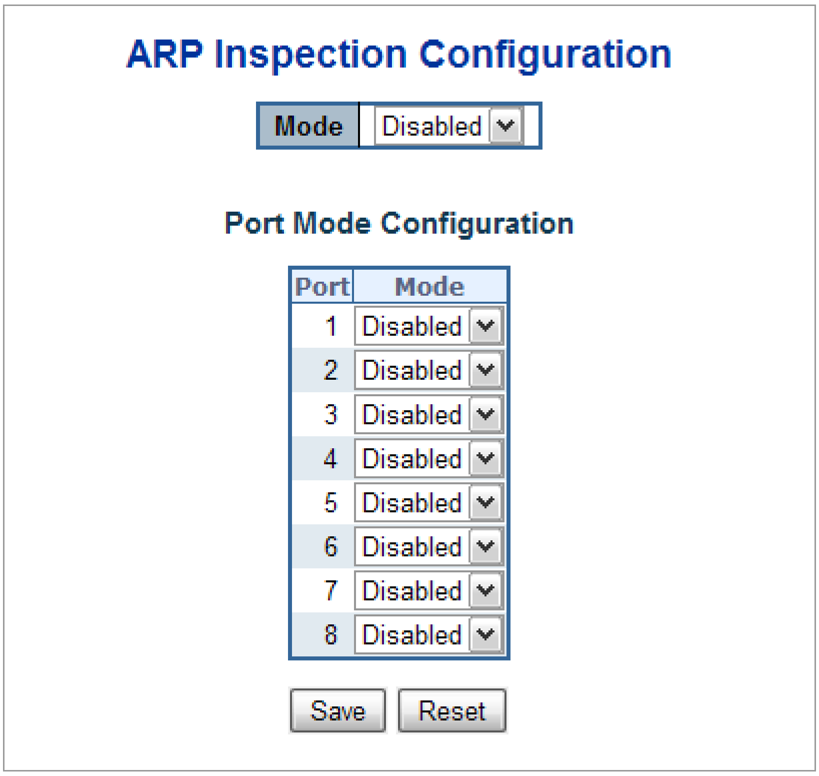
The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **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 netwok with IP address.
• **Adding new entry**	Click **Adding new entry** to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click "**Save**".

4.12.9 ARP Inspection

This page provides ARP Inspection related configuration.

ARP Inspection is a secure feautre. 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.



ARP Inspection Configuration

Mode: Disabled

Port Mode Configuration

Port	Mode
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

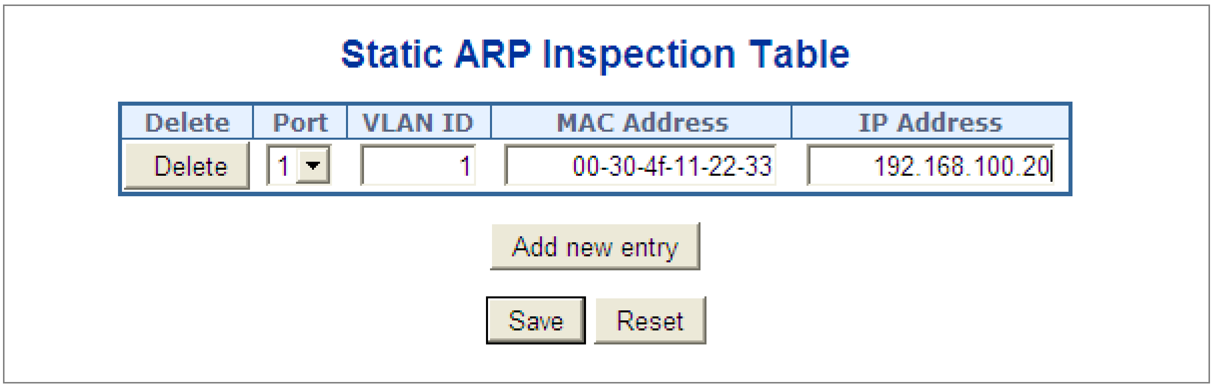
Figure 4-12-11 ARP Inspection Configuration page screenshot

The page includes the following fields:

Object	Description
• **Mode**	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.

4.12.10 ARP Inspection Static Table

Configure ARP Inspection Static Table on this page.



Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1 ▾	1	00-30-4f-11-22-33	192.168.100.20

Figure 4-12-12 Static ARP Inspection 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.
• **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. The format of MAC Address is "xx-xx-xx-xx-xx-xx".
• **IP Address**	Allowed Source IP address in ARP request packets.
• **Adding new entry**	Click **Adding new entry** to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "**Save**".

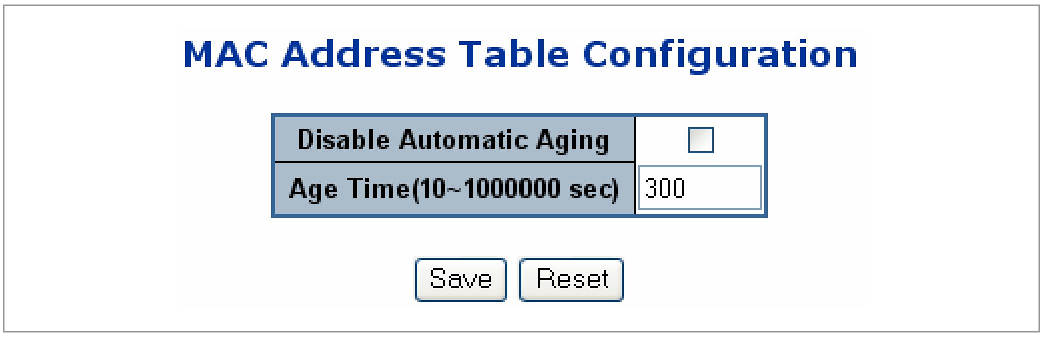
4.13 Address Table

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 here. The MAC Address Table Configuration screen in Figure 4-13-1 appears.



MAC Address Table Configuration

Disable Automatic Aging	□
Age Time(10~1000000 sec)	300

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

Aging Configuration

The page includes the following fields:

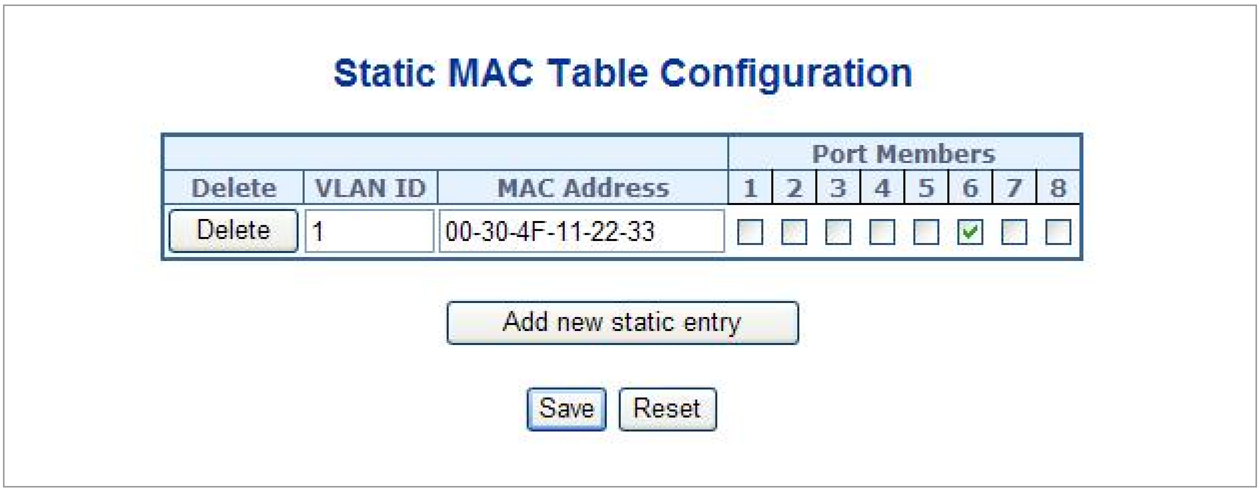
Object	Description
• **Disable Automatic Aging**	Enables/disables the the automatic aging of dynamic entries
• **Aging Time**	The time after which a learned entry is discarded. By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging. (Range: 10-10000000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

4.13.2 Static MAC Table Configuration

The Static MAC Address Table is configured on this page. The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

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.



Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Port Members							
			1	2	3	4	5	6	7	8
Delete	1	00-30-4F-11-22-33	□	□	□	□	□	☑	□	□

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

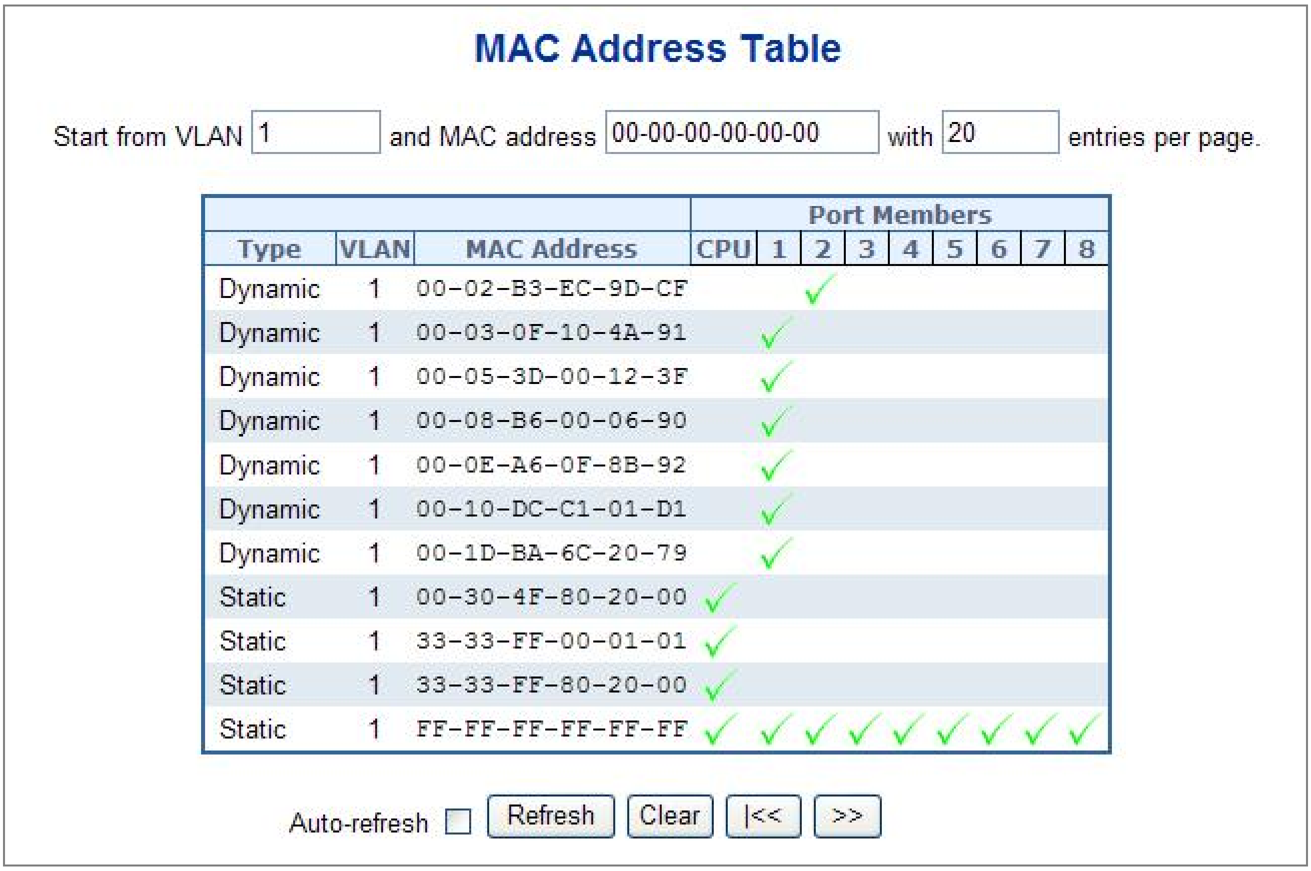
The page includes the following fields:

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.
• **Adding a New Static Entry**	Click **Adding new static entry** to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

4.13.3 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.



MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members								
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8
Dynamic	1	00-02-B3-EC-9D-CF			✓						
Dynamic	1	00-03-0F-10-4A-91		✓							
Dynamic	1	00-05-3D-00-12-3F		✓							
Dynamic	1	00-08-B6-00-06-90		✓							
Dynamic	1	00-0E-A6-0F-8B-92		✓							
Dynamic	1	00-10-DC-C1-01-D1		✓							
Dynamic	1	00-1D-BA-6C-20-79		✓							
Static	1	00-30-4F-80-20-00	✓								
Static	1	33-33-FF-00-01-01	✓								
Static	1	33-33-FF-80-20-00	✓								
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 4-13-3 MAC Address Table Status page screenshot

Navigating the MAC Table

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

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

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

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

MAC Table Columns

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.

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

Clear : Flushes all dynamic entries.

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

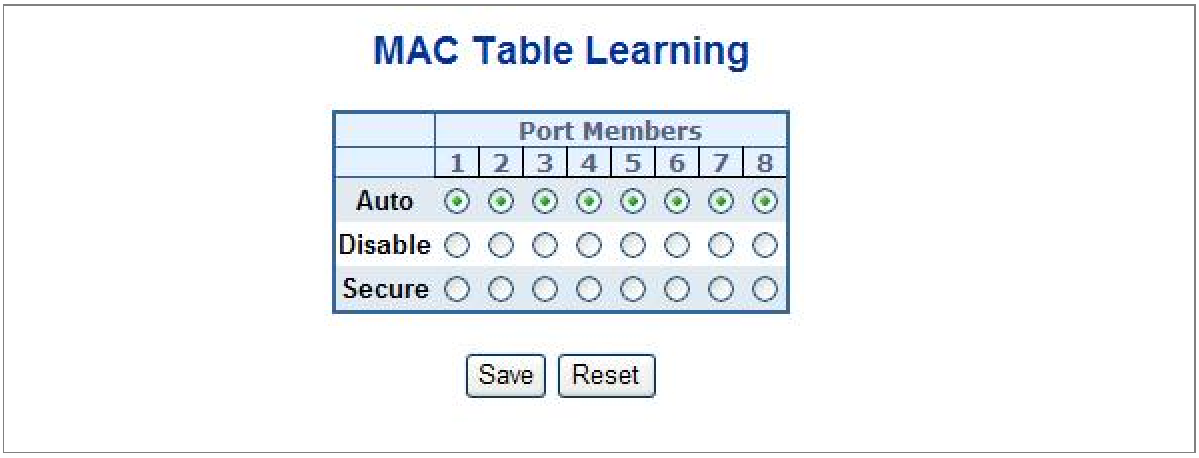
>>|: Updates the table, starting with the entry after the last entry currently displayed.

4.13.4 MAC Table Learning

The MAC Address Table Learning is configured on this page.

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:



MAC Table Learning

	Port Members							
	1	2	3	4	5	6	7	8
Auto	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○

Figure 4-13-4 Port Security Settings page 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.

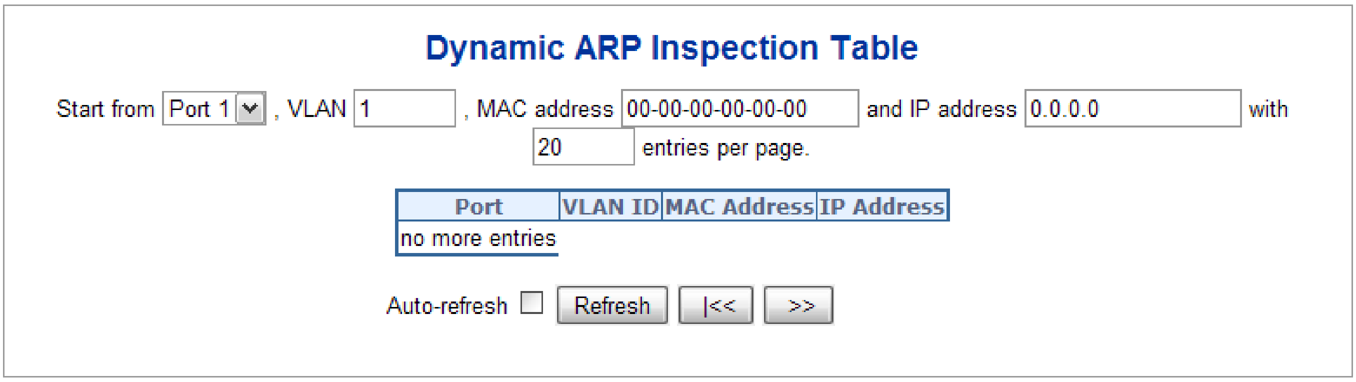
- **Secure**	Only static MAC entries are learned, all other frames are dropped.

Note

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.

4.13.5 Dynamic ARP Inspection Table

This page is to display Dynamic ARP Inspection entries.



Dynamic ARP Inspection Table

Start from Port 1 , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

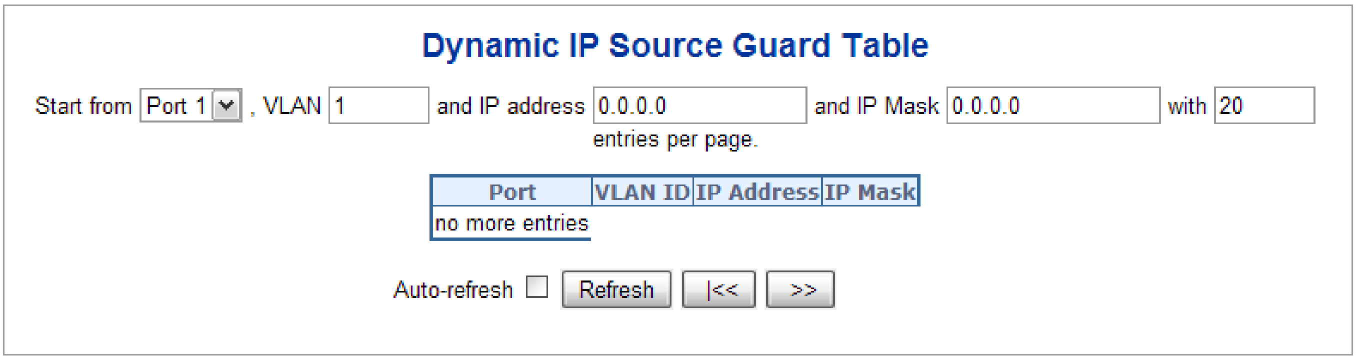
Port	VLAN ID	MAC Address	IP Address
no more entries			

Auto-refresh □ Refresh |<< >>

Figure 4-13-5 Dynamic ARP Inspection Table page screenshot

4.13.6 Dynamic IP Source Guard Table

This page is to display Dynamic IP Source Guard entries.



Dynamic IP Source Guard Table

Start from Port 1 , VLAN 1 and IP address 0.0.0.0 and IP Mask 0.0.0.0 with 20 entries per page.

Port	VLAN ID	IP Address	IP Mask
no more entries			

Auto-refresh □ Refresh |<< >>

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

4.14 LLDP

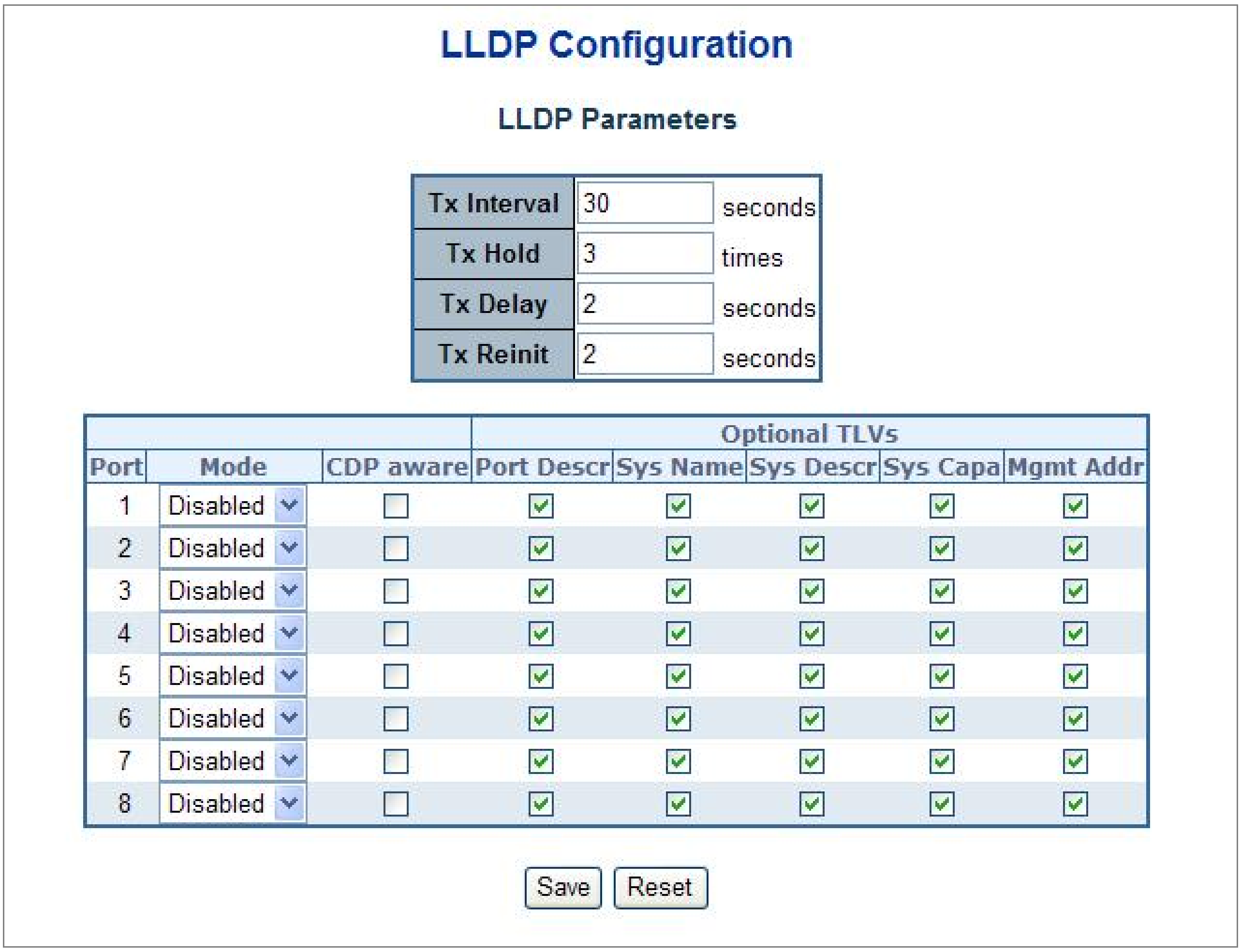
4.14.1 Link Layer Discovery Protocol

LLDP is an IEEE 802.1ab standard protocol. The **Link Layer Discovery Protocol(LLDP)**, is used for network discovery, and works by having the units in the network exchanging information with their neighbor devices using LLDP frames on the local broadcaset 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.



LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	3	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
1	Disabled	□	☑	☑	☑	☑	☑
2	Disabled	□	☑	☑	☑	☑	☑
3	Disabled	□	☑	☑	☑	☑	☑
4	Disabled	□	☑	☑	☑	☑	☑
5	Disabled	□	☑	☑	☑	☑	☑
6	Disabled	□	☑	☑	☑	☑	☑
7	Disabled	□	☑	☑	☑	☑	☑
8	Disabled	□	☑	☑	☑	☑	☑

Figure 4-14-1 LLDP Configuration page screenshot

- **LLDP Parameters**

The page includes the following fields:

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

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

4.14.2.1 LLDP Port Configuration

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

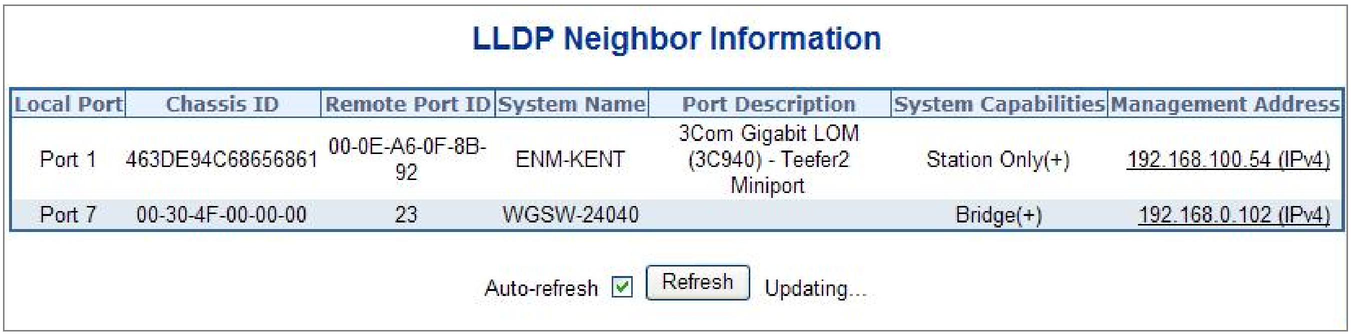
The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical LLDP port.
• **Mode**	Select LLDP mode. • **Rx only** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. • **Tx only** The switch will drop LLDP information received from neighbors, but will send out LLDP information. • **Disabled** The switch will not send out LLDP information, and will drop LLDP information received from neighbors. • **Enabled** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
• **Port Descr**	Optional TLV: When checked the "port description" is included in LLDP information transmitted.

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

4.14.3 LLDP Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP Neighbor screen in Figure 4-14-2 appears.



LLDP Neighbor Information

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 1	463DE94C68656861	00-0E-A6-0F-8B-92	ENM-KENT	3Com Gigabit LOM (3C940) - Teefer2 Miniport	Station Only(+)	192.168.100.54 (IPv4)
Port 7	00-30-4F-00-00-00	23	WGSW-24040		Bridge(+)	192.168.0.102 (IPv4)

Figure 4-14-2 LLDP Neighbor Information page screenshot

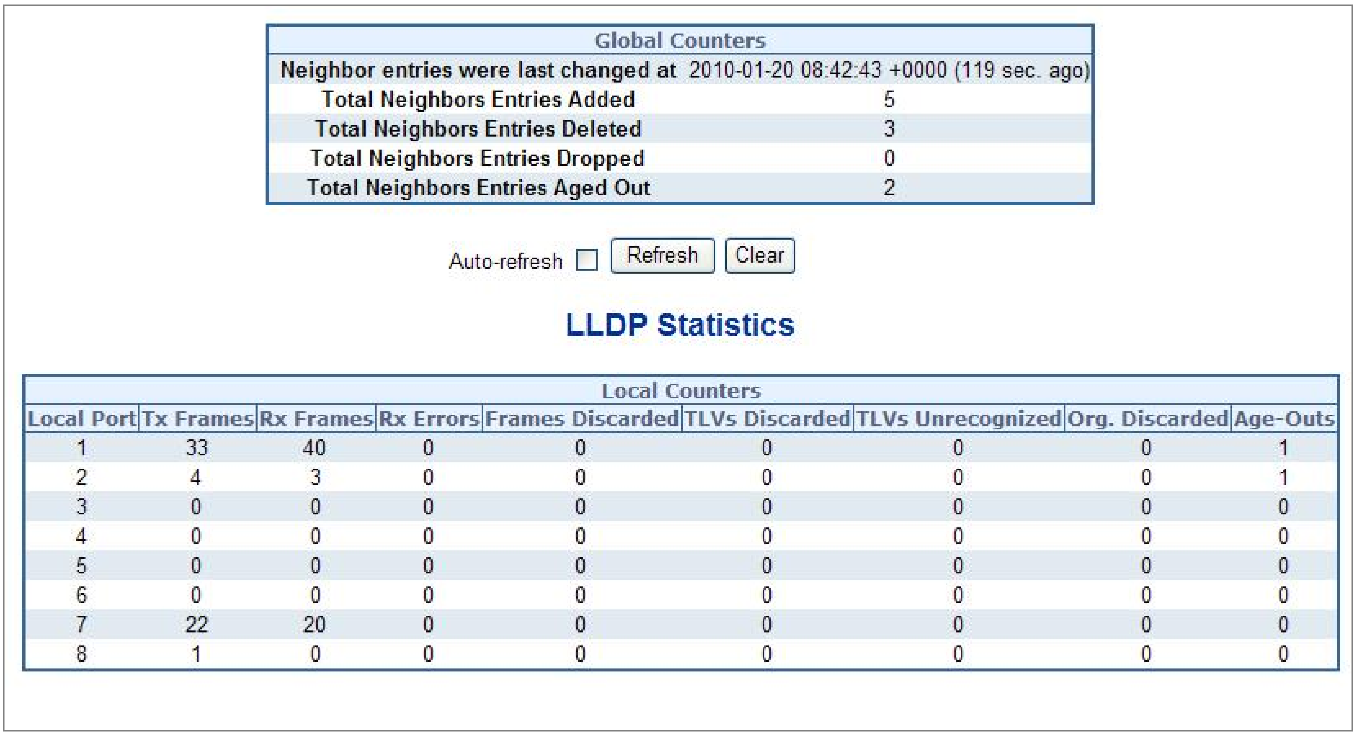
The columns hold the following information:

Object	Description
• **Local Port**	The port on which the LLDP frame was received.
• **Chassis ID**	The **Chassis ID** is the identification of the neighbor's LLDP frames.
• **Remote Port ID**	The **Remote Port ID** is the identification of the neighbor port.

• **System Name**	**System Name** is the name advertised by the neighbor unit.
• **Port Description**	**Port Description** is the port description advertised by the neighbor unit.
• **System Capabilities**	**System Capabilities** describes the neighbor unit's capabilities. The possible capabilities are: **1. Other** **2. Repeater** **3. Bridge** **4. WLAN Access Point** **5. Router** **6. Telephone** **7. DOCSIS cable device** **8. Station only** **9. Reserved** When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
• **Management Address**	**Management Address** is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.

4.14.4 LLDP Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refers to counters for the currently selected switch. The LLDP Statistics screen in Figure 4-14-3 appears.



Global Counters	
Neighbor entries were last changed at	2010-01-20 08:42:43 +0000 (119 sec. ago)
Total Neighbors Entries Added	5
Total Neighbors Entries Deleted	3
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	2

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	33	40	0	0	0	0	0	1
2	4	3	0	0	0	0	0	1
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	22	20	0	0	0	0	0	0
8	1	0	0	0	0	0	0	0

Figure 4-14-3 LLDP Statistics page screenshot

- **Global Counters**

The page includes the following fields:

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 page includes the following fields:

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

4.15 Network Diagnastics

This section provide the Physical layer and IP layer network diagnastics 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 Diagnastic**

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 Diagsastic

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.

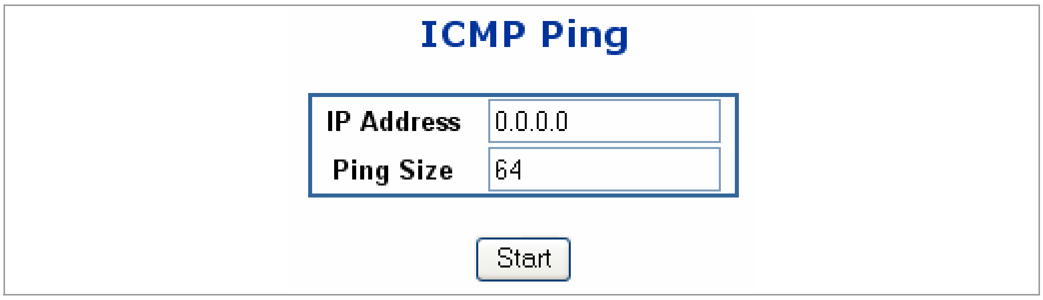
After the diagnostics are finished, the link is reestablished. And the following functions are available.

- Coupling between cable pairs.
- Cable pair termination
- Cable Length

4.15.1 Ping

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

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



ICMP Ping

IP Address	0.0.0.0
Ping Size	64

Figure 4-15-1 ICMP Ping page screenshot

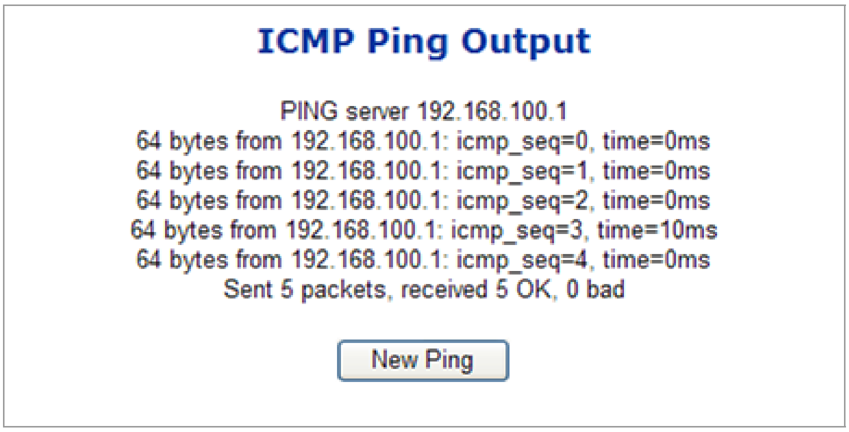
The page includes the following fields:

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

Note

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

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



ICMP Ping Output

```
PING server 192.168.100.1
64 bytes from 192.168.100.1: icmp_seq=0, time=0ms
64 bytes from 192.168.100.1: icmp_seq=1, time=0ms
64 bytes from 192.168.100.1: icmp_seq=2, time=0ms
64 bytes from 192.168.100.1: icmp_seq=3, time=10ms
64 bytes from 192.168.100.1: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

Figure 4-15-2 ICMP Ping Output page screenshot

4.15.2 IPv6 Ping

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press , 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.

```
PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

You can configure the following properties of the issued ICMP packets:

The page includes the following fields:

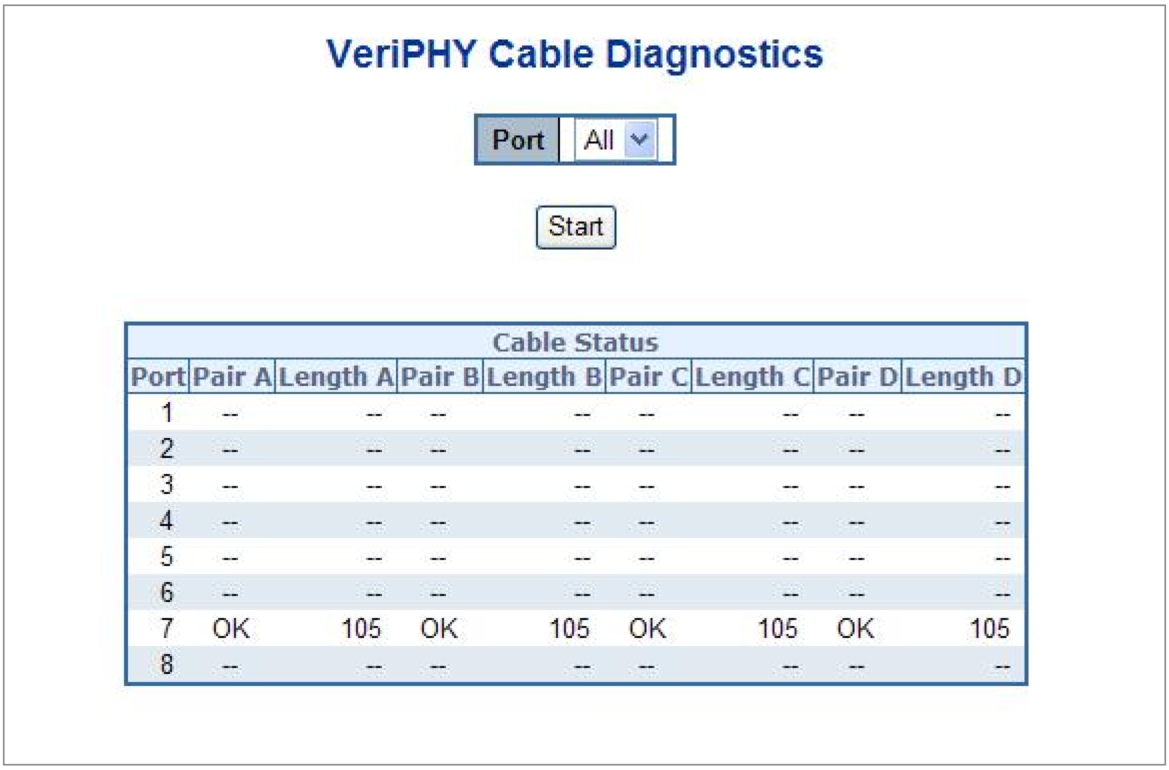
Object	Description
• **IPv6 Address**	The destination IPv6 Address.
• **Ping Size**	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

4.15.3 Cable Diagnostics

This page is used for running the Cable Diagnostics.

Press **Start** 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 Cable Diagnastic is complete. The ports belong to the currently selected stack unit, as reflected by the page header.



VeriPHY Cable Diagnostics

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	OK	105	OK	105	OK	105	OK	105
8	--	--	--	--	--	--	--	--

Figure 4-15-3 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.

Note

Be sure to running the Cable diagnostics with standard Cat 5e or Cat 6 UTP cable. With some of the UTP cables that not match the standard of Cat 5e, it might cause the 10/100Base-TX link down after the cable 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.

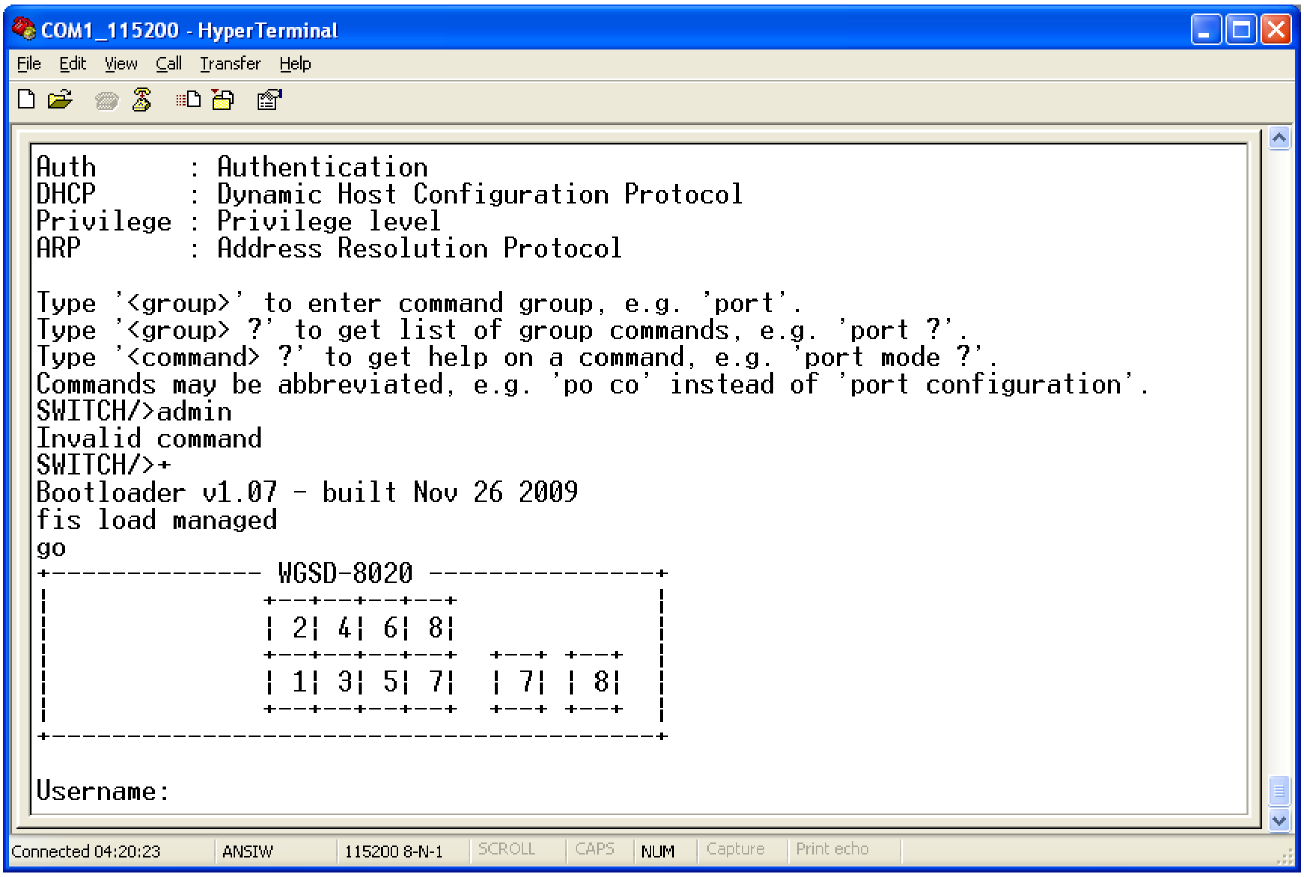
This chapter describes how to use the Command Line Interface (CLI).

Logon to the Console

Once the terminal has connected to the device, power on the WGSD Managed Switch, the terminal will display that it is running testing procedures.

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

User Name: **admin**
Password: **admin**



```
Auth      : Authentication
DHCP      : Dynamic Host Configuration Protocol
Privilege : Privilege level
ARP       : Address Resolution Protocol

Type '<group>' to enter command group, e.g. 'port'.
Type '<group> ?' to get list of group commands, e.g. 'port ?'.
Type '<command> ?' to get help on a command, e.g. 'port mode ?'.
Commands may be abbreviated, e.g. 'po co' instead of 'port configuration'.
SWITCH/>admin
Invalid command
SWITCH/>+
Bootloader v1.07 - built Nov 26 2009
fis load managed
go
+--------------- WGSD-8020 ---------------+
|              +---+---+---+---+          |
|              | 2| 4| 6| 8|              |
|              +---+---+---+---+  +---+ +---+ |
|              | 1| 3| 5| 7|  | 7| | 8|  |
|              +---+---+---+---+  +---+ +---+ |
|                                         |
+-----------------------------------------+

Username:
```

Figure 5-1-1 WGSD-8020 Managed Switch Console Login screen

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 WGSD Managed Switch is shipped with default IP address as following.

IP Address : **192.168.0.100**

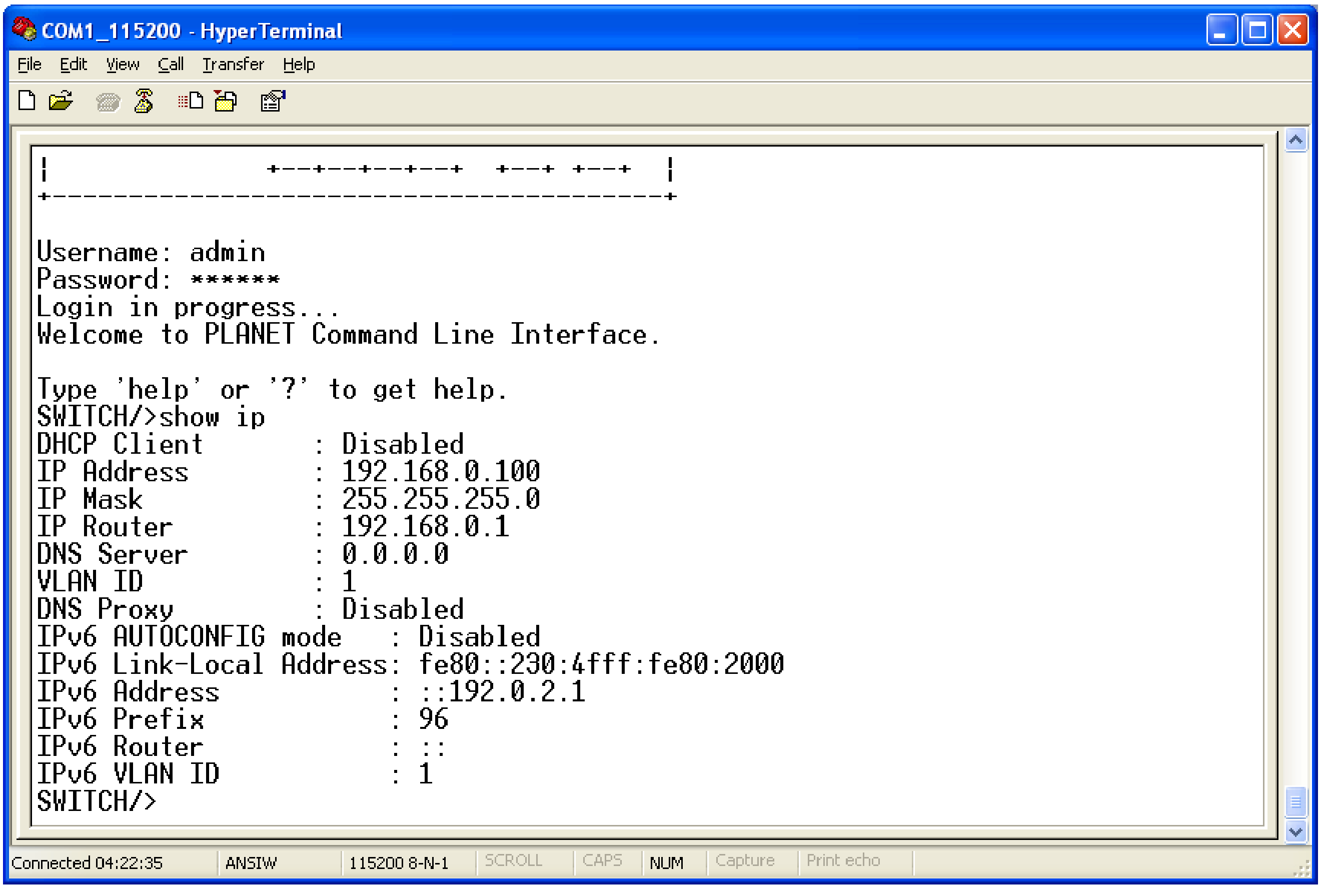
Subnet Mask : **255.255.255.0**

To check the current IP address or modify a new IP address for the Switch, please use the procedures as follow:

- **Show the current IP address**

1. On **"Switch/> "** prompt, enter **"show ip".**

2. The screen displays the current IP address, Subnet Mask and Gateway. As show in Figure 5-1-2.



```
|              +--+--+--+--+  +--+ +--+   |
+------------------------------------------+

Username: admin
Password: ******
Login in progress...
Welcome to PLANET Command Line Interface.

Type 'help' or '?' to get help.
SWITCH/>show ip
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:fe80:2000
IPv6 Address            : ::192.0.2.1
IPv6 Prefix             : 96
IPv6 Router             : ::
IPv6 VLAN ID            : 1
SWITCH/>
```

Figure 5-1-2 Show IP information screen

- **Configure IP address**

3. On "**Switch/>** " prompt, enter the following command and press **<Enter>.** As show in Figure 5-1-3.

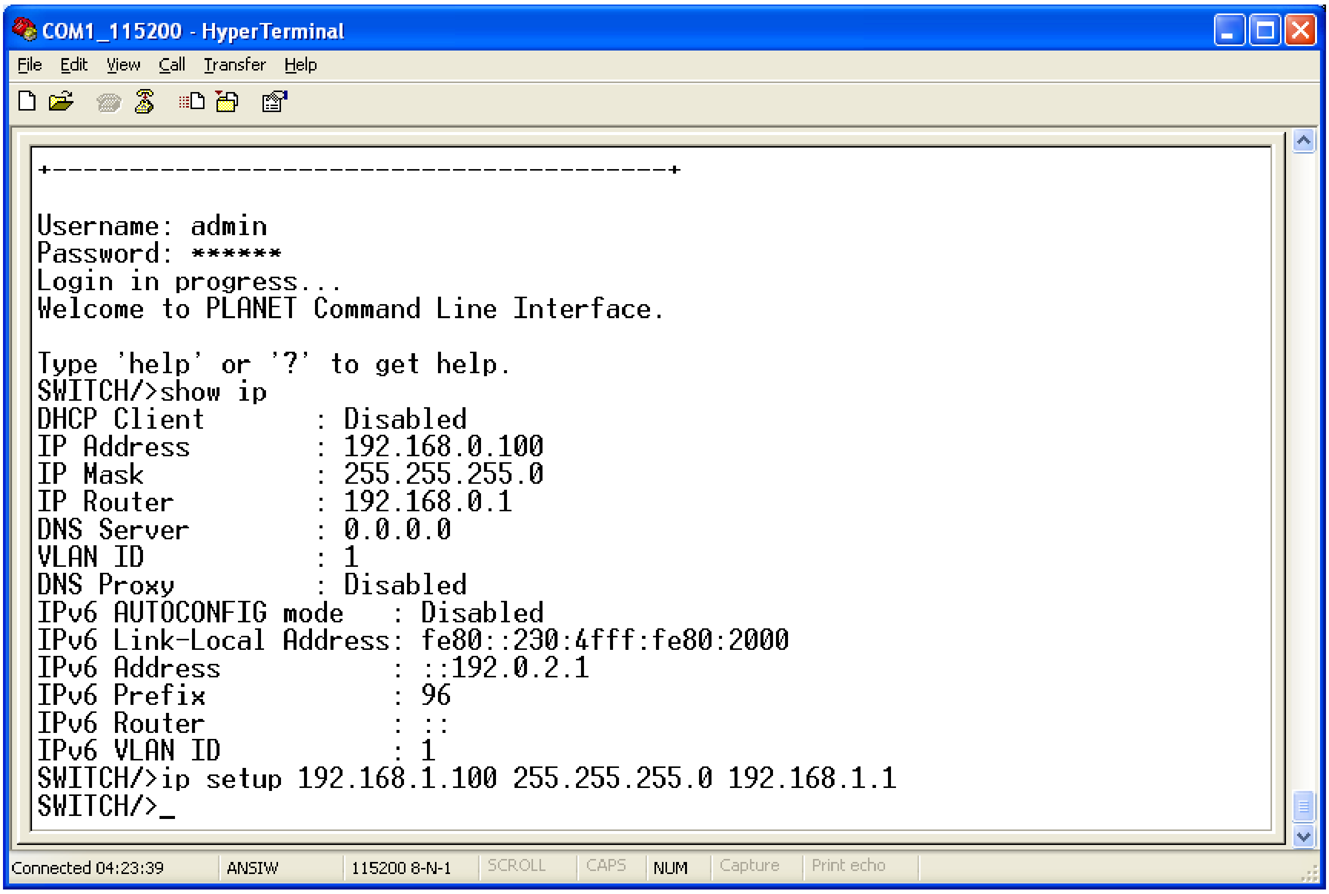
```
Switch/> ip setup 192.168.1.100 255.255.255.0 192.168.1.1
```

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

IP: 192.168.1.100

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1


COM1_115200 - HyperTerminal
File Edit View Call Transfer Help
Connected 04:23:39 ANSIW 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
+-----------------------------------------+

Username: admin
Password: ******
Login in progress...
Welcome to PLANET Command Line Interface.

Type 'help' or '?' to get help.
SWITCH/>show ip
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:fe80:2000
IPv6 Address            : ::192.0.2.1
IPv6 Prefix             : 96
IPv6 Router             : ::
IPv6 VLAN ID            : 1
SWITCH/>ip setup 192.168.1.100 255.255.255.0 192.168.1.1
SWITCH/>_
```

Figure 5-1-3 Set IP address screen

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

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

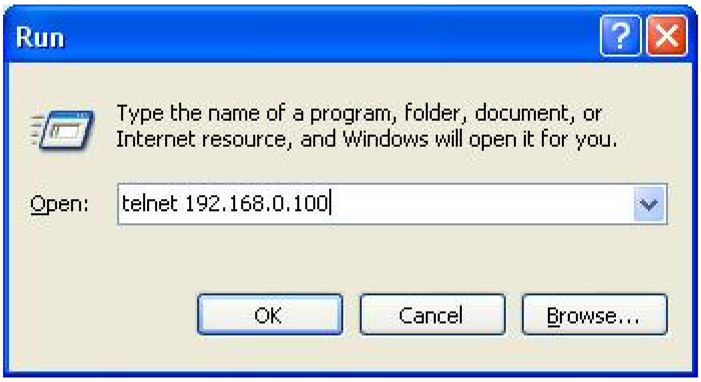
You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action 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. Telnet operates over the IP transport protocol. In this environment, your management station and target Managed Switch you want to manage over the network must have a valid IP address.

Note: The IP address for the Managed Switch is 192.168.0.100 by default.

To login the Managed Switch, run Telnet client program included in Windows with the specified Telnet target.

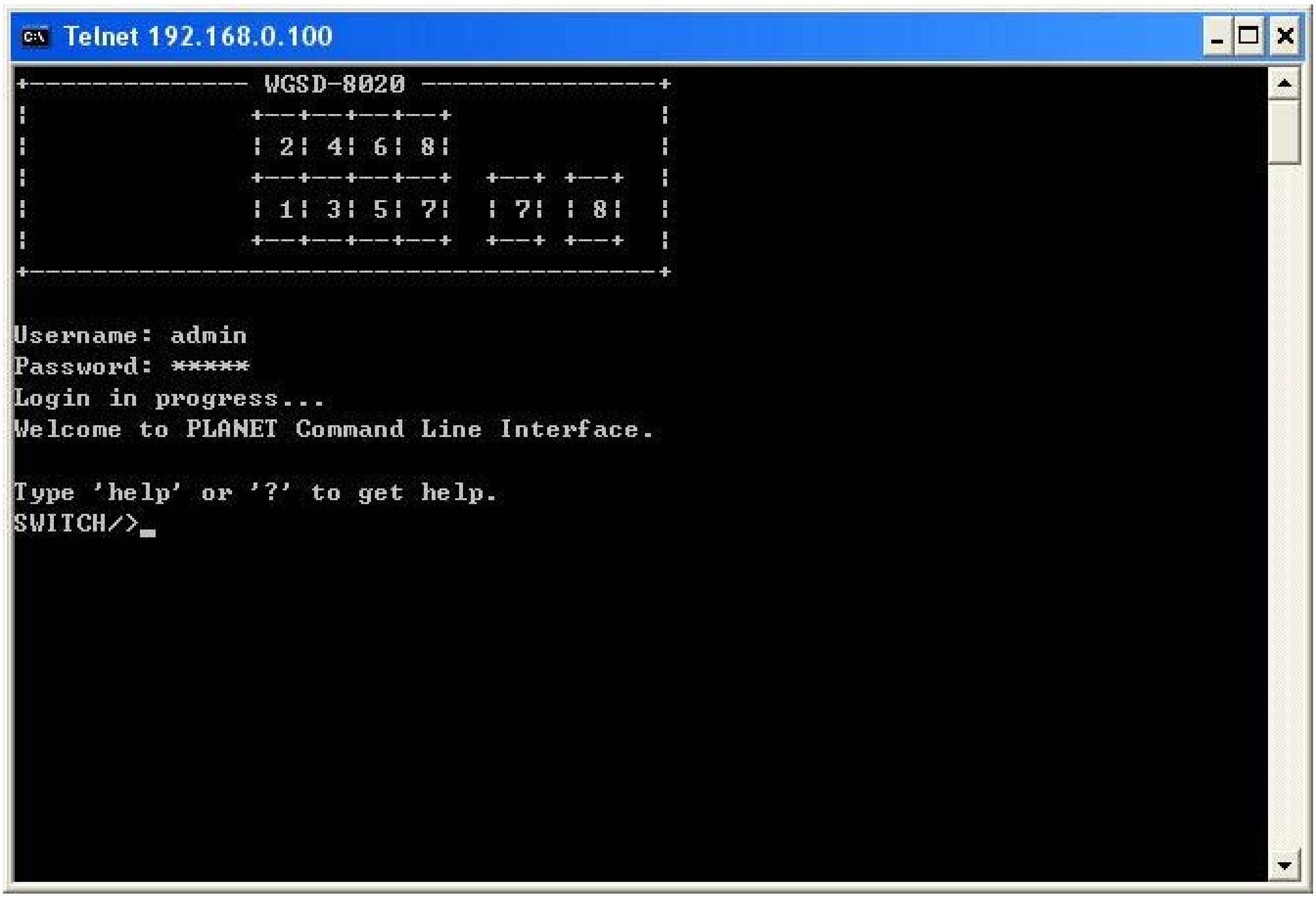


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:

telnet 192.168.0.100

Figure 5-2-1 Run telnet client program included in Windows

The Managed Switch asks for user name and password for remote login when using telnet, please enter **"admin / admin"**.



```
+--------------- WGSD-8020 ---------------+
|              +---+---+---+---+          |
|              | 2| 4| 6| 8|              |
|              +---+---+---+---+ +---+ +---+ |
|              | 1| 3| 5| 7|  | 7| | 8|  |
|              +---+---+---+---+ +---+ +---+ |
+-----------------------------------------+

Username: admin
Password: *****
Login in progress...
Welcome to PLANET Command Line Interface.

Type 'help' or '?' to get help.
SWITCH/>_
```

Figure 5-2-2 Telnet login screen

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**
SNMP	**Simple Network Management Protocol**
Port	**Port management**
Aggr	**Link Aggregation**
VLAN	**Virtual LAN**
STP	**Spanning Tree Protocol**
IGMP	**Internet Group Management Protocol snooping**
QoS	**Quality of Service**
Dot1x	**IEEE 802.1X port authentication**
ACL	**Access Control List**
MAC	**MAC address table**
LLDP	**Link Layer Discovery Protocol**
Auth	**Authentication**
DHCP	**Dynamic Host Configuration Protocol**
Privilege	**Privilege level**
ARP	**Address Resolution Protocol**

6.1 System Command

System Configuration

Description:

Show system configuration.

Syntax:

System Configuration [all] [<port_list>]

Parameters:

all : Show all switch configuration, default: Show system configuration

<port_list>: Port list or 'all', default: All ports

Example:

To display system information:

```
Switch/>system configuration
System Name       : WGSD-8020
System Password: admin
CLI Prompt        : Switch
Timezone Offset: 0
MAC Address       : 00-30-4f-24-04-03
System Time       : 1970-01-01 03:13:21 +0000
System Uptime    : 03:13:21

SID    Software Version
---    ----------------
3       Beta_080813
```

System Reboot

Description:

Reboot the system.

Syntax:

System Reboot

Example:

To reboot device without changing any of the settings:

```
Switch/>system reboot
```

System Restore Default

Description:

Restore factory default configuration.

Syntax:

System Restore Default [keep_ip]

Parameters:

keep_ip: Keep IP configuration, default: Restore full configuration

Example:

To restore default value but not reset IP address:

```
Switch/>system restore default keep_ip
```

System 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 system device contact:

```
SWITCH/>system contact 1
```

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:

WGSD-8020

Example:

To set device title:

```
Switch/>system name WGSD-8020-LAB
```

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 system location:

```
SWITCH/>system location 1
```

System Password

Description:

Set or show the system password.

Syntax:

System Password [<password>]

Parameters:

<password>: System password or 'clear' to clear

Default Setting:

admin

Example:

To set password:

```
Switch/>system password admin
```

System 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:

Empty

Example:

To set system prompt:

```
SWITCH/>system prompt WGSD-8020
WGSD-8020>
```

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
```

System Access Configuration

Description:

Show access management configuration.

Syntax:

System Access Configuration

Example:

Show system access configuration:

```
SWITCH/>system access configuration
System Access Mode : Disabled
System Access number of entries: 0
```

System Access Mode

Description:

Set or show the access management mode.

Syntax:

System Access Mode [enable|disable]

Parameters:

enable : Enable access management

disable: Disable access management

(**default**: Show access management mode)

Default Setting:

disable

Example:

To set system access mode:

```
SWITCH/>system access mode enable
```

System Access Add

Description:

Add access management entry.

Syntax:

System 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 interface

snmp : SNMP interface

telnet : TELNET interface

(**default**: Show configured and current mode)

Default Setting:

Empty

Example:

To set system access add:

```
SWITCH/>system access add 1 192.168.0.20 192.168.0.30 snmp
```

System Access Ipv6 Add

Description:

Add access management IPv6 entry.

Syntax:

System 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<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,'::192.1.2.3web : WEB interface

snmp : SNMP interface

telnet : TELNET interface

(**default**: Show configured and current mode)

Default Setting:

empty

Example:

To set IPv6 address:

```
SWITCH/>system access ipv6 add 1 2001::192:168:0:1 2001::192:168:0:2 telnet
```

System Access Delet

Description:

Delete access management entry.

Syntax:

System Access Delete <access_id>

Parameters:

<access_id>: entry index (1-16)

Default Setting:

0.0.0.0

Example:

To set system access delet:

```
SWITCH/>system access delet 1
```

System Access Lookup

Description:

Lookup access management entry.

Syntax:

System Access Lookup [<access_id>]

Parameters:

<access_id>: entry index (1-16)

Example:

Show system access lookup:

```
SWITCH/>system access lookup 1
```

System Access Clear

Description:

Clear access management entry.

Syntax:

System Access Clear

Example:

Clear access management entry:

```
SWITCH/>system access clear
```

System Access Statistics

Description:

Show or clear access management statistics.

Syntax:

System Access Statistics [clear]

Parameters:

clear: Clear access management statistics

Example:

Show access management statistics:

```
SWITCH/>system access statistics

Access Management Statistics:
-----------------------------
HTTP      Receive:         0    Allow:         0    Discard:         0
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
```

System HTTPS Configuration

Description:

Show HTTPS configuration.

Syntax:

System HTTPS Configuration

Example:

Show HTTPS configuration:

```
SWITCH/>system https configuration
HTTPS Mode              : Disabled
HTTPS Redirect Mode    : Disabled
```

System HTTPS Mode

Description:

Set or show the HTTPS mode.

Syntax:

System HTTPS Mode [enable|disable]

Parameters:

enable : Enable HTTPS

disable: Disable HTTPS

(**default:** Show HTTPS mode)

Default Setting:

Disable

Example:

To set HTTPS mode:

```
SWITCH/>system https mode enable
```

System HTTPS Redirect

Description:

Set or show the HTTPS redirect mode. Automatic redirect web browser to HTTPS during HTTPS mode enabled.

Syntax:

System HTTPS Redirect [enable|disable]

Parameters:

enable : Enable HTTPS redirect

disable: Disable HTTPS redirect

(**default:** Show HTTPS redirect mode)

Default Setting:

Disable

Example:

To set HTTPS redirect:

```
SWITCH/>system https redirect enable
```

System SSH Configuration

Description:

Show SSH configuration.

Syntax:

System SSH Configuration

Parameters:

Disable

Example:

Show SSH configuration:

```
SWITCH/>system ssh configuration
SSH Mode : Disabled
```

System SSH Mode

Description:

Set or show the SSH mode.

Syntax:

System SSH Mode [enable|disable]

Parameters:

enable : Enable SSH

disable: Disable SSH

(**default**: Show SSH mode)

Default Setting:

Disable

Example:

To set SSH mode:

```
SWITCH/>system ssh mode enable
```

System UPnP Configuration

Description:

Show UPnP configuration.

Syntax:

System UPnP Configuration

Example:

Show UPnP configuration:

```
SWITCH/>system upnp configuration
UPnP Mode                          : Disabled
UPnP TTL                           : 4
UPnP Advertising Duration : 100
```

System UPnP mode

Description:

Set or show the UPnP mode.

Syntax:

System UPnP Mode [enable|disable]

Parameters:

enable : Enable UPnP

disable: Disable UPnP

(**default**: Show UPnP mode)

Default Setting:

Disable

Example:

To set UPnP mode:

```
SWITCH/>system upnp mode enable
```

System UPnP TTL

Description:

Set or show the TTL value of the IP header in SSDP messages.

Syntax:

System UPnP TTL [<ttl>]

Parameters:

<ttl>: ttl range (1..255), default: Show UPnP TTL

Default Setting:

4

Example:

To set UPnP TTL:

```
SWITCH/>System upnp ttl 10
```

System UPnP Advertising Duration

Description:

Set or show UPnP Advertising Duration.

Syntax:

System UPnP Advertising Duration [<duration>]

Parameters:

<duration>: duration range (100..86400), default: Show UPnP duration range

Default Setting:

100

Example:

To set UPnP duration:

```
SWITCH/>system upnp advertising duration 200
```

System Firmware Load

Description:

Load new firmware from TFTP server.

Syntax:

System Firmware Load <ip_server> <file_name>

Parameters:

<ip_server>: TFTP server IP address (a.b.c.d)

<file_name>: Firmware file name

System Firmware IPv6 Load

Description:

Load new firmware from IPv6 TFTP server.

Syntax:

System Firmware IPv6 Load <ipv6_server> <file_name>

Parameters:

<ipv6_server>: TFTP server IPv6 address

<file_name> : Configuration file name

System Config Save

Description:

Save configuration to TFTP server.

Syntax:

System Config Save <ip_server> <file_name>

Parameters:

<ip_server>: TFTP server IP address (a.b.c.d)

<file_name>: Configuration file name

System Config Load

Description:

Load configuration from TFTP server.

Syntax:

System 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

6.2 IP Management Command

IP Configuration

Description:

Show IP configuration.

Syntax:

IP Configuration

Example:

Show IP configuration:

```
Switch/>ip configuration
DHCP Client: Disabled
IP Address : 192.168.100.105
IP Mask      : 255.255.255.0
IP Router   : 192.168.100.1
VLAN ID      : 1
SNTP Server: 0.0.0.0
```

IP DHCP

Description:

Set or show the DHCP client mode.

Syntax:

IP DHCP [enable|disable]

Parameters:

enable : Enable or renew DHCP client

disable: Disable DHCP client

Default Setting:

Disable

Example:

Disable DHCP sever:

```
SWITCH/>ip dhcp disable
```

IP Setup

Description:

Set or show the IP setup.

Syntax:

IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

Parameters:

<ip_addr> : IP address (a.b.c.d), default: Show IP address

<ip_mask> : IP subnet mask (a.b.c.d), default: Show IP mask

<ip_router>: IP router (a.b.c.d), default: Show IP router

<vid> : VLAN ID (1-4095), default: Show VLAN ID

Default Setting:

IP Address : 192.168.0.100

IP Mask : 255.255.255.0

IP Router : 192.168.0.1

VLAN ID : 1

Example:

Set IP address:

```
SWITCH/>ip setup 192.168.0.100 255.255.255.0
```

IP Ping

Description:

Ping IP address (ICMP echo).

Syntax:

IP Ping <ip_addr> [<ping_length>]

Parameters:

<ip_addr> : IP host address (a.b.c.d)

<ping_length>: Ping data length (8-1400), excluding MAC, IP and ICMP headers

Example:

```
SWITCH/>ip ping 192.168.0.51
PING server 192.168.0.51
60 bytes from 192.168.0.51: icmp_seq=0, time=0ms
60 bytes from 192.168.0.51: icmp_seq=1, time=0ms
60 bytes from 192.168.0.51: icmp_seq=2, time=10ms
60 bytes from 192.168.0.51: icmp_seq=3, time=0ms
60 bytes from 192.168.0.51: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

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:

To set DNS address:

```
SWITCH/>ip DNS 168.95.1.1
```

IP DNS Proxy

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

IP NTP Configuration

Description:

Show NTP configuration.

Syntax:

IP NTP Configuration

Default Setting:

Disable

Example:

Show NTP configuration:

```
SWITCH/> 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)

Example:

To set IP 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 Delet

Description:

Delete NTP server entry.

Syntax:

IP NTP Server Delete <server_index>

Parameters:

<server_index>: The server index (1-5)

Example:

To delet NTP server:

```
SWITCH/>ip ntp server delet 1
```

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,'::SWITCH/IP>

IP IPv6 AUTOCONFIG

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

Example:

To set IPv6 AUTOCONFIG:

```
SWITCH/>ip ipv6 autoconfig enable
```

IP 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 appea<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 le<vid> : VLAN ID (1-4095), default: Show VLAN ID

Default Setting:

IPv6 AUTOCONFIG mode : Enabled

IPv6 Link-Local Address : fe80::230:4fff:fe80:20aa

IPv6 Address : ::192.0.2.1

IPv6 Prefix : 96

IPv6 Router : ::

IPv6 VLAN ID : 1

Example:

To set IPv6 address:

```
SWITCH/>ip ipv6 setup 2001::192:168:0:100 96 2001::192:168:0:1 1
```

IP IPv6 Ping6

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.

<ping_length>: Ping data length (8-1400), excluding MAC, IP and ICMP headers.

Example:

```
SWITCH/>ip ipv6 ping6 ????????????????????????
```

IP SourceGuard Configuration

Description:

Show IP source guard configuration.

Syntax:

IP SourceGuard Configuration

Example:

Show IP source guard configuration.:

```
SWITCH/>ip sourceguard 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

IP Source Guard Static Table:

Port   VLAN   IP Address        IP Mask
----   ----   ---------------   ---------------

IP Source Guard Dynamic Table:

Port   VLAN   IP Address        IP Mask
----   ----   ---------------   ---------------
```

IP SourceGuard Mode

Description:

Set or show IP source guard mode.

Syntax:

IP SourceGuard Mode [enable|disable]

Parameters:

enable : Enable IP Source Guard

disable : Disable IP Source Guard

Default Setting:

Disable

Example:

To set source guard mode:

```
SWITCH/>ip sourceguard mode enable
```

IP SourceGuard Port

Description:

Set or show the IP Source Guard port mode.

Syntax:

IP SourceGuard port [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable IP Source Guard port

disable : Disable IP Source Guard port

(**default**: Show IP Source Guard port mode)

Default Setting:

```
Port   Port Mode
----   -----------
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
```

Example:

To set source guard port:

```
SWITCH/>ip sourceguard port 1
```

IP SourceGuard Limit

Description:

Set or show the IP Source Guard port limitation for dynamic entries.

Syntax:

IP SourceGuard limit [<port_list>] [<dynamic_entry_limit>|unlimited]

Parameters:

<port_list> : Port list or 'all', default: All ports

<dynamic_entry_limit>|unlimited: dynamic entry limit (0-3) or unlimited

Default Setting:

```
Port   Dynamic Entry Limit
----   ---------------------
1      unlimited
2      unlimited
3      unlimited
4      unlimited
5      unlimited
6      unlimited
7      unlimited
8      unlimited
```

Example:

To set source guard limit:

```
SWITCH/>ip sourceguard limit 1 1
```

IP SourceGuard Entry

Description:

Add, delete or show IP source guard static entries.

Syntax:

IP SourceGuard Entry [<port_list>] [add|del] [vid] [allowed_ip] [ip_mask]

Parameters:

<port_list>: Port list or 'all', default: All ports

add : Add new port IP source guard static entry

del : Del existing port IP source guard static entry

(**default**: Show port IP source guard static entry list)

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

Default Setting:

Emptry

Example:

To set source guard entry:

```
SWITCH/>ip sourceguard entry 1 add 1 192.168.0.50 255.255.255.0
```

IP SourceGuard Status

Description:

Show IP source guard dynamic entries.

Syntax:

IP SourceGuard Status

Example:

Show IP source guard dynamic entries:

```
SWITCH/>ip sourceguard status
```

6.3 SNMP Manamgement Command

SNMP Configuration

Description:

Show SNMP configuration.

Syntax:

SNMP Configuration

Example:

Show SNMP configuration

```
S SWITCH/>snmp configuration
SNMP Mode                          : Disabled
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                : Disabled
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
```

SNMP Mode

Description:

Set or show the SNMP mode.

Syntax:

SNMP Mode [enable|disable]

Parameters:

enable : Enable SNMP

disable: Disable SNMP

(**default**: Show SNMP mode)

Default Setting:

Disable

Example:

Set the SNMP mode

```
SWITCH/>snmp mode enable
```

SNMP Version

Description:

Set or show the SNMP protocol version.

Syntax:

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 the SNMP version

```
SWITCH/>snmp version 1
```

SNMP Read Community

Description:

Set or show the community string for SNMP read access.

Syntax:

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 the SNMP read community

```
SWITCH/>snmp read community private
```

SNMP Write Community

Description:

Set or show the community string for SNMP write access.

Syntax:

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 the SNMP write community

```
SWITCH/>snmp write community public
```

SNMP Trap Mode

Description:

Set or show the SNMP trap mode.

Syntax:

SNMP Trap Mode [enable|disable]

Parameters:

enable : Enable SNMP traps

disable: Disable SNMP traps

(**default**: Show SNMP trap mode)

Default Setting:

disable

Example:

Set the SNMP trap mode

```
SWITCH/>snmp trap mode enable
```

SNMP Trap Version

Description:

Set or show the SNMP trap protocol version.

Syntax:

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 the SNMP trap version

```
SWITCH/>snmp trap version 2c
```

SNMP Trap Community

Description:

Set or show the community string for SNMP traps.

Syntax:

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 the SNMP trap community

```
SWITCH/>snmp trap community private
```

SNMP Trap Destination

Description:

Set or Show the SNMP trap destination address.

Syntax:

SNMP Trap Destination [<ip_addr_string>]

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Default Setting:

empty

Example:

Set the SNMP trap destination

```
SWITCH/>snmp trap destination 192.168.0.20
```

SNMP Trap IPv6 Destination

Description:

Set or Show the SNMP trap destination IPv6 address.

Syntax:

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 appea SWITCH/SNMP>

Default Setting:

empty

Example:

Set the SNMP trap IPv6 destination

```
SWITCH/>snmp trap IPv6 destination ????????????????????
```

SNMP Trap Authentication Faulure

Description:

Set or show the SNMP authentication failure trap mode.

Syntax:

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:

Set the SNMP authentication failure trap mode

```
SWITCH/>snmp trap authentication disable
```

SNMP Trap Link-up

Description:

Set or show the port link-up and link-down trap mode.

Syntax:

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:

Set the SNMP trap link-up

```
SWITCH/>snmp trap link-up disable
```

SNMP Trap Inform Mode

Description:

Set or show the SNMP trap inform mode.

Syntax:

SNMP Trap Inform Mode [enable|disable]

Parameters:

enable : Enable SNMP trap inform

disable: Disable SNMP trap inform

(**default**: Show SNMP inform mode)

Default Setting:

disable

Example:

Set the SNMP trap inform mode

```
SWITCH/>snmp trap inform mode enable
```

SNMP Trap Inform Timeout

Description:

Set or show the SNMP trap inform timeout (usecs).

Syntax:

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 the SNMP trap inform timeout

```
SWITCH/>snmp trap inform timeout 10
```

SNMP Trap Inform Retry Times

Description:

Set or show the SNMP trap inform retry times.

Syntax:

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 the SNMP trap inform timeout

```
SWITCH/>snmp trap inform retry time 10
```

SNMP Trap Probe Security Engine ID

Description:

Show SNMP trap security engine ID probe mode.

Syntax:

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:

Set the SNMP trap probe security engine ID

```
SWITCH/>snmp trap probe security engine id disable
```

SNMP Trap Security Engine ID

Description:

Set or show SNMP trap security engine ID.

Syntax:

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

Default Setting:

empty

Example:

Set the SNMP trap security engine ID

```
SWITCH/>snmp trap security engine id 800007e5017f000011
```

SNMP Trap Security Name

Description:

Set or show SNMP trap security name.

Syntax:

SNMP Trap Security Name [<security_name>]

Parameters:

<security_name>: A string representing the security name for a principal

(**default**: Show SNMP trap security name)

Default Setting:

none

Example:

Set the SNMP trap security name

```
SWITCH/>snmp trap security name 12345678
```

SNMP Engine ID

Description:

Set or show SNMPv3 local engine ID.

Syntax:

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 the SNMP engine ID

```
SWITCH/>snmp engine id 800007e5017f000002
```

SNMP Community Add

Description:

Add or modify SNMPv3 community entry. The entry index key is <community>.

Syntax:

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/>snmp community add snmpv3_test 192.168.0.20 255.255.255.0
```

SNMP Community Delet

Description:

Delete SNMPv3 community entry.

Syntax:

SNMP Community Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 community entry

```
SWITCH/>snmp community delet 3
```

SNMP Community Lookup

Description:

Lookup SNMPv3 community entry.

Syntax:

SNMP Community Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 community entry

```
SWITCH/>snmp community lookup
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
3     snmpv3_test                     192.168.0.20       255.255.255.0

Number of entries: 3
```

SNMP User Add

Description:

Add SNMPv3 user entry. The entry index key are <engineid> and <user_name> and it doesn't allow modify.

Syntax:

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/>snmp user add 800007e5017f000003 admin_snmpv3 md5 12345678 des abcdefgh
```

SNMP User Change Key

Description:

Change SNMPv3 user password.

Syntax:

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

SNMP User Lookup

Description:

Lookup SNMPv3 user entry.

Syntax:

SNMP User Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 user entry

```
SWITCH/>snmp user lookup
Idx Engine ID User Name                           Level          Auth   Priv
--- --------- --------------------------------   --------------   ----   ----
1    Remote    admin_snmpv3                       Auth, Priv     MD5    DES

Number of entries: 1
```

SNMP Group Add

Description:

Add or modify SNMPv3 group entry. The entry index key are <security_model> and <security_name>.

Syntax:

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

<group_name> : A string identifying the group name that this entry should belong to

Example:

Add SNMPv3 group entry

```
SWITCH/>snmp group add usm admin_snmpv3 group_snmpv3
```

SNMP Group Delete

Description:

Delete SNMPv3 group entry.

Syntax:

SNMP Group Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 group entry

```
SWITCH/>snmp group delete 3
```

SNMP Group Lookup

Description:

Lookup SNMPv3 group entry.

Syntax:

SNMP Group Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 group entry

```
SWITCH/> snmp group lookup
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
```

SNMP View Add

Description:

Add or modify SNMPv3 view entry. The entry index key are <view_name> and <oid_subtree>.

Syntax:

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/> snmp view add snmpv3_viwe include .1
```

SNMP View Delete

Description:

Delete SNMPv3 view entry.

Syntax:

SNMP View Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 view entry

```
SWITCH/> snmp view delete 3
```

SNMP View Lookup

Description:

Lookup SNMPv3 view entry.

Syntax:

SNMP View Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 view entry

```
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
```

SNMP Access Add

Description:

Add or modify SNMPv3 access entry. The entry index key are <group_name>, <security_model> and <security_level>.

Syntax:

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/> snmp access add group_snmpv3 usm authpriv snmpv3_view snmpv3_view
```

SNMP Access Delete

Description:

Delete SNMPv3 access entry.

Syntax:

SNMP Access Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Add SNMPv3 access entry

```
SWITCH/> snmp access delete 3
```

SNMP Access Lookup

Description:

Lookup SNMPv3 access entry.

Syntax:

SNMP Access Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 access entry

```
SWITCH/> 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
```

6.4 Port Management Command

Port Configuration

Description:

Show port configuration.

Syntax:

Port Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Display port1~4 status

```
SWITCH/>port configuration 1-4

Port  State     Mode    Flow Control  MaxFrame   Power     Excessive  Link
------ --------  ------  ------------- ---------- --------  ---------  ----
1     Enabled   Auto    Disabled      9600       Enabled   Discard    Down
2     Enabled   Auto    Disabled      9600       Enabled   Discard    Down
3     Enabled   Auto    Disabled      9600       Enabled   Discard    Down
4     Enabled   Auto    Disabled      9600       Enabled   Discard    100fdx
```

Port State

Description:

Set or show the port administrative state.

Syntax:

Port State [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port

disable : Disable port

(**default**: Show administrative mode)

Default Setting:

Enable

Example:

Disable port1

```
SWITCH/>port state 1 disable
```

Port Mode

Description:

Set or show the port speed and duplex mode.

Syntax:

Port Mode [<port_list>] [10hdx|10fdx|100hdx|100fdx|1000fdx|auto]

Parameters:

<port_list>: Port list or 'all', default: All ports

10hdx : 10 Mbps, half duplex

10fdx : 10 Mbps, full duplex

100hdx : 100 Mbps, half duplex

100fdx : 100 Mbps, full duplex

1000fdx : 1 Gbps, full duplex

auto : Auto negotiation of speed and duplex

(**default**: Show configured and current mode)

Default Setting:

Auto

Example:

Set 10Mbps (half duplex) speed for port1

```
SWITCH/>port mode 1 10hdx
```

Port Flow Control

Description:

Set or show the port flow control mode.

Syntax:

Port Flow Control [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable flow control

disable : Disable flow control

(**default**: Show flow control mode)

Default Setting:

Disable

Example:

Enable flow control function for port1

```
SWITCH/>port flow control 1 enable
```

Port Maximum Frame

Description:

Set or show the port maximum frame size.

Syntax:

Port MaxFrame [<port_list>] [<max_frame>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<max_frame>: Port maximum frame size (1518-9600), default: Show maximum frame size

Default Setting:

9600

Example:

Set 2048 frame size for port1

```
SWITCH/>port maxframe 1 2048
```

Port SFP

Description:

Show SFP port information.

Syntax:

Port SFP [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show SFP port information

```
SWITCH/>port sfp

Port   Type              Speed        Wave Length(nm)   Distance(m)
----   --------------     --------     ---------------    -----------
7       --                  --          --                  --
8       1000Base-LX        1000-Base   1550               70000
```

Port Power

Description:

Set or show the port PHY power mode.

Syntax:

Port Power [<port_list>] [enable|disable|actiphy|dynamic]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable all power control

disable: Disable all power control

actiphy: Enable ActiPHY power control

dynamic: Enable Dynamic power control

Default Setting:

Enable

Example:

Disable port power function for port1-4

```
SWITCH/>port power 1-4 disable
```

Port Excessive

Description:

Set or show the port excessive collision mode.

Syntax:

Port Excessive [<port_list>] [discard|restart]

Parameters:

<port_list>: Port list or 'all', default: All ports

discard : Discard frame after 16 collisions

restart : Restart backoff algorithm after 16 collisions

(default: Show mode)

Default Setting:

Discard

Example:

```
SWITCH/>port excessive 1 restart
```

Port Statistics

Description:

Show port statistics.

Syntax:

Port Statistics [<port_list>] [<command>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<command> : The command parameter takes the following values:

clear : Clear port statistics

packets : Show packet statistics

bytes : Show byte statistics

errors : Show error statistics

discards : Show discard statistics

filtered : Show filtered statistics

low : Show low priority statistics

normal : Show normal priority statistics

medium : Show medium priority statistics

high : Show high priority statistics

(default: Show all port statistics)

Port VeriPHY

Description:

Run cable diagnostics.

Syntax:

Port VeriPHY [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Port Numbers

Description:

Show port numbering.

Syntax:

Port Numbers

Port Mirror Configuration

Description:

Show mirror configuration.

Syntax:

Mirror Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Port Mirror Port

Description:

Set or show the mirror port.

Syntax:

Mirror Port [<port>|disable]

Parameters:

<port>|disable: Mirror port or 'disable', default: Show port

Default Setting:

Disable

Port Mirror Mode

Description:

Set or show the mirror mode.

Syntax:

Mirror Mode [<port_list>] [enable|disable|rx|tx]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable Rx and Tx mirroring

disable: Disable Mirroring

rx : Enable Rx mirroring

tx : Enable Tx mirroring

(default: Show mirror mode)

Default Setting:

Disable

Example:

Enable mirror mode for port20

```
SWITCH/>mirror mode 20 enable
```

6.5 Link Aggregation Command

Link Aggregation Configuration

Description:

Show link aggregation configuration.

Syntax:

Aggr LACP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

```
SWITCH/>aggr 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
```

Link Aggregation Mode

Description:

Set or show LACP mode.

Syntax:

Aggr 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:

Set LACP mode

```
SWITCH/>aggr lacp mode 1-4 enable
```

LACP Key

Description:

Set or show the LACP key.

Syntax:

Aggr 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/>aggr lacp key 1-4 1
```

LACP Role

Description:

Set or show the LACP role.

Syntax:

Aggr 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/>aggr lacp role 1-4 passive
```

LACP Status

Description:

Show LACP Status.

Syntax:

Aggr LACP Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LACP status of port1~4

```
SWITCH/>aggr lacp status 1-4

Port   Mode        Key     Aggr ID   Partner System ID   Partner Port
------ ----------- -----   -------   -----------------   ------------
1      Disabled    1          -          -                   -
2      Disabled    1          -          -                   -
3      Disabled    1          -          -                   -
4      Disabled    1          -          -                   -
```

LACP Statistics

Description:

Show LACP Statistics.

Syntax:

Aggr 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/>aggr 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
```

Aggregation Configuration

Description:

Show link aggregation configuration.

Syntax:

Aggr Configuration

Default Setting:

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

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      Configured Ports     Aggregated Ports
-------    ------    ------    ----------------     ----------------
1          LLAG1     Static     1-4                  None
```

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
```

6.6 VLAN Configuration Command

VLAN Configuration

Description:

Show VLAN configuration.

Syntax:

VLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show VLAN status of port1

```
SWITCH/>vlan configuration 1

Mode : IEEE 802.1Q
Port PVID   IngrFilter   FrameType    LinkType   Q-in-Q Mode    Eth type
-------------   ----------     ---------------    ------------    ------------------    --------
1      1       Disabled      All            UnTag       Disable          N/A

VID     Ports
----       -----
1        1-26
```

VLAN Mode

Description:

Set or show the VLAN Mode.

Syntax:

VLAN Mode [portbased|dot1q]

Parameters:

portbased : Port-Based VLAN Mode

dot1q : 802.1Q VLAN Mode

(**default**: Show VLAN mode)

Default Setting:

IEEE 802.1Q

Example:

Set VLAN mode in port base

```
SWITCH/>vlan mode portbased
```

VLAV PVID

Description:

Set or show the port VLAN ID.

Syntax:

VLAN PVID [<port_list>] [<vid>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<vid> : VLAN ID (1-4095)

Default Setting:

1

Example:

Set PVID2 for port20

```
SWITCH/>vlan pvid 20 2
```

VLAN Frame Type

Description:

Set or show the port VLAN frame type.

Syntax:

VLAN FrameType [<port_list>] [all|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports

all : Allow tagged and untagged frames

tagged : Allow tagged frames only

(**default**: Show accepted frame types)

Default Setting:

All

Example:

Set port20 that allow tagged frames only

```
SWITCH/>vlan frametype 20 tagged
```

VLAN Ingress Filter

Description:

Set or show the port VLAN ingress filter.

Syntax:

VLAN IngressFilter [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable VLAN ingress filtering

disable : Disable VLAN ingress filtering

(**default**: Show VLAN ingress filtering)

Default Setting:

Disable

Example:

Enable VLAN ingress filtering for port20

```
SWITCH/>vlan ingressfilter 20 enable
```

VLAN Link Type

Description:

Set or show the port VLAN link type.

Syntax:

VLAN LinkType [<port_list>] [untagged|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports

untagged : VLAN Link Type Tagged

tagged : VLAN Link Type Untagged

(**default**: 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 Q-in-Q VLAN mode)

Default Setting:

disable

Example:

Enable Q-in-Q for port2

```
SWITCH/>vlan qinqmode 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 Q-in-Q VLAN out layer VLAN tag ether type)

Default Setting:

N/A

Example:

```
SWITCH/>vlan ethtype 10 man
```

VLAN Add

Description:

Add or modify VLAN entry.

Syntax:

VLAN Add <vid> [<port_list>]

Parameters:

<vid> : VLAN ID (1-4095)

<port_list>: Port list or 'all', default: All ports

Default Setting:

1

Example:

Add port17 to port24 in VLAN10

```
SWITCH/>vlan add 10 17-24
```

VLAN Delete

Description:

Delete VLAN entry.

Syntax:

VLAN Delete <vid>

Parameters:

<vid>: VLAN ID (1-4095)

Example:

Delete port17 to port24 in VLAN10

```
SWITCH/>vlan delete 10 17-24
```

VLAN Lookup

Description:

Lookup VLAN entry.

Syntax:

VLAN Lookup [<vid>]

Parameters:

<vid>: VLAN ID (1-4095), default: Show all VLANs

Example:

Show VLAN status

```
SWITCH/>vlan lookup


VID     Ports
----    -----
1       1-8
```

PVLAN Configuration

Description:

Show Private VLAN configuration.

Syntax:

VLAN PVLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show private VLAN configuration

```
SWITCH/>vlan pvlan configuration

Port   Isolation
----   ---------
1        Promiscuous
2        Promiscuous
3        Promiscuous
4        Promiscuous
5        Promiscuous
6        Promiscuous
7        Promiscuous
8        Promiscuous

PVLAN ID   Ports
--------         -----
1                   1-8
```

PVLAN Add

Description:

Add or modify Private VLAN entry.

Syntax:

VLAN PVLAN Add <pvlan_id> [<port_list>]

Parameters:

<pvlan_id> : Private VLAN ID

<port_list>: Port list or 'all', default: All ports

Example:

Add port1 in PVLAN5

```
SWITCH/>vlan pvlan add 5 1
```

PVLAN Delete

Description:

Delete Private VLAN entry.

Syntax:

VLAN PVLAN Delete <pvlan_id>

Parameters:

<pvlan_id>: Private VLAN ID

Example:

Delete PVLAN5

```
SWITCH/>vlan pvlan delete 5
```

PVLAN Lookup

Description:

Lookup Private VLAN entry.

Syntax:

VLAN PVLAN Lookup [<pvlan_id>]

Parameters:

<pvlan_id>: Private VLAN ID, default: Show all PVLANs

Example:

Delete PVLAN5

```
SWITCH/>vlan pvlan lookup

PVLAN ID   Ports
--------   -----
1          1-8
```

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/>vlan pvlan isolate 10 enable
```

6.7 Spanning Tree Protocol Command

STP Configuration

Description:

Show STP Bridge configuration.

Syntax:

STP Configuration

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

Example:

Show STP Bridge configuration

```
SWITCH/> configuration
Protocol Version    : MSTP
Max Age             : 20
Forward Delay       : 15
Tx Hold Count       : 6
Max Hop Count       : 20
BPDU Filtering      : Disabled
BPDU Guard          : Disabled
Error Recovery      : Disabled
```

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 Max Hops

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 Max Age

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 Forward Delay

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 BPDU Filter

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 BPDU Guard

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
```

MSTP Configuration

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 root 10
```

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

Example:

Show STP Bridge status.

```
SWITCH/>stp status
CIST Bridge STP Status
Bridge ID      : 80:00-00:30:4F:80:20:AA
Root ID        : 80:00-00:30:4F:80:20:AA
Root Port      : -
Root PathCost: 0
Regional Root: 80:00-00:30:4F:80:20:AA
Int. PathCost: 0
Max Hops       : 20
TC Flag        : Steady
TC Count       : 0
TC Last        : -
Port       Port Role       State        Pri   PathCost  Edge  P2P   Uptime
---------  --------------  ----------   ---   --------  ----  ---   -------------
     5     DesignatedPort  Forwarding   128   20000     Yes   Yes   0d 00:01:52
```

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 stutas 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 Auto Edge

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 Restricted Role

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 Restricted TCN

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 BPDU Guard

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

STP Port Migration Check

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

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

6.8 Multicast Configuration Command

IGMP Configuration

Description:

Show IGMP snooping configuration.

Syntax:

IGMP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Default Setting:

IGMP Mode: Disabled

Flooding : Disabled

Example:

Show IGMP snooping

```
SWITCH/>igmp configuration
IGMP Mode: Disabled
IGMP Leave Proxy: Disabled
Flooding : Disabled

VID    State      Querier
----   --------   --------
1      Enabled    Disabled

Port   Router     Dynamic Router    Fast Leave   Group Throttling Number
----   --------   ----------------  ----------   -------------------------
1      Disabled   no                Disabled     Unlimited
2      Disabled   no                Disabled     Unlimited
3      Disabled   no                Disabled     Unlimited
4      Disabled   no                Disabled     Unlimited
5      Disabled   no                Disabled     Unlimited
6      Disabled   no                Disabled     Unlimited
7      Disabled   no                Disabled     Unlimited
8      Disabled   no                Disabled     Unlimited

Port   Filtering Groups
----   ------------------
1      No Filtering Group
2      No Filtering Group
3      No Filtering Group
```

```
4      No Filtering Group
5      No Filtering Group
6      No Filtering Group
7      No Filtering Group
8      No Filtering Group
```

IGMP Mode

Description:

Set or show the IGMP snooping mode.

Syntax:

IGMP Mode [enable|disable]

Parameters:

enable : Enable IGMP snooping

disable: Disable IGMP snooping

(default: Show IGMP snooping mode)

Default Setting:

Disabled

Example:

Enable IGMP mode

```
SWITCH/>igmp mode enable
```

IGMP State

Description:

Set or show the IGMP snooping state for VLAN.

Syntax:

IGMP State [<vid>] [enable|disable]

Parameters:

<vid> : VLAN ID (1-4095), default: Show all VLANs

enable : Enable IGMP snooping

disable: Disable IGMP snooping

(default: Show IGMP snooping mode)

Parameters:

Enable

Example:

Disable IGMP state for vlan1

```
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 IGMP snooping querier in vlan1

```
SWITCH/>igmp querier 1 enable
```

IGMP Fast Leave

Description:

Set or show the IGMP snooping fast leave port mode.

Syntax:

IGMP Fastleave [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable IGMP fast leave

disable : Disable IGMP fast leave

(default: Show IGMP fast leave mode)

Default Setting:

Disable

Example:

Enable IGMP snooping fast leave mode for port1

```
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 IGMP port throttling status for port1 in value 10

```
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 group

Example:

Set IGMP port group filtering list in port1 with 224.0.0.1

```
SWITCH/>igmp filtering 1 add 224.0.0.1
```

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

Example:

Enable IGMP flooding function

```
SWITCH/>igmp status 1

Switch 1:
---------

      Querier   Rx          Tx          Rx          Rx          Rx          Rx
VID   Status    Queries     Queries     V1 Reports  V2 Reports  V3 Reports  V2 Leave
----  --------  ----------  ----------  ----------  ----------  ----------  ---------
1     IDLE      0           0           0           0           0           0
```

6.9 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

```
SWITCH/> 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
5       Low        0                1          Disabled       Disabled     Strict       1/2/4/8
6       Low        0                1          Disabled       Disabled     Strict       1/2/4/8
7       Low        0                1          Disabled       Disabled     Strict       1/2/4/8
8       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 Tag Priority

Description:

Set or show the port VLAN tag priority.

Syntax:

QoS Tagprio [<port_list>] [<tag_prio>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<tag_prio> : VLAN tag priority (0-7)

Default Setting:

0

Example:

Set priority7 for VLAN3

```
SWITCH/>qos tagprio 3 7
```

QoS QCL Port

Description:

Set or show the port QCL ID.

Syntax:

QoS QCL Port [<port_list>] [<qcl_id>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<qcl_id> : QCL ID

Default Setting:

1

Example:

Set QCL ID5 for port10

```
SWITCH/>qos qcl port 10 5
```

QoS QCL Add

Description:

Add or modify QoS Control Entry (QCE).

If the QCE ID parameter <qce_id> is specified and an entry with this QCE ID already exists, the QCE will be modified. Otherwise, a new QCE will be added. If the QCE ID is not specified, the next available QCE ID will be used.

If the next QCE ID parameter <qce_id_next> is specified, the QCE will be placed before this QCE in the list. If the next QCE ID is not specified, the QCE will be placed last in the list.

Syntax:

```
QoS QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>]
            (etype <etype>) |
            (vid <vid>) |
            (port <udp_tcp_port>) |
            (dscp <dscp>) |
            (tos <tos_list>) |
            (tag_prio <tag_prio_list>)
            <class>
```

Parameters:

<qcl_id> : QCL ID

<qce_id> : QCE ID (1-24)

<qce_id_next> : Next QCE ID (1-24)

etype : Ethernet Type keyword

<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 port10

```
SWITCH/>qos mode 10 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 port1~8

```
SWITCH/>qos rate limiter 1-8 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 1~8

```
SWITCH/>qos shaper 1-8 enable 1000
```

QoS Strom 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 Storm Multicast

Description:

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Multicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable multicast storm control

disable : Disable multicast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable multicast storm rate limiter in 1kpps

```
SWITCH/>qos storm multicast enable 1k
```

QoS Broadcast

Description:

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Broadcast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable broadcast storm control

disable : Disable broadcast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable broadcast storm rate limiter in 1kpps

```
SWITCH/>qos storm broadcast enable 1k
```

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 DSCP remarking in port1

```
SWITCH/>qos dscp remarking 1 enable
```

QoS DSCP Queue Mapping

Description:

Set or show the DSCP value for QoS DSCP Remarking.

Syntax:

QoS DSCP Queue Mapping [<port_list>] [<class>] [<dscp>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<class> : Traffic class low/normal/medium/high or 1/2/3/4

<dscp> : QoS DSCP Remarking Value 0/8/16/24/32/40/48/56/46

6.10 802.1x Port Access Control Command

Dot1x Configuration

Description:

Show 802.1X configuration.

Syntax:

Dot1x Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show IEEE802.1x status of port1

```
SWITCH/>dot1x configuration 1
Mode              : Disabled
Reauthentication  : Disabled
Period            : 3600
Timeout           : 30
Age Period        : 300
Hold Time         : 10

Port  Admin State   Port State            Last Source       Last ID
----   ------------   ---------------------   -----------------   -------
1      Authorized    802.1X Disabled        -                   -
```

Dotx1 Mode

Description:

Set or show the 802.1X mode for the switch.

Syntax:

Dot1x Mode [enable|disable]

Parameters:

enable : Enable 802.1X

disable: Disable 802.1X

(default: Show 802.1X mode)

Default Setting:

Disable

Example:

Enable IEEE802.1x founction for port1

```
SWITCH/>dot1x mode enable
```

Dot1x State

Description:

Set or show the 802.1X port state.

Syntax:

Dot1x State [<port_list>] [macbased|auto|authorized|unauthorized]

Parameters:

<port_list>: Port list or 'all', default: All ports

macbased : Switch performs 802.1X authentication on behalf of the client

auto : Port access requires 802.1X authentication

authorized : Port access is allowed

unauthorized: Port access is not allowed

(default: Show 802.1X state)

Default Setting:

Authorized

Example:

Change IEEE802.1x mode in auto for port1.

```
SWITCH/>dot1x state 1 auto
```

Dot1x Authenticate

Description:

Refresh (restart) 802.1X authentication process.

Syntax:

Dot1x Authenticate [<port_list>] [now]

Parameters:

<port_list>: Port list or 'all', default: All ports

now : Force reauthentication immediately

Dot1x Re-authentication

Description:

Set or show Reauthentication mode.

Syntax:

Dot1x Reauthentication [enable|disable]

Parameters:

enable : Enable reauthentication

disable: Disable reauthentication

(default: Show reauthentication mode)

Default Setting:

Disable

Example:

Enable re-authentication function

```
SWITCH/>dot1x reauthentication enable
```

Dot1x Period

Description:

Set or show the period between reauthentications.

Syntax:

Dot1x Period [<reauth_period>]

Parameters:

<reauth_period>: Period between reauthentications (1-3600 seconds)

(default: Show reauthentication period)

Default Setting:

3600

Example:

Set period re-authentication time in 3000 seconds

```
SWITCH/>dot1x period 3000
```

Dot1x Timeout

Description:

Set or show the time between EAPOL retransmissions.

Syntax:

Dot1x Timeout [<eapol_timeout>]

Parameters:

<eapol_timeout>: Time between EAPOL retransmissions (1-255 seconds)

(default: Show retransmission timeout)

Default Setting:

30

Example:

Set re-transmission time in 60 seconds

```
SWITCH/>dot1x timeout 60
```

Dot1x Statistics

Description:

Show 802.1X statistics.

Syntax:

Dot1x Statistics [<port_list>] [clear|eapol|radius]

Parameters:

<port_list>: Port list or 'all', default: All ports

eapol : Show EAPOL statistics

radius : Show RADIUS statistics

(default: Show all statistics)

Dot1x Clients

Description:

Set or show the maximum number of allowed clients for MAC-based ports.

Syntax:

Dot1x Clients [<port_list>] [all|<client_cnt>]

Parameters:

<port_list> : Port list or 'all', default: All ports

all|<client_cnt>: MAC-based authentication: Set maximum number of clients allowed on a port.

all : Allow all new clients

<client_cnt> : A number >= 1

(default: Show current maximum)

Default Setting:

All

Dot1x Agetime

Description:

Time in seconds between check for activity on successfully authenticated MAC addresses.

Syntax:

Dot1x Agetime [<age_time>]

Parameters:

<age_time>: Time between checks for activity on a MAC address that succeeded authentication

(default: Show age time)

Default Setting:

300

Example:

Set age time in 100 seconds

```
SWITCH/>dot1x agetime 100
```

Dot1x Holdtime

Description:

Time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Syntax:

Dot1x Holdtime [<hold_time>]

Parameters:

<hold_time>: Hold time before MAC addresses that failed authentication expire

(default: Show hold time)

Default Setting:

10

Example:

Set hold time in 100 seconds

```
SWITCH/>dot1x holdtime 100
```

6.11 Access Control List Command

ACL Configuration

Description:

Show ACL Configuration.

Syntax:

ACL Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Default Setting:

300

Example:

Show ACL configuration state for port1

```
SWITCH/>acl configuration 1

Port  Policy  Action  Rate Limiter  Port Copy  Logging  Shutdown  Counter
----  ------  ------  ------------  ---------  -------- --------  -------
1     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
```

ACL Action

Description:

Set or show the ACL port default action.

Syntax:

ACL Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]

Parameters:

<port_list> : Port list or 'all', default: All ports

permit : Permit forwarding (default)

deny : Deny forwarding

<rate_limiter>: Rate limiter number (1-15) or 'disable'

<port_copy> : Port number for copy of frames or 'disable'

<logging> : System logging of frames: log|log_disable

<shutdown> : Shut down ingress port: shut|shut_disable

Default Setting:

Action: Permit

Rate Limiter: Disable

Port Copy: Disable

Loading: Disable

Shut down: Disable

Example:

Set ACL rule in port1~8

```
SWITCH/>acl action 1-8 deny 1 8 log shut
```

ACL Policy

Description:

Set or show the ACL port policy.

Syntax:

ACL Policy [<port_list>] [<policy>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<policy> : Policy number (1-8)

Default Setting:

1

Example:

Set policy ID 8 for port 1-8

```
SWITCH/>acl policy 1-8 8
```

ACL Rate

Description:

Set or show the ACL rate limiter.

Syntax:

ACL Rate [<rate_limiter_list>] [<packet_rate>]

Parameters:

<rate_limiter_list>: Rate limiter list (1-15), default: All rate limiters

<packet_rate> : Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

1

Example:

Set the ACL rate limiter

```
SWITCH/>acl rate 15 1024k
```

ACL Add

Description:

Add or modify Access Control Entry (ACE).

If the ACE ID parameter <ace_id> is specified and an entry with this ACE ID already exists, the ACE will be modified. Otherwise, a new ACE will be added. If the ACE ID is not specified, the next available ACE ID will be used.

If the next ACE ID parameter <ace_id_next> is specified, the ACE will be placed before this ACE in the list. If the next ACE ID is not specified, the ACE will be placed last in the list.

Syntax:

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>]

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

ACL Delete

Description:

Delete ACE.

Syntax:

ACL Delete <ace_id>

Parameters:

<ace_id>: ACE ID (1-128)

ACL Lookup

Description:

Show ACE, default: All ACEs.

Syntax:

ACL Lookup [<ace_id>]

Parameters:

<ace_id>: ACE ID (1-128)

ACL Clear

Description:

Clear all ACL counters.

Syntax:

ACL Clear

6.12 MAC Address Table Command

MAC Configuration

Description:

Show MAC address table configuration.

Syntax:

MAC Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show port1 Mac state

```
SWITCH/>mac configuration 1
MAC Age Time: 300

Port   Learning
----   --------
1        Auto
```

MAC Add

Description:

Add MAC address table entry.

Syntax:

MAC Add <mac_addr> <port_list> [<vid>]

Parameters:

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)

<port_list>: Port list or 'all' or 'none'

<vid> : VLAN ID (1-4095), default: 1

Example:

Add Mac address 00-30-4F-01-01-02 in port1 and vid1

```
SWITCH/>mac add 00-30-4f-01-01-02 1 1
```

MAC Delete

Description:

Delete MAC address entry.

Syntax:

MAC Delete <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

<vid> : VLAN ID (1-4095), default: 1

Example:

Delete Mac address 00-30-4F-01-01-02 in vid1

```
SWITCH/>mac delete 00-30-4f-01-01-02 1
```

MAC Lookup

Description:

Lookup MAC address entry.

Syntax:

MAC Lookup <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

<vid> : VLAN ID (1-4095), default: 1

Example:

Lookup state of Mac address 00-30-4F-01-01-02

```
SWITCH/>mac lookup 00-30-4f-01-01-02
```

MAC Age Time

Description:

Set or show the MAC address age timer.

Syntax:

MAC Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (10-1000000), default: Show age time

Default Setting:

300

Example:

Set agetime value in 30

```
SWITCH/>mac agetime 30
```

MAC Learning

Description:

Set or show the port learn mode.

Syntax:

MAC Learning [<port_list>] [auto|disable|secure]

Parameters:

<port_list>: Port list or 'all', default: All ports

auto : Automatic learning

disable: Disable learning

secure : Secure learning

(default: Show learn mode)

Default Setting:

Auto

Example:

Set secure learning mode in port1

```
SWITCH/>
```

MAC 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

MAC Statistics

Description:

Show MAC address table statistics.

Syntax:

MAC Statistics [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Set all of MAC statistics

```
SWITCH/>mac statistics
```

MAC Flash

Description:

Flush all learned entries.

Syntax:

MAC Flush

6.13 LLDP Command

LLDP Configuration

Description:

Show LLDP configuration.

Syntax:

LLDP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

LLDP Mode

Description:

Set or show LLDP mode.

Syntax:

LLDP Mode [<port_list>]   [enable|disable|rx|tx]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable LLDP reception and transmission

disable: Disable LLDP

rx   : Enable LLDP reception only

tx   : Enable LLDP transmission only

(default: Show LLDP mode)

Default Setting:

Disable

Example:

Enable port1 LLDP function.

```
SWITCH/>lldp mode 1 enable
```

LLDP Optional TLV

Description:

Set or show 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:

2

Example:

Set LLDP delay value in 1

```
SWITCH/>lldp delay 1
```

LLDP Reinit

Description:

Set or show LLDP reinit delay.

Syntax:

LLDP Reinit [<reinit>]

Parameters:

<reinit>: LLDP reinit delay (1-10)

Default Setting:

2

Example:

Set LLDP reinit delay value in 3

```
SWITCH/>lldp reinit 3
```

LLDP Information

Description:

Show LLDP neighbor device information.

Syntax:

LLDP Info [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

LLDP Statistics

Description:

Show LLDP Statistics.

Syntax:

LLDP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear LLDP statistics

LLDP CDP Aware

Description:

Set or show if discovery information from received CDP (Cisco Discovery Protocol) frames is added to the LLDP neighbor table.

Syntax:

LLDP cdp_aware [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable CDP awareness (CDP discovery information is added to the LLDP neighbor table)

disable : Disable CDP awareness

(default: Show LLDP mode)

6.14 Authentication Command

Aythentication Configuration

Description:

Show Auth configuration.

Syntax:

Auth Configuration

Example:

Show Auth configuration

```
SWITCH/> 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

Client Configuration:
=====================
Client     Authentication Method     Local Authentication Fallback
-------      ----------------------        ----------------------------
telnet     local                             Disabled
ssh         local                             Disabled
web          local                           Disabled
console     local                            Disabled
```

Authentication Timeout

Description:

Set or show server timeout.

Syntax:

Auth Timeout [<timeout>]

Parameters:

<timeout>: Server response timeout (3-3600 seconds)

(default: Show server timeout configuration)

Default:

15 seconds

Example:

Set 30 seconds in server timeout value

```
SWITCH/>auth timeout 30
```

Authentication Dead Time

Description:

Set or show server dead time.

Syntax:

Auth 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:

300 seconds

Example:

Set 3000 seconds in server timeout value

```
SWITCH/>auth deadtime 3000
```

Authentication RADIUS Server

Description:

Set or show RADIUS authentication server setup.

Syntax:

Auth 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)

Default:

Mode: Disable, Port: 1812

Example:

Set all of parameters for RADIUS server

```
SWITCH/>auth radius 5 enable 192.168.0.111 1234567890 1812
```

Authentication RADIUS Accounting Server

Description:

Set or show RADIUS accounting server setup.

Syntax:

Auth ACCT_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 (1813)

Default:

Mode: Disable, Port: 1813

Example:

Set all of parameters for RADIUS accounting server

```
SWITCH/>auth acct_radius 5 enable 192.168.0.111 1234567890 1813
```

Authentication TACACS+ Server

Description:

Set or show TACACS+ authentication server setup.

Syntax:

Auth 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)

Default:

Mode: Disable, Port: 49

Example:

Set all of parameters for TACACS+ server

```
SWITCH/>auth tacacs+ 5 enable 192.168.0.111 1234567890 49
```

Authentication Client

Description:

Set or show client setup.

Syntax:

Auth Client [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

(default: Show agent setup)

none : Authentication disabled

local : Use local authentication

radius : Use remote RADIUS authentication

tacacs+ : Use remote TACACS+ authentication

(default: Show agent authentication)

enable : Enable local authentication if remote authentication fails

disable : Disable local authentication if remote authentication fails

(default: Show backup agent authentication configuration)

Default:

Client	Authentication Method	Local Authentication Fallback
-------	----------------------	-----------------------------
telnet	local	Disabled
ssh	local	Disabled
web	local	Disabled
console	local	Disabled

Example:

Enable console interface with a remove RADIUS server for authentication

```
SWITCH/>auth client console radius enable
```

Authentication Statistics

Description:

Show RADIUS statistics.

Syntax:

Auth Statistics [<server_index>]

Parameters:

The server index (1-5)

(default: Show statistics for all servers)

6.15 DHCP Relay Command

DHCP Relay Configuration

Description:

Show DHCP relay configuration.

Syntax:

DHCP Relay Configuration

Example:

DHCP Relay Configuration

```
SWITCH/>dhcp relay configuration
DHCP Relay Mode                      : Disabled
DHCP Relay Server                    : NULL
DHCP Relay Information Mode         : Disabled
DHCP Relay Information Policy        : replace
```

DHCP Relay Mode

Description:

Set or show the DHCP relay mode.

Syntax:

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:

disable

Example:

Enable DHCP relay mode

```
SWITCH/>dhcp relay mode enable
```

DHCP Relay Server

Description:

Show or set DHCP relay server.

Syntax:

DHCP Relay Server [<ip_addr>]

Parameters:

<ip_addr>: IP address (a.b.c.d), default: Show IP address

Default:

0.0.0.0

Example:

Set up 192.168.0.30 for DHCP relay server

```
SWITCH/>dhcp relay server 192.168.0.30
```

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:

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:

disable

Example:

Enable DHCP relay information mode

```
SWITCH/>dhcp relay information mode enable
```

DHCP Relay Information Policy

Description:

Set or show the DHCP relay mode. When enable DHCP relay information mode operation, if agent receive a DH message that already contains relay agent information. It will enforce the policy..

Syntax:

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:

replace

Example:

Change DHCP relay information policy in "keep" mode

```
SWITCH/>dhcp relay information policy keep
```

DHCP Relay Statistics

Description:

Show or clear DHCP relay statistics.

Syntax:

DHCP Relay Statistics [clear]

Parameters:

clear: Clear DHCP relay statistics

DHCP Snooping Configuration

Description:

Show DHCP snooping configuration.

Syntax:

DHCP Snooping Configuration

Default:

disable

DHCP Snooping Mode

Description:

Set or show the DHCP snooping mode.

Syntax:

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:

disable

Example:

Enable DHCP snooping mode

```
SWITCH/>dhcp snooping mode enable
```

DHCP Snooping Port Mode

Description:

Set or show the DHCP snooping port mode.

Syntax:

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:

truated

Example:

Set DHCP snooping port mode in untrusted source in port1

```
SWITCH/>dhcp snooping port mode 1 untrusted
```

DHCP Snooping Statistics

Description:

Show or clear DHCP snooping statistics.

Syntax:

DHCP Snooping Statistics [<port_list>] [clear]

Parameters:

<port_list> : Port list or 'all', default: All ports

clear : Clear DHCP snooping statistics

6.16 Privilege Level Command

Privilege Level Users Configuration

Description:

Show users configuration.

Syntax:

Privilege Users Configuration

Example:

Show users configuration

```
SWITCH/>privilege users configuration
User Name                          Priviliege Level
-------------------------------    ----------------
admin                                          15
guest                                           5
```

Privilege Level Users Add

Description:

Add or modify users entry.

Syntax:

Privilege 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 users entry

```
SWITCH/>privilege users users add admin_neo 12345 10
```

Privilege Level Users Delete

Description:

Delete users entry.

Syntax:

Privilege Users Delete <user_name>

Parameters:

<user_name>: A string identifying the user name that this entry should belong to

Example:

Delete users entry

```
SWITCH/>privilege users users delete admin_neo
```

Privilege Level Configuration

Description:

Show privilege configuration.

Syntax:

Privilege Level Configuration

Parameters:

<user_name>: A string identifying the user name that this entry should belong to

Example:

Show privilege configuration

```
SWITCH/>privilege level configuration
Privilege Current Level: 15
Group Name                        Priviliege Level
                                 CRO   CRW   SRO   SRW
-------------------------------- --- --- --- ---
Aggregation                        5    10     5    10
DHCP_Relay                         5    10     5    10
DHCP_Snooping                      5    10     5    10
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
MAC_Table                          5    10     5    10
Maintenance                       15    15    15    15
Mirroring                          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                             1    10     5    10
```

```
UPnP                                    5     10      5    10
VLANs                                   5     10      5    10
```

Privilege Level Group

Description:

Configure a privilege level group.

Syntax:

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 VLAN's privilege level

```
SWITCH/>privilege level group vlans 10 15 10 15
```

Privilege Level Current

Description:

Show the current privilege level.

Syntax:

Privilege Level Current

Default:

15

6.17 ARP Command

ARP Inspection Configuration

Description:

Show users configuration.

Syntax:

Privilege Users Configuration

ARP Inspection Mode

Description:

Set or show ARP inspection mode.

Syntax:

ARP Inspection Mode [enable|disable]

Parameters:

enable : Enable ARP Inspection

disable: Disable ARP Inspection

Default:

disable

Example:

Enable ARP inspection mode

```
SWITCH/>arp inspection mode enable
```

ARP Inspection Port

Description:

Set or show the ARP Inspection port mode.

Syntax:

ARP Inspection port [<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:

disable

Example:

Enable ARP inspection port mode for port1

```
SWITCH/>arp inspection port 1 enable
```

ARP Inspection Entry

Description:

Add, delete or show ARP inspection static entries.

Syntax:

ARP Inspection Entry [<port_list>] [add|del] [vid] [allowed_mac] [allowed_ip]

Parameters:

<port_list> : Port list or 'all', default: All ports

add : Add new port ARP inspection static entry

del : Del existing port ARP inspection static entry

(default: Show port ARP inspection static entry list)

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

Example:

Add ARP inspection entry for port1

```
SWITCH/>arp inspection entry 1 add 00-30-4f-01-02-03 192.168.0.33
```

ARP Inspection Status

Description:

Show ARP inspection dynamic entries.

Syntax:

ARP Inspection Status

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.

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.

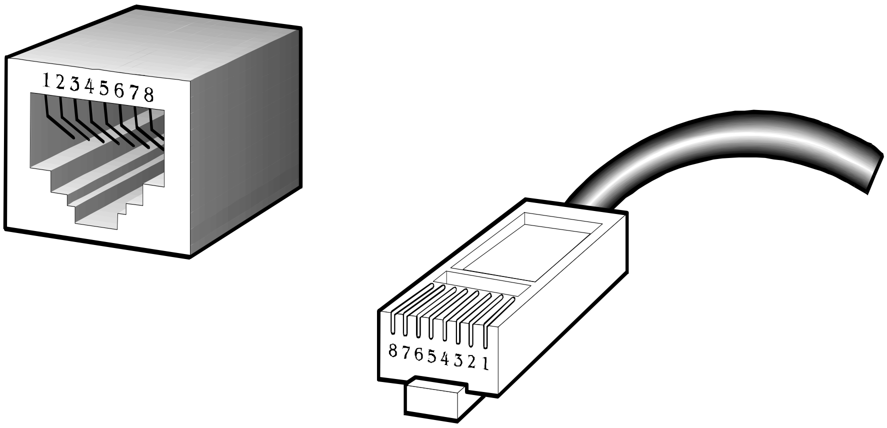
A.2 10/100Mbps, 10/100Base-TX

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**	

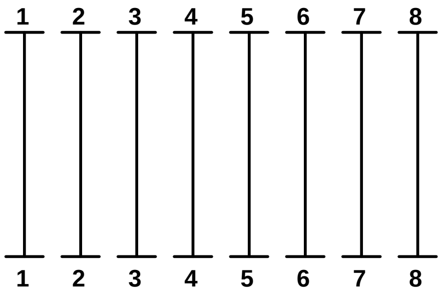
The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

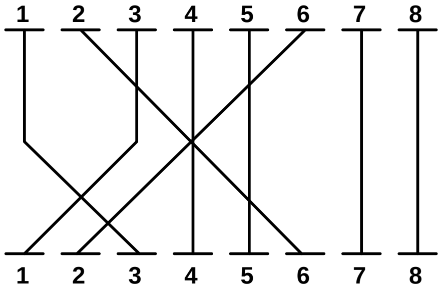
There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

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.

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 feautre. 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.

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

CDP

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

D

DES

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

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

DHCP

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

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

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

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

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 agent¡¦s MAC address.

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.

DNS

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

DoS

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

Dotted Decimal Notation

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

DSCP

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

E

Ethernet Type

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

F

FTP

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

Fast Leave

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

H

HTTP

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

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

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

HTTPS

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

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

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

I

ICMP

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

IEEE 802.1X

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

IGMP

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

IGMP Querier

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

IMAP

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

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

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

IP

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

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

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

IPMC

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

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, is used for network discovery, and works by having the units in the network exchanging information with their neighbors using LLDP frames.

M

MAC Table

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

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

MD5

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

Mirroring

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

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

N

NetBIOS

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

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

NFS

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

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

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.

P

PING

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

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

Policer

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

POP3

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

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

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

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

Private VLAN

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

Q

QCE

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

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

QCL

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

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

QoS

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

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

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

R

RARP

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

RADIUS

RADIUS is an acronym for **R**emote **A**uthentication **D**ial **I**n **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.

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.

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.

Switch ID

Switch IDs (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

T

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

A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV (TLV is short for "Type Length Value").

U

UDP

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

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

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

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

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.

EC Declaration of Conformity

For the following equipment:

*Type of Product: 8-Port 10/100/1000Mbps with 2 Shared SFP Managed Gigabit Switch
*Model Number: WGSD-8020

* 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:

EN55022	(CLASS A: 2006)
EN 61000-3-2	(2006)
EN 61000-3-3	(1995 / A1: 2001 / A2: 2005)
EN55024	(1998 / A1: 2001 / A2: 2003)
IEC 61000-4-2	(2001)
IEC 61000-4-3	(2008)
IEC 61000-4-4	(2004)
IEC 61000-4-5	(2005)
IEC 61000-4-6	(2008)
IEC 61000-4-8	(2001)
IEC 61000-4-11	(2004)

Responsible for marking this declaration if the:

☒ **Manufacturer** □ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **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 **22th Jan., 2010** Kent Kang
Place *Date* *Legal Signature*